OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI PEDAGOG KADRLARNI QAYTA TAYYORLASH VA ULARNING MALAKASINI OSHIRISH TARMOQ MARKAZI

“ZAMONAVIY KRIPTOTAHLIL USULLARI”
MODULI BO‘YICHA
O‘ Q U V –U S L U B I Y M A J M U A

Toshkent – 2025

O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

OLIY TA’LIM TIZIMI PEDAGOG VA RAHBAR KADRLARINI QAYTA TAYYORLASH VA ULARNING MALAKASINI OSHIRISHNI TASHKIL ETISH BOSH ILMIY - METODIK MARKAZI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI PEDAGOG KADRLARNI QAYTA TAYYORLASH VA ULARNING MALAKASINI OSHIRISH TARMOQ MARKAZI

“Kriptologiya” yo‘nalishi

“ZAMONAVIY KRIPTOTAHLIL USULLARI”

MODULI BO‘YICHA

O‘ Q U V –U S L U B I Y M A J M U A

Toshkent – 2025

Modulning o‘quv-uslubiy majmuasi Oliy ta’lim, fan va innovatsiyalar vazirligining 2024 yil 27 dekabrdagi №485-sonli buyrug‘i bilan tasdiqlangan o‘quv dasturi va o‘quv rejasiga muvofiq ishlab chiqilgan.

Tuzuvchilar: **I.M. Boyquziyev -** fizika-matematika fanlari bo‘yicha PhD

Taqrizchilar: **B.F. Abduraximov** - fizika-matematika fanlari doktori, professor
I.R. Rahmatullayev - texnika fanlari bo‘yicha PhD

O‘quv-uslubiy majmua O‘quv dasturi Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Kengashining qarori bilan tasdiqqa tavsiya qilingan (2024-yil 27-noyabrdagi 3/4 (745/746)- sonli bayonnoma).

MUNDARIJA

I-BO‘LIM
ISHCHI DASTUR

I. ISHCHI DASTUR

KIRISH

Dastur O‘zbekiston Respublikasining 2020 yil 23 sentabrda tasdiqlangan “Ta’lim to‘g‘risida”gi Qonuni, O‘zbekiston Respublikasi Prezidentining 2024 yil 15 avgustdagi “O‘zbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-293-sonli Qarori, O‘zbekiston Respublikasi Prezidentining 2017 yil 7 fevraldagi “O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasi to‘g‘risida”gi PF-4947-son, 2019 yil 27 avgustdagi “Oliy ta’lim muassasalari rahbar va pedagog kadrlarining uzluksiz malakasini oshirish tizimini joriy etish to‘g‘risida”gi PF-5789-son, 2019 yil 8 oktabrdagi “O‘zbekiston Respublikasi oliy ta’lim tizimini 2030 yilgacha rivojlantirish konsepsiyasini tasdiqlash to‘g‘risida”gi PF-5847-son va 2020 yil 29 oktabrdagi “Ilm-fanni 2030 yilgacha rivojlantirish konsepsiyasini tasdiqlash to‘g‘risida”gi PF-6097-sonli Farmonlari hamda O‘zbekiston Respublikasi Vazirlar Mahkamasining 2019 yil 23 sentabrdagi “Oliy ta’lim muassasalari rahbar va pedagog kadrlarining malakasini oshirish tizimini yanada takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi 797-sonli Qarorlarida belgilangan ustuvor vazifalar mazmunidan kelib chiqqan holda tuzilgan bo‘lib, u oliy ta’lim muassasalari pedagog kadrlarining kasb mahorati hamda innovatsion kompetentligini rivojlantirish, sohaga oid ilg‘or xorijiy tajribalar, yangi bilim va malakalarni o‘zlashtirish, shuningdek amaliyotga joriy etish ko‘nikmalarini takomillashtirishni maqsad qiladi.

Qayta tayyorlash va malaka oshirish yo‘nalishining o‘ziga xos xususiyatlari hamda dolzarb masalalaridan kelib chiqqan holda dasturda tinglovchilarning ushbu fan doirasidagi bilim, ko‘nikma, malaka hamda kompetensiyalariga qo‘yiladigan talablar takomillashtirilishi mumkin.

Modulning maqsadi va vazifalari

Modulining maqsadi: tinglovchilarni kiberxavfsizlikni ta’minlash sohasida zamonaviy kriptotahlil usullarini nazariy va amaliy izlanishlar orqali tanishtirish hisoblanadi. Kriptotahlilda foydalaniladigan turli zamonaviy yondashuvlar, usullar va vositalarni qo‘llashga doir bilimlar va ko‘nikmalar hosil qilishdan iborat.

Modulning vazifalari:

- kriptologiyaning asosiy tushunchalarini;
- axborotning kriptografik himoyasining zaruriyatini;
- kriptotahlilning zaruriyatini;
- klassik shifrlarning tahlilini amalga oshirish ketma-ketligini;

- kriptotahlilning universal usullari.
- klassik shifrlarning tahlilini amalga oshirish, kriptotahlilning universal usullaridan foydalanish, zamonaviy kriptografik algoritmlarning kriptotahlilini amalga oshirish, kriptografik akslantirishlarning xususiyatlariga qarab kriptotahlil usulini tanlash, zamonaviy kriptotahlil usullarining qiyosiy tahlilini amalga oshirish ko‘nikma va malakalarni shakllantirishdan iborat.

Modul bo‘yicha tinglovchilarning bilim, ko‘nikma, malaka va kompetensiyalariga qo‘yiladigan talablar

“Zamonaviy kriptotahlil usullari” modulini o‘zlashtirish jarayonida amalga oshiriladigan masalalar doirasida:

Tinglovchi:

– kriptologiyaning asosiy tushunchalarini;
– axborotning kriptografik himoyasining zaruriyatini;
– kriptotahlilning zaruriyatini;
– klassik shifrlarning tahlilini amalga oshirish ketma-ketligini;
– kriptotahlilning universal usullarini *bilishi* **kerak**.
– klassik shifrlarning tahlilini amalga oshirish, kriptotahlilning universal usullaridan foydalanish, zamonaviy kriptografik algoritmlarning kriptotahlilini amalga oshirish, kriptografik akslantirishlarning xususiyatlariga qarab kriptotahlil usulini tanlash, zamonaviy kriptotahlil usullarining qiyosiy tahlilini amalga oshirish ***malaka va ko‘nikmalariga*** ega bo‘lishi lozim.
– klassik shifrlarning tahlilini amalga oshirish, kriptotahlilning universal usullaridan foydalanish, zamonaviy kriptografik algoritmlarning kriptotahlilini amalga oshirish, kriptografik akslantirishlarning xususiyatlariga qarab kriptotahlil usulini tanlash, zamonaviy kriptotahlil usullarining qiyosiy tahlilini amalga oshirish ***kompetensiyalariga*** ega bo‘lishi lozim.

Modulni tashkil etish va o‘tkazish bo‘yicha tavsiyalar

“Zamonaviy kriptotahlil usullari” moduli ma’ruza va amaliy mashg‘ulotlar shaklida olib boriladi.

Modulni o‘qitish jarayonida ta’limning zamonaviy metodlari, pedagogik texnologiyalar va axborot-kommunikatsiya texnologiyalari qo‘llanilishi nazarda tutilgan:

- ma’ruza darslarida zamonaviy kompyuter texnologiyalari yordamida prezentatsion va elektron-didaktik texnologiyalardan;

- o‘tkaziladigan amaliy mashg‘ulotlarda texnik vositalardan, ekspress-so‘rovlar, test so‘rovlari, aqliy hujum, guruhli fikrlash, kichik guruhlar bilan ishlash, kollokvium o‘tkazish, va boshqa interaktiv ta’lim usullarini qo‘llash nazarda tutiladi.

Modulning o‘quv rejadagi boshqa modullar bilan bog‘liqligi va uzviyligi

“Zamonaviy kriptotahlil usullari” moduli mazmuni o‘quv rejadagi “Kriptografiyaning matematik asoslari”, “Kriptografik protokollar”, “Yengil vaznli kriptografiya”, “Post kvant kriptografiyasi” o‘quv modullari bilan uzviy bog‘langan holda tinglovchilarda kriptografik algoritmlarning bardoshliligini baholashning zamonaviy usullari hamda ulardan foydalanishning turli yondashuvlari bo‘yicha bilim darajasini oshirishga xizmat qiladi.

Modulning oliy ta’limdagi o‘rni

Modulni o‘zlashtirish orqali tinglovchilar ta’lim jarayonida kriptografik algoritmlarning bardoshliligini baholashning zamonaviy usullari hamda ulardan foydalanishning turli yondashuvlaridan foydalanish va amalda qo‘llashga doir kasbiy kompetentlikka ega bo‘ladilar.

MODUL BO‘YICHA SOATLAR TAQSIMOTI

№	Modul mavzulari	Auditoriya uquv yuklamasi			
		Jami	jumladan		
			Nazariy	Amaiy mashg‘ulot	Ko‘chma mashg‘uloti
1.	**Kriptologiyaning ilmiy yo‘nalishlari, kriptografiya va kriptotahlil.** Klassik shifrlarning kriptotahlili, kriptotahlilning sodda usullari. Kriptografik algoritmlar bardoshliligi va hisoblash murakkabligi nazariyasi, kriptografik bardoshlilik tushunchasi.	4	2	2	
2.	**Simmetrik blokli shifrlar kriptotahlilida statistik usullar.** Chiziqli, differensial va chiziqli-differensial kriptotahlil usullari.	4	2	2	
3.	**Simmetrik blokli shifrlar kriptotahlili.** Algebraik, integral, “Slaydli hujum” va apparat xatoliklarni generatsiyalashga asoslangan	4	2	2	

	kriptotahlil usullari.				
4.	**Asimmetrik kriptotizimlarni kriptotahlil qilish usullari.** Faktorlash va diskret logorifmlash muammosining murakkabligiga asoslangan kriptotizimlarning bardoshliligi.	4	2	2	
5.	**Xesh funksiyalarning kriptotahlili, Psevdotasodifiy va tasodifiy sonlar generatorlarining tahlilli.** Tug‘ilgan kun muammosi, MD4 va MD5 algoritmlarining kriptotahlili. NIST va DIEHARD statistik testlar to‘plami.	4	2	2	
5	**Oqimli shifrlash algoritmlarining kriptotahlili. Kriptotahlilda qo‘shimcha kanallar va yangi texnologiyalardan foydalanish.** Chiziqli, differensial, algebraik va boshqa kriptotahlil usullarining oqimli shifrlash algoritmlariga nisbatan qo‘llanilishi. Qo‘shimcha kanallardan foydalanishga asoslangan kriptotahlil usullari va kriptotahlilda yangi texnologiyalardan foydalanish.	2	2		
	Jami:	**22**	**12**	**10**	

NAZARIY MASHG‘ULOTLAR MAZMUNI

1-MAVZU: KRIPTOLOGIYANING ILMIY YO‘NALISHLARI, KRIPTOGRAFIYA VA KRIPTOTAHLIL (2 SOAT)

Klassik shifrlarning kriptotahlili, kriptotahlilning sodda usullari. Kriptografik algoritmlar bardoshliligi va hisoblash murakkabligi nazariyasi, kriptografik bardoshlilik tushunchasi.

2-MAVZU: SIMMETRIK BLOKLI SHIFRLAR KRIPTOTAHLILI.IDA STATISTIK USULLAR (2 SOAT)

Simmetrik blokli shifrlash algoritmlariga nisbatan chiziqli, differensial va chiziqli-differensial kriptotahlil usullari. Korrelyatsion matritsa va ayirma matritsani hisoblash.

3-MAVZU: SIMMETRIK BLOKLI SHIFRLAR KRIPTOTAHLILI (2 SOAT)

Algebraik, integral, “Slaydli hujum” va apparat xatoliklarni generatsiyalashga asoslangan kriptotahlil usullari. Algebraik tenglamalarni shakllantirish. Adaptiv tanlangan ochiq matnlar.

4-MAVZU: ASIMMETRIK KRIPTOTIZIMLARNI KRIPTOTAHLIL QILISH USULLARI (2 SOAT)

Faktorlash va diskret logorifmlash muammosining murakkabligiga asoslangan kriptotizimlarning bardoshliligi.

5-MAVZU: XESH FUNKSIYALARNING KRIPTOTAHLILI, PSEVDOTASODIFIY VA TASODIFIY SONLAR GENERATORLARINING TAHLILLI (2 SOAT)

Tug‘ilgan kun muammosi, MD4 va MD5 algoritmlarining kriptotahlili. NIST va DIEHARD statistik testlar to‘plami.

6-MAVZU: OQIMLI SHIFRLASH ALGORITMLARINING KRIPTOTAHLILI. KRIPTOTAHLILDA QO‘SHIMCHA KANALLAR VA YANGI TEXNOLOGIYALARDAN FOYDALANISH (2 SOAT)

Chiziqli, differensial, algebraik va boshqa kriptotahlil usullarining oqimli shifrlash algoritmlariga nisbatan qo‘llanilishi. Qo‘shimcha kanallardan foydalanishga asoslangan kriptotahlil usullari va kriptotahlilda yangi texnologiyalardan foydalanish.

AMALIY MASHG‘ULOTLAR MAZMUNI

1-MAVZU: KRIPTOLOGIYANING ILMIY YO‘NALISHLARI, KRIPTOGRAFIYA VA KRIPTOTAHLIL (2 SOAT)

Klassik shifrlarning kriptotahlili, kriptotahlilning sodda usullari. Kriptografik algoritmlar bardoshliligi va hisoblash murakkabligi nazariyasi, kriptografik bardoshlilik tushunchasi.

2-MAVZU: SIMMETRIK BLOKLI SHIFRLAR KRIPTOTAHLILI.IDA STATISTIK USULLAR (2 SOAT)

Simmetrik blokli shifrlash algoritmlariga nisbatan chiziqli, differensial va chiziqli-differensial kriptotahlil usullari. Korrelyatsion matritsa va ayirma matritsani hisoblash.

3-MAVZU: SIMMETRIK BLOKLI SHIFRLAR KRIPTOTAHLILI (2 SOAT)

Algebraik, integral, “Slaydli hujum” va apparat xatoliklarni generatsiyalashga asoslangan kriptotahlil usullari. Algebraik tenglamalarni shakllantirish. Adaptiv tanlangan ochiq matnlar.

4-MAVZU: ASIMMETRIK KRIPTOTIZIMLARNI KRIPTOTAHLIL QILISH USULLARI (2 SOAT)

Faktorlash va diskret logorifmlash muammosining murakkabligiga asoslangan kriptotizimlarning bardoshliligi.

5-MAVZU: XESH FUNKSIYALARNING KRIPTOTAHLILI, PSEVDOTASODIFIY VA TASODIFIY SONLAR GENERATORLARINING

TAHLILLI (2 SOAT)

Tug‘ilgan kun muammosi, MD4 va MD5 algoritmlarining kriptotahlili. NIST va DIEHARD statistik testlar to‘plami.

O‘QITISH SHAKLLARI

Mazkur modul bo‘yicha quyidagi o‘qitish shakllaridan foydalaniladi:

- ma’ruzalar, amaliy mashg‘ulotlar (ma’lumotlar va texnologiyalarni anglab olish, motivatsiyani rivojlantirish, nazariy bilimlarni mustahkamlash);
- davra suhbatlari (ko‘rilayotgan loyiha yechimlari bo‘yicha taklif berish qobiliyatini rivojlantirish, eshitish, idrok qilish va mantiqiy xulosalar chiqarish);

bahs va munozaralar (loyihalar yechimi bo‘yicha dalillar va asosli argumentlarni taqdim qilish, eshitish va muammolar yechimini topish qobiliyatini rivojlantirish).

II-BO‘LIM

MODULNI O‘QITISHDA FOYDALANILADIGAN INTERFAOL TA’LIM METODLARI

II. MODULNI O‘QITISHDA FOYDALANILADIGAN INTERFAOL TA’LIM METODLARI

“Blum kubigi” metodi

Metodning maqsadi: Mazkur metod tinglovchilarda yangi axborotlar tizimini qabul qilish va bilimlarni o‘zlashtirilishini yengillashtirish maqsadida qo‘llaniladi, shuningdek, bu metod tinglovchilar uchun “Ochiq” savollar tuzish va ularga javob topish mashqi vazifasini belgilaydi.

Metodni amalga oshirish tartibi:

1. Ushbu metodni ko‘llash uchun, oddiy kub kerak bo‘ladi. Kubning har bir tomonida ko‘yidagi so‘zlar yoziladi:
   - **Sanab bering, ta’rif bering (oddiy savol)**
   - **Nima uchun (sabab-oqibatni aniqlashtiruvchi savol)**
   - **Tushintirib bering (muammoni har tomonlama qarash savoli)**
   - **Taklif bering (amaliyot bilan bog‘liq savol)**
   - **Misol keltiring (ijodkorlikni rivojlantirovchi savol)**
   - **Fikr bering (tahlil kilish va baxolash savoli)**

2. O‘qituvchi mavzuni belgilab beradi.

3. O‘qituvchi kubikni stolga tashlaydi. Qaysi so‘z chiqsa, unga tegishli savolni beradi.

“KWHL” metodi

Metodning maqsadi: Mazkur metod tinglovchilarda yangi axborotlar tizimini qabul qilish va bilimlarni tizimlashtirish maqsadida qo‘llaniladi, shuningdek, bu metod tinglovchilar uchun mavzu bo‘yicha quyidagi jadvalda berilgan savollarga javob topish mashqi vazifasini belgilaydi.

Izoh. *KWHL:*
Know – nimalarni bilaman?
Want – nimani bilishni xohlayman?
How - qanday bilib olsam bo‘ladi?
Learn - nimani o‘rganib oldim?.

“KWHL” metodi	
1. Nimalarni bilaman: -	***2. Nimalarni bilishni xohlayman, nimalarni bilishim kerak:*** -
3. Qanday qilib bilib va topib olaman: -	***4. Nimalarni bilib oldim:*** -

“5W1H” metodi

Metodning maqsadi: Mazkur metod tinglovchilarda yangi axborotlar tizimini qabul qilish va bilimlarni tizimlashtirish maqsadida qo‘llaniladi, shuningdek, bu metod tinglovchilar uchun mavzu bo‘yicha qo‘yidagi jadvalda berilgan oltita savollarga javob topish mashqi vazifasini belgilaydi.

What?	Nima? (ta’rifi, mazmuni, nima uchun ishlatiladi)	
Where?	Qayerda (joylashgan, qayerdan olish mukin)?	
What kind?	Qanday? (parametrlari, turlari mavjud)	
When?	Qachon? (ishlatiladi)	
Why?	Nima uchun? (ishlatiladi)	
How?	Qanday qilib? (yaratiladi, saqlanadi, to‘ldiriladi, tahrirlash mumkin)	

“SWOT-tahlil” metodi

Metodning maqsadi: mavjud nazariy bilimlar va amaliy tajribalarni tahlil qilish, taqqoslash orqali muammoni hal etish yo‘llarini topishga, bilimlarni mustahkamlash, takrorlash, baholashga, mustaqil, tanqidiy fikrlashni, nostandart tafakkurni shakllantirishga xizmat qiladi.

S – (strength)	• kuchli tomonlari
W – (weakness)	• zaif, kuchsiz tomonlari
O – (opportunity)	• imkoniyatlari
T – (threat)	• xavflari

“VEYER” metodi

Metodning maqsadi: Bu metod murakkab, ko‘ptarmoqli, mumkin qadar, muammoli xarakteridagi mavzularni o‘rganishga qaratilgan. Metodning mohiyati shundan iboratki, bunda mavzuning turli tarmoqlari bo‘yicha bir xil axborot beriladi va ayni paytda, ularning har biri alohida aspektlarda muhokama etiladi. Masalan, muammo ijobiy va salbiy tomonlari, afzallik, fazilat va kamchiliklari, foyda va zararlari bo‘yicha o‘rganiladi. Bu interfaol metod tanqidiy, tahliliy, aniq mantiqiy fikrlashni muvaffaqiyatli rivojlantirishga hamda o‘quvchilarning mustaqil g‘oyalari, fikrlarini yozma va og‘zaki shaklda tizimli bayon etish, himoya qilishga imkoniyat yaratadi. “Veyer” metodidan ma’ruza mashg‘ulotlarida individual va juftliklardagi ish shaklida, amaliy va seminar mashg‘ulotlarida kichik guruhlardagi ish shaklida mavzu yuzasidan bilimlarni mustahkamlash, tahlil qilish va taqqoslash maqsadida foydalanish mumkin.

Metodni amalga oshirish tartibi:

trener-o‘qituvchi ishtirokchilarni 5-6 kishidan iborat kichik guruhlarga ajratadi;

trening maqsadi, shartlari va tartibi bilan ishtirokchilarni tanishtirgach, har bir guruhga umumiy muammoni tahlil qilinishi zarur bo‘lgan qismlari tushirilgan tarqatma materiallarni tarqatadi;

har bir guruh o‘ziga berilgan muammoni atroflicha tahlil qilib, o‘z mulohazalarini tavsiya etilayotgan sxema bo‘yicha tarqatmaga yozma bayon qiladi;

navbatdagi bosqichda barcha guruhlar o‘z taqdimotlarini o‘tkazadilar. Shundan so‘ng, trener tomonidan tahlillar umumlashtiriladi, zaruriy axborotlr bilan to‘ldiriladi va mavzu yakunlanadi.

Muammoli savol					
1-usul		**2-usul**		**3-usul**	
afzalligi	kamchiligi	afzalligi	kamchiligi	afzalligi	kamchiligi
Xulosa:					

Muammoli savol					
1-usul		**2-usul**		**3-usul**	
afzalligi	kamchiligi	afzalligi	kamchiligi	afzalligi	kamchiligi
Xulosa:					

“Keys-stadi” metodi

«Keys-stadi» - inglizcha so‘z bo‘lib, («case» – aniq vaziyat, hodisa, «stady» – o‘rganmoq, tahlil qilmoq) aniq vaziyatlarni o‘rganish, tahlil qilish asosida o‘qitishni amalga oshirishga qaratilgan metod hisoblanadi. Mazkur metod dastlab 1921 yil Garvard universitetida amaliy vaziyatlardan iqtisodiy boshqaruv fanlarini o‘rganishda foydalanish tartibida qo‘llanilgan. Keysda ochiq axborotlardan yoki aniq voqea-hodisadan vaziyat sifatida tahlil uchun foydalanish mumkin.

“Keys metodi” ni amalga oshirish bosqichlari

Ish bosqichlari	Faoliyat shakli va mazmuni
1-bosqich: Keys va uning axborot ta’minoti bilan tanishtirish	✓ yakka tartibdagi audio-vizual ish; ✓ keys bilan tanishish(matnli, audio yoki media shaklda); ✓ axborotni umumlashtirish; ✓ axborot tahlili; ✓ muammolarni aniqlash
2-bosqich: Keysni aniqlashtirish va o‘quv topshirig‘ni belgilash	✓ individual va guruhda ishlash; ✓ muammolarni dolzarblik iyerarxiyasini aniqlash; ✓ asosiy muammoli vaziyatni belgilash
3-bosqich: Keysdagi asosiy muammoni tahlil etish orqali o‘quv topshirig‘ining yechimini izlash, hal etish yo‘llarini ishlab chiqish	✓ individual va guruhda ishlash; ✓ muqobil yechim yo‘llarini ishlab chiqish; ✓ har bir yechimning imkoniyatlari va to‘siqlarni tahlil qilish; ✓ muqobil yechimlarni tanlash
4-bosqich: Keys yechimini yechimini shakllantirish va asoslash, taqdimot.	✓ yakka va guruhda ishlash; ✓ muqobil variantlarni amalda qo‘llash imkoniyatlarini asoslash; ✓ ijodiy-loyiha taqdimotini tayyorlash; ✓ yakuniy xulosa va vaziyat yechimining amaliy aspektlarini yoritish

“Assesment” metodi

Metodning maqsadi: mazkur metod ta’lim oluvchilarning bilim darajasini baholash, nazorat qilish, o‘zlashtirish ko‘rsatkichi va amaliy ko‘nikmalarini tekshirishga yo‘naltirilgan. Mazkur texnika orqali ta’lim oluvchilarning bilish faoliyati turli yo‘nalishlar (test, amaliy ko‘nikmalar, muammoli vaziyatlar mashqi, qiyosiy tahlil, simptomlarni aniqlash) bo‘yicha tashhis qilinadi va baholanadi.

Metodni amalga oshirish tartibi:

“Assesment”lardan ma’ruza mashg‘ulotlarida talabalarning yoki qatnashchilarning mavjud bilim darajasini o‘rganishda, yangi ma’lumotlarni bayon qilishda, seminar, amaliy mashg‘ulotlarda esa mavzu yoki ma’lumotlarni o‘zlashtirish darajasini baholash, shuningdek, o‘z-o‘zini baholash maqsadida individual shaklda foydalanish tavsiya etiladi. Shuningdek, o‘qituvchining ijodiy yondashuvi hamda o‘quv maqsadlaridan kelib chiqib, assesmentga qo‘shimcha topshiriqlarni kiritish mumkin.

Har bir katakdagi to‘g‘ri javob 5 ball yoki 1-5 balgacha baholanishi mumkin.

Test

Muammoli vaziyat

Tushuncha tahlili (simptom)

Amaliy vazifa

“Insert” metodi

Metodni amalga oshirish tartibi:

➢ o‘qituvchi mashg‘ulotga qadar mavzuning asosiy tushunchalari mazmuni yoritilgan matnni tarqatma yoki taqdimot ko‘rinishida tayyorlaydi;

➢ yangi mavzu mohiyatini yorituvchi matn ta’lim oluvchilarga tarqatiladi yoki taqdimot ko‘rinishida namoyish etiladi;

➢ ta’lim oluvchilar individual tarzda matn bilan tanishib chiqib, o‘z shaxsiy qarashlarini maxsus belgilar orqali ifodalaydilar. Matn bilan ishlashda talabalar yoki qatnashchilarga quyidagi maxsus belgilardan foydalanish tavsiya etiladi:

Belgilar	Matn
“V” – tanish ma’lumot.	
“?” – mazkur ma’lumotni tushunmadim, izoh kerak.	
“+” bu ma’lumot men uchun yangilik.	
“– ” bu fikr yoki mazkur ma’lumotga qarshiman?	

Belgilangan vaqt yakunlangach, ta’lim oluvchilar uchun notanish va tushunarsiz bo‘lgan ma’lumotlar o‘qituvchi tomonidan tahlil qilinib, izohlanadi, ularning mohiyati to‘liq yoritiladi. Savollarga javob beriladi va mashg‘ulot yakunlanadi.

III-BO‘LIM

NAZARIY MATERIALLAR

III. NAZARIY MATERIALLAR

1-ma’ruza. Kriptologiyaning ilmiy yo‘nalishlari, kriptografiya va kriptotahlil (2 soat)

Reja:

1.1. Kriptologiyaning ilmiy yo‘nalishlari, kriptografiya va kriptotahlil.

1.2. Klassik shifrlarning kriptotahlili, kriptotahlilning sodda usullari.

1.3. Kriptografik algoritmlar bardoshliligi va hisoblash murakkabligi nazariyasi, kriptografik bardoshlilik tushunchasi.

Tayanch iboralar: *kriptologiyaning ilmiy yo‘nalishlari, kriptografiya va kriptotahlil, klassik shifrlarning kriptotahlili, chastotali tahlil, kriptotahlilning sodda usullari, kriptografik algoritmlar bardoshliligi, hisoblash murakkabligi nazariyasi, kriptografik bardoshlilik tushunchasi, nazariy va amaliy bardoshlilik tushunchasi*

1.1. Kriptologiyaning ilmiy yo‘nalishlari, kriptografiya va kriptotahlil.

Har qanday soha va yo‘nalish haqida to‘liq ma’lumotga ega bo‘lish uchun dastlab shu soha va yo‘nalishning asosiy tushunchalari bilan tanishish lozim. Kriptoanaliz haqida to‘liqroq ma’lumotga ega bo‘lish uchun quyidagi keltirilgan atamalar va ularning ta’riflari muhim ahamiyatga ega.

Algoritm - deganda masalani cheklangan qadamlarda yechish uchun aniq belgilangan qoidalarning tartiblangan chekli to‘plami tushuniladi.

Axborotni buzib ko‘rsatish imkoniyatining oldini olish va ruxsatsiz foydalanishdan muhofaza qilish maqsadida uni almashtirishning matematik usuli *kriptografik algoritm* deb ataladi.

Sonlarning ma’lum to‘plamidagi har bir son bir xil ehtimollik bilan tanlab olinishi mumkin bo‘lgan, ushbu sonlar to‘plamidan tanlab olingan son *tasodifiy son* deb ataladi.

Qandaydir algoritm bo‘yicha olingan, amalda esa tasodifiy sonlar sifatida foydalaniladigan sonlar *psevdotasodifiy sonlar* deb yuritiladi.

Ma’lum bir natijaga erishish maqsadida ikki va undan ko‘p subyekt tomonidan berilgan ketma-ketlikda bajariladigan harakatlar (yo‘riqno-malar, buyruqlar, hisoblashlar, algoritmlar) to‘plami *protokol* deyiladi.

Kriptoalgoritmdan va shifrlash kalitlaridan foydalanishni belgilab beradigan qoidalar to‘plami *kriptografik protokol* deb ataladi.

Shifrlash va/yoki elektron raqamli imzo prinsiplariga asoslangan axborotni muhofaza qilish *kriptografik himoya* usuli deyiladi.

Axborotni muhofaza qilish tizimining bir qismini yoki butun tizimni buzishga bo‘lgan muvaffaqiyatli yoki muvaffaqiyatsiz urinish *hujum* deb ataladi.

Hujumning quyidagi turlari mavjud:

1. *Aktiv (faol) hujum* - tizimga yolg‘on axborot joylashtirish yoki mavjud axborotni o‘zgartirish yo‘li bilan qilinadigan hujum;

2. *Adaptiv hujum* - kriptotizimga qilingan hujum bo‘lib, bunda raqib yoki buzg‘unchining ta’sir ko‘rsatish xarakteri kriptotizim qonuniy foydalanuvchilarining xatti-harakatlari yoki boshqa shartlarga bog‘liq ravishda vaqt davomida o‘zgarishi mumkin. Masalan, raqib kriptotizimga ta’sir ko‘rsatish uchun turli dastlabki ma’lumotlarni tanlashi mumkin;

3. *Kriptotizimga qilinadigan hujum* - raqib yoki buzg‘unchining kriptoanalizning ma’lum usullari asosida va ba’zi taxminlar yordamida muayyan kriptografik tizimning xavfsizlik darajasini pasaytirishga urinishi;

4. *Lug‘at bo‘yicha hujum* - to‘g‘ridan-to‘g‘ri qilinadigan turli ko‘rinishli hujumning biri bo‘lib, bu hujum paytida maxfiy so‘z (parol)lar qayta saralanadi yoki oldindan tuzilgan maxfiy so‘zlar ro‘yxatiga murojaat etiladi;

5. *Qo‘pol kuch yoki to‘liq tanlash hujumi* - mumkin bo‘lgan qiymatlarning barchasini yoki salmoqli miqdorini haqiqiy qiymat topilmaguncha tanlashga asoslangan hujum.

Yolg‘on xabarlar o‘rnatishga, xabarlarni tutib olish va o‘zgartirishga, ma’lumotlar bazasidan foydalanishga, o‘z vakolatini kengaytirishga, yolg‘on ochiq kalitni joylashtirishga, soxta hujjatlar tayyorlashga, imzodan bosh tortishga va shu kabilarga urinayotgan buzg‘unchi *aktiv (faol) buzg‘unchi* hisoblanadi.

Kriptografik bayonnomani izdan chiqarish bo‘yicha harakat qilmaydigan buzg‘unchi *passiv (sust)* buzg‘unchi deyiladi.

Axborotni uzatishda, saqlashda yoki qayta ishlashda raqobatchi oldida muayyan foyda olish yoki unga ziyon yetkazish maqsadida ataylab, axborotni ruxsat etilmagan tarzda o‘zgartirish *axborotni soxtalashtirish* deyiladi.

Dastlabki matnni shifrlangan matndan shifrlash kalitini bilmasdan turib tiklash *deshifrlash* deb ataladi.

Kriptotizimni buzish deganda ma’qul bo‘lgan vaqtda zamonaviy hisoblash vositalaridan foydalanib kriptoanaliz masalalarini hal etish usulini topish tushuniladi.

Yuqorida keltirilgan atamalar kriptototahlilning asosiy tushunchalari bo‘lib, ba’zi keltirib o‘tilmagan atamalarga keyingi bo‘limlarning kerakli joylarida tegishli ta’riflar berib boriladi.

Kriptologiya (grekchada kryptos – “sirli” va logos – “so‘z”) degan ma’noni bildirib, shifrlash va deshifrlash bilan shug‘ullanuvchi fan sohasi hisoblanadi. Kriptologiya fani ikki qismdan iborat - kriptografiya va kriptoanaliz.

Kriptografiya ma’lumotlarni ruxsatsiz o‘qish va o‘zgartirishdan himoyalash bilan shug‘ullanuvchi fan sohasi bo‘lib, uning asosini shifrlash va deshifrlash usullari tashkil etadi.

Kriptonaliz shifrlash usullarining kuchli, zaif tomonlarini baholash va kriptotizimlarni buzish usullarini ishlab chiqish bilan shug‘ullanuvchi fan sohasi bo‘lib, asosiy maqsadi shifrlangan xabarlarning mazmunini kalitsiz oshkor qilish hisoblanadi.

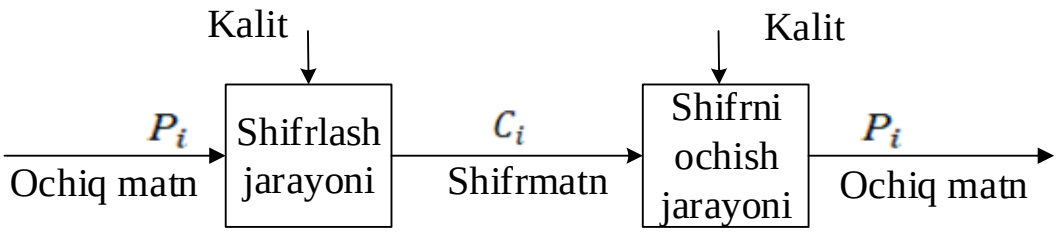
Ochiq matn bu mazmunga ega bo‘lgan dastlabki xabar hisoblanadi, *shifrmatn* esa ochiq matnni kriptografik o‘zgartirishlar orqali mazmuni

o‘zgartirilgan xabar hisoblanadi. Ochiq manni shifrmatnga o‘girish jarayoni *shifrlash*, bu jarayonga teskari amal *shifrni ochish* deyiladi.

Kalit kriptotizimda ma’lumotni shifrlash va shifrni ochish uchun ishlatiladigan vosita hisoblanadi. Kriptotizimlar foydalaniladigan kalit turiga qarab *simmetrik* va *asimmetrik* kabi turlarga bo‘linadi.

Simmetrik kriptotizimlarda ma’lumotni shifrlash va shifrni ochishda bir xil kalitdan foydanaladi. *Asimmetrik* kriptotizimlarda esa ma’lumotni shifrlash va shifrni ochishda turli xil kalitdan foydalaniladi.

Oddiy shifrlash va shifrni ochish jarayonini quyidagi 1.1-rasmda ko‘rsatillganidek tasvirlash mumkin.



1.1-rasm. **Shifrlash va shifrni ochish jarayoni**

Bu yerda P_i - ochiqmatnning birligi, C_i- shifrmatn birligi va shifrlangan matnni ochiq kanal orqali uzatilishini ifodalaydi.

Shifrmatn ochiq kanal orqali uzatilar ekan, uni tutib olish va mazmunini bilishga qaratilgan xavf-hatarlar doim mavjud bo‘ladi. Bunda kriptoanaliz sohasining bilimlaridan foydalaniladi. Shuning uchun quyida kriptoanalizning turlariga to‘xtalib o‘tildi.

1.1-jadval

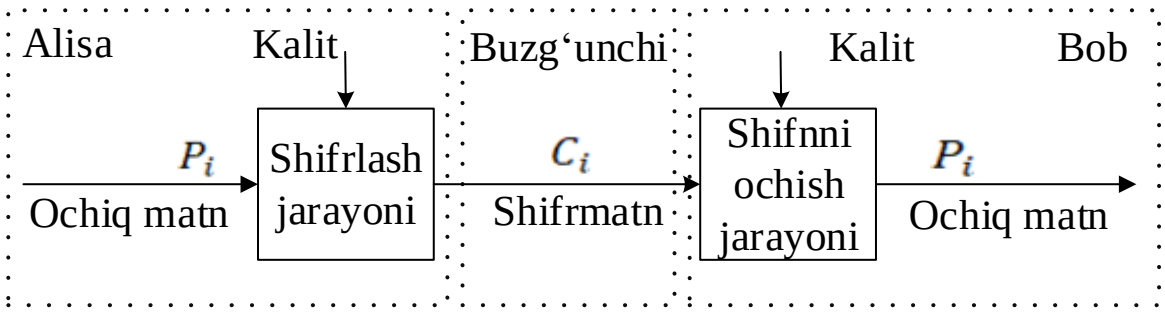
Kriptoanaliz turlari

Kriptoanaliz turi	**Kriptoanalizchiga ma’lum ma’lumotlar**
Faqat shifrmatn bo‘yicha tahlil	• Shifrlash algoritmi • Deshifrlash lozim bo‘lgan shifrmatn
Ma’lum ochiq matn bo‘yicha tahlil	• Shifrlash algoritmi • Deshifrlash lozim bo‘lgan shifrmatn • Bitta maxfiy kalit bilan hosil qilingan ochiq (dastlabki, asl) matn va shifrmatnlar mos qismlarining bir yoki bir nechta juftligi
Tanlab olingan ochiq matn asosidagi tahlil	• Shifrlash algoritmi • Deshifrlash lozim bo‘lgan shifrmatn • Kriptoanalizchi tanlagan ochiq matn va unga mos, maxfiy kalit yordamida yaratilgan shifrmatn
Tanlangan shifrmatn bo‘yicha tahlil	• Shifrlash algoritmi • Deshifrlash lozim bo‘lgan shifrmatn • Kriptoanalizchi tanlagan shifrmatn va unga mos maxfiy kalit yordamida shifri ochilgan ochiq matn.
Tanlangan matn bo‘yicha tahlil	• Shifrlash algoritmi

	• Deshifrlash lozim bo‘lgan shifrmatn • Kriptoanalizchi tanlagan ochiq matn va unga mos, maxfiy kalit yordamida yaratilgan shifrmatn • Kriptoanalizchi tanlagan shifrmatn va unga mos maxfiy kalit yordamida shifri ochilgan ochiq matn.

Kriptoanaliz bilimlaridan foydalanib kriptografik tizimlarni baholovchi yoki buzuvchi shaxslar kriptoanalizchi deb yuritiladi. Yuqorida keltirilgan kriptoanaliz usullarining deyarli barchasida kriptoanalizchining maqsadi shifrlash kalitini topishga qaratiladi. Biroq amalda kalitni bilmasdan ochiq matnni tiklashga qaratilgan hujum turlari ham mavjud. Agar shifrlash algoritmi yuqorida ko‘rsatilgan barcha hujumlarga bardoshli bo‘lmasa u xavfsiz hisoblanmaydi. Shuning uchun shifrlash algoritmining bardoshliligi kriptografik tomondan isbotlangan bo‘lishi kerak. Bundan tashqari kriptografiyada Kerkgoffs prinsipidan foydalaniladi. Unga ko‘ra kriptotizimlarda shifrlash kalitidan boshqa barcha ma’lumotlar foydalanuvchilarga oshkor bo‘lishi kerak. Bu esa kriptoanalizchiga kalitdan boshqa ma’lumotlar(shifrlash algoritmi, ishlatilatilayotgan protokol va hk.)ni bilish imkonini beradi. Bu bir tomondan kriptoanalizchining imkoniyatini oshirsa, ikkinchi tomondan kriptografik algoritmlarning bardoshliligiga yuqori talab qo‘yadi.

Aytaylik Alisa xabarni shifrlaydi va shifrmatnni Bobga yuboradi. Quyidagi 1.2-rasmda Alisa, Bob va Tridi qanday ma’lumotlarga ega bo‘lishi ko‘rsatilgan. Kerkgoffs prinsipiga ko‘ra Tridi shifrmanga va shifrlash algoritmi haqida ma’lumotlarga ega bo‘ladi. Ba’zi hollarda Tridi tanlangan, ma’lum ochiq matn va boshqa ma’lumotlarga ega bo‘lishi mumkin.



1.2-rasm. **Kim nima biladi**

Kriptoanalizchining imkoniyatlarining oshishi kriptografik tizim bardoshliligiga xavf tug‘diradi. Shu nuqtai nazardan kriptografik tizimlarning bardoshliligini ta’minlashda kriptoanalizning o‘rni beqiyos. Shuning uchun keyingi bo‘limda kriptoanalizning zaruriyatiga to‘xtalib o‘tiladi

So‘ngi yillarda kriptologiyaning barcha masalalari bo‘yicha ochiq nashr etilgan ilmiy ishlar soni ortib bormoqda. Bular orasida kriptoanaliz eng faol rivojlanayotgan tadqiqot sohalaridan biri hisoblanadi. Kriptoanalizning rivojlanishi bardoshliligi shubha ostiga olinmagan ko‘plab kriptotizimlarning zaifliklarini ko‘rsatib berdi. Kriptoanalizchi uchun katta qiziqish uyg‘otadigan matematik usullarning katta arsenali yaratildi.

1970-yilning boshida faqat simmetrik kriptotizimlar ma’lum bo‘lib, bu soha bo‘yicha ochiq e’lon qilingan ishlar juda kam edi. Unga qiziqishning pastligi qator sabablar bilan belgilanadi.

Birinchidan, tijorat uchun mo‘ljallangan kriptotizimlarga talab sezilarli darajada ko‘p emas edi. Ikkinchidan, asosiy ishlar ko‘lami yopiq ekanligi yangi natija olishni istagan ko‘plab tadqiqotchi olimlarga qiyinchilik tug‘dirar edi. Uchinchidan, kriptoanaliz ilmiy fan sifatida shakllanmagan bo‘lib, matematik tamoyillar bilan birlashmagan tarqoq usullar majmui edi xolos.

1970-yilning oxiriga kelib vaziyat tubdan o‘zgardi. Birinchidan, aloqa tarmoqlarining rivojlanishi va kompyuterlarning kundalik hayotga kirib borishi tufayli axborotni kriptografik muhofaza qilish zaruratini jamiyatning tobora ko‘proq tabaqalari tushuna boshladi. Ikkinchidan, Diffi-Xellman tomonidan 1976-yilda oshkora(ochiq) kalitli kriptografiyaning yaratilishi maxfiylikka bo‘lgan tijorat talablarini qondirish uchun zamin yaratdi. Bu bilan klassik kriptografiyaning kamchiligini belgilovchi asrlar davomida yechilmay kelgan kalitlarni taqsimlash muammosi hal bo‘ldi. Aslida bu yangilik ilmiy hamjamiyatga katta turtki bo‘lib, sifat jihatdan yangi tadqiq etilmagan sohani ochib berdi. Bu soha tez sur’atlar bilan rivojlanib borayotgan hisoblash murakkabligi nazariyasiga oid yangi ilmiy natijalarni ishlab chiqishga zamin yaratdi va buning oqibatida murakkab matematik tamoyillarga asoslangan kriptoanaliz yo‘nalishi ilmiy fan sifatida shakllana boshladi.

Shifrlash algoritmlariga qo‘yiladigan asosiy(birinchi) talabning mohiyati shundaki, aloqa kanali orqali uzatilayotgan axborotning ma’nosini ochish xuddi shu kalit bilan shifrlangan boshqa axborotning ma’nosini ochishga imkon tug‘dirmasligi lozim. Ikkinchi talab shifrlash va deshifrlash vositalarini ishlatuvchi operator yoki maxfiylashtirilgan axborotni shakllantirishga aralashish imkoni bor shaxslar tomonidan yo‘l qo‘yiladigan ba’zi erkinliklarni e’tiborga olish lozim.

Bundan tashqari kriptoanaliz umumiy matematik natijalardan foydalanishga ham (masalan, katta sonlarni tub ko‘paytuvchilarga ajratish RSA-Rivers Shamir Adliman) kriptotizimni ochish uchun, diskret logorifmlash El Gamal tizimini ochish uchun, muayyan kriptoalgoritm uchun olingan xususiy hol bo‘yicha natijalarga ham tayanishi mumkin. Qoida tarzida, kriptoanaliz algoritmlari ehtimollikka asoslanadigan algoritmlar hisoblanadi. Yuqorida keltirilganlarning barchasida kriptoanalizning maqsadi maxfiy kalitni bilmagan holda, shifrmatnni ochish, shifrmatnning aslini tiklash yoki shifrlangan signallarga asliga mos deb qabul qilinadagan boshqa mazmun berib, ularni soxtalashtirishga qaratiladi. Kriptoanalizda odatda maxfiy kalitdan boshqa shifrlashning barcha algoritmi va protokollari ma’lum deb hisoblanadi. Shifrmatnni shu hol uchun yetarli darajada bardoshli qilib hosil qilish ushbu soha bilan shug‘ullanuvchi kriptografning asosiy vazifasidir. Agar kriptograf bularga qo‘shimcha tarzda, raqib tomon kriptoanalizchisiga shifrmatnga tegishli asl matnning o‘zi yoki uning bir necha qismi ma’lum deb sanalgan hol uchun yetarli bardoshlilikka ega bo‘lgan kriptotizim hosil etsa, bunday tizimni ochiq matn asosida tahlilga nisbatan bardoshli tizim deb hisoblash mumkin bo‘ladi.

Ko‘pchilik zamonaviy shifrlash algoritmi yaratuvchilar tizim bardoshliligini tanlangan ochiq matn asosida kriptoanalizga nisbatan bardoshlilik (bunda shifr matni ham ma’lumligi nazarda tutiladi) bilan belgilaydilar. Biroq, asimmetrik kriptotizimlarga qaratilgan hujumlarda kriptoanalizchining asosiy maqsadi, maxfiy(shaxsiy) kalitni bilmagan holda oshkora kalit va himoyalanmagan aloqa kanalidan jo‘natilgan oshkora axborotdan foydalangan holda jo‘natilgan axborotni soxtalashtirib, bu axborotni oshkora kalit egasiga tegishli ekaniga axborot qabul qiluvchini ishontirishga qaratiladi. Bu maqsadga erishish uchun kriptoanalizchi quyidagi ikki yo‘ldan birini tanlashi mumkin:

- xesh-funksiyada (u barcha uchun oshkora) kolliziyani topa olsa;
- faktorlash, diskret logarifm yoki EEChda diskret logorifmlash muammolaridan birini yechishga yetarli vaqt va hisoblash resurslariga ega bo‘lsa.

ERI(Elektron raqamli imzo) va autentifikatsiya muammolarini yechishda kriptograf tizimning xavfsizligini ta’minlashda ochiqmatn va shifrmatnga qo‘shimcha xesh-funksiyaning ham ma’lumligini e’tiborga olishi lozim. Chunki xesh–funksiya kriptotizimning shifrlash va deshifrlashga oid barcha mexanizmlari sifatida kriptoanalizchiga ma’lum hisoblanadi va muhim hujum obyekti sanaladi.

Xesh-funksiya axborotni bir tomonlama o‘zgartirishdir. Uning alohida tomoni shundaki, $y = H(x)$ oson hisoblanadi. Lekin, uning teskarisi $x = H(y)$ ni hisoblash mushkul.

Xesh-funksiyalarning qo‘llanishi shundaki, berilgan matnning shunday zichlashtirilgan obrazi yaratiladiki, uning aslini hisoblab topish asosida tiklashning imkoniyati bo‘lmasin.

1.2. Klassik shifrlarning kriptotahlili, kriptotahlilning sodda usullari

To‘liq tanlash usuli

To‘liq tanlash, ya’ni kalitlarning *barcha mumkin bo‘lgan variantlarini tanlash usuli*, kriptoanalizchining asimmetrik kriptotizim algoritmini, oshkora kalitni bilgan holda barcha mumkin bo‘lgan kalitlarni tanlash va sinab ko‘rishga asoslanadi. Simmetrik kriptotizimlarda ham shifrmatn va ochiq matn asosida to‘liq tanlash usuli qo‘llaniladi. Kriptoanalizchilar ko‘pincha kompyuter yordamida kalitlarni to‘liq tanlash usulidan foydalanib shifrlarni oshkor etadilar. Kriptoanaliz jarayonida milliard dona kalitlarni sekundiga tanlashga to‘g‘ri keladi.

Faraz qilinsin, buzg‘unchi uchun bir yoki bir necha (x, y) juftliklar ma’lum bo‘lsin. Osonlik uchun har qanday juftlik (x, y) uchun $E_k(x) = y$ munosabatni qanoatlantiruvchi yagona k kalit mavjud bo‘lsin. Mumkin bo‘lgan kalitlar to‘plamini tartibga solinadi va K to‘plamdagi kalitlarni ketma-ket ravishda $E_k(x) = y$ tenglik bajarilishiga tekshirib chiqiladi. Agar k, K kalitning bir variantini tekshirish bir amal yordamida hisoblansa, unda kalitlarni to‘liq tanlash uchun $|K|$ amal talab etiladi. Bunda $|K|$ - to‘plamdagi elementlar soni. Shifrlash sxemasida kalit tasodifiy va teng ehtimollik bilan K to‘plamdan tanlangan bo‘lsin. Bunda kalit $1/|K|$ ehtimollik bilan bilan topiladi va to‘liq tanlash usulining ish hajmi 1 ga teng bo‘ladi.

Misol uchun shaxsiy kalit uzunligi *100 bit bo‘lsa, unda barcha shaxsiy kalitlar soni* 2^{100} ga teng, ya’ni kalitlar to‘plami quvvati $|K|=2^{100}$. Shaxsiy kalit

uzunligi *56* bit bo‘lganda, barcha mumkin bo‘lgan shaxsiy kalitlar soni $|K| = 2^{56} \approx 0.5 * 10^{17}$ ga teng. Bunda, agar hisoblash qurilmasi har bitta maxfiy kalitga mos oshkora kalitni hisoblash va uni hech qiyinchiliksiz taqqoslash uchun 10^{-6} sekund vaqt sarflasa, *24* soatda barcha kalitlarni sinab chiqish uchun $5.787*10^5$ ta EHM kerak bo‘ladi.

Shuning uchun ham shaxsiy va shifrlashda foydalaniladigan kalitni topishni murakkablashtirish maqsadida shaxsiy kalitlar uzunligi *128* bitdan katta bo‘lgan uzunlikda generatsiya qilinadi.

Chastotaviy tahlil usuli

Chastotaviy, ya’ni statistik xarakteristikalar usulida simmetrik yoki asimmetrik kriptotizim kriptoanalizchisi shifrmatndagi belgilar, harflar, so‘zlarning takrorlanishlari sonini (chastotalarini) hisoblab, ochiq matn qaysi tilda yozilganini aniqlaydi. So‘ngra esa, shifrmatn shifr belgilari parametrlarini ochiq matn qaysi tilda yozilgan bo‘lsa, shu tilning parametrlari bilan solishtiradi. Masalan, rus tilida *O* harfi chastotasi yuqori, shifrmatnda *П* harfi chastotasi yuqori. Shifrmatndagi *П* harfini *O* harfi bilan almashtiriladi, ya’ni shifrmatn va ochiq matn yozilgan til chastotalarini kamayish tartibida yozib, tartibi to‘g‘ri kelgan belgilar o‘zaro almashtiriladi. Keyin shifrmatn bigramma, trigramma va k-grammalarining takrorlanishlar sonini topib, ochiq matn yozilgan til bigramma, trigramma va k-grammalari bilan mos holda almashtiradi. Bigramma, trigramma, *k*-gramma deganda, matnda ikkita, uchta va *k*-ta belgining ketma-ket kelishi tushuniladi. Masalan, rus tilida *ст, но, ен, то, на* bigrammalari, *сто, ено, нов, тов, ова* trigrammalari ko‘p uchraydi. Quyidagi 2.1-jadvalda rus tili harflarining paydo bo‘lishining nisbiy chastotasi keltirilgan

2.1-jadval

Rus tili harflarining paydo bo‘lishining nisbiy chastotasi

Harf	**Chastota**	**Harf**	**Chastota**	**Harf**	**Chastota**	**Harf**	**Chastota**
о	0.09	о	0.038	о	0.016	о	0.007
е,ё	0.072	л	0.035	ы	0.016	ш	0.006
а	0.062	к	0.028	б	0.014	ю	0.006
и	0.062	м	0.026	ь,ъ	0.014	ц	0.004
н	0.053	д	0.025	г	0.013	щ	0.003
т	0.053	п	0.023	ч	0.012	э	0.003
с	0.045	у	0.021	й	0.01	ф	0.002
р	0.04	я	0.018	х	0.009		

Yuqorida aytib o‘tilgan prinsiplar hozirgi kunda keng tarqalgan parollarni tanlash bo‘yicha dasturlarda qo‘llaniladi. Parollarni tanlash bo‘yicha dastur avvalo ehtimolligi katta bo‘lgan parollarni tanlaydi, ehtimolligi kichik bo‘lgan parollarni keyinga olib qo‘yadi. Bunda parollarni tanlash jarayoni o‘n va yuz martalab kamayadi. Quyidagi 2.2-jadvalda parollarni tanlashda olingan qator natijalar keltirilgan.

2.2-jadval

Parollarni tanlash natijalari

Tanlash murakkabligi	Tanlash vaqti	Protsessor turi
$2{,}08 \cdot 10^{11}$	15 minut	486DX/4-100
$5{,}68 \cdot 10^{10}$	8 soat	Pentium-120

Pollard usuli

Pollard usuli grafik shaklda “o‘rtada uchrashish” usuliga biroz o‘xshashdir. Unda "tasodifiy akslantirish grafida uchrashish" masalasi yechiladi. Bu yerda ham ikkita grafning boshlang‘ich tugunlaridan chiqib toki ildiz tugunidan o‘tuvchi sikl hosil bo‘lguncha qarama-qarshi yo‘nalishda harakati davom ettiriladi. Uchrashish murakkabligi $0{,}5\varphi\left(\frac{p}{8}\right)\#I'$, yakuniy murakkablik $6{,}5\varphi\left(\frac{p}{8}\right)\#I'$ ga teng.

Pollard usuli siklik gruppada diskret logorifm masalasini yechish uchun qisman ekvivalent kalitlarni topishda qo‘llaniladi. Bular bir xil xesh-funksiya beruvchi ikki argumentni topishda ham asqotadi.

Diskret logorifmlash masalasiga tadbiqan bu usul avvalgi "o‘rtada uchrashish" usuliga nisbatan katta xotiradan voz kechish imkonini yaratadi. Ma’lumotlar bazasini sortlash zarurati ham yo‘qoladi. Shu tufayli vaqt bo‘yicha murakkablik $O(log\#M)$ marta kam bo‘lib, murakkablik $O(\varphi\#M)$ qadam, xotira hajmi $O(1)$ blokdan iborat bo‘ladi.

«O‘rtada uchrashish» usuli

Agar kriptoalgoritmning maxfiy kalitlar to‘plami kompozitsiya amaliga nisbatan berk bo‘lsa, ya’ni har qanday ikki kalit $z_i$va z_j uchun shunday kalit z_k topilsinki, har qanday matni ketma-ket z_i va z_j kalitlarida shifrlash natijasi shu matnni $z_k$bilan shifrlangan matnga aynan teng bo‘lsin, ya’ni

$$F(z_j, F(z_i, x)) = F(z_k, x).$$

Unda bu xossadan foydalanib, shifrlash kalitini topish mumkin, ya’ni z_k ni topish uchun ekvivalent juftlik $< z_i, z_j >$ ni topish kifoya. Bu usul *"tug‘ilgan kunlar paradoksi"* ga asoslanadi. Ma’lumki, tug‘ilgan kunlar tekis taqsimlangan deb hisoblansa, 24 kishilik guruhda $r = 0{,}5$ ehtimollik bilan ikki kishining tug‘ilgan kuni bir xil chiqadi.

Umumiy holda bu paradoks quyidagicha ifodalanadi: agar $a \in n$ predmetlar n ta predmet orasidan qaytarilish bilan tanlansa, ikki predmetning bir xil bo‘lish ehtimoli $p = 1 - e^{-a^2/2}$ ga teng.

Faraz qilinsinki, ochiq matn x va uning shifrogrammasi u ma’lum. x uchun tasodifiy tarzda kalitlar to‘plami z_l va shifrogrammalar $w = F(z_l, x)$ to‘plamini saqlovchi ma’lumotlar bazasi (MB) tuziladi va shifrogrammalarni w bo‘yicha tartibga solinadi. MB hajmini $O((p\#\{z\})$ ga teng qilib olinadi.

So‘ngra tasodifan z_{l1} kalitni olib, u shifrmatn ochiladi va natija $v = F(z_{l1}, u)$ ni MB bilan taqqoslanadi. Agar v biror w bilan teng chiqsa, kalit z_{l1} izlangan kalit z_l ga ekvivalent.

Vaqt bo‘yicha usul murakkabligi $O(\varphi\#\{Z\}log\#\{z\}$ ga teng bo‘ladi.

Ko‘paytuvchi $log\#\{z\}$ saralash murakkabligini hisobga oladi.

Zarur xotira $O((r\ \#\{z\}log\#\{z\})$ bit yoki $O((r\ \#\{z\})$ blokdan iborat. Blok uzunligi va kalit uzunligi cheklangan doimiyga farq qiladi deb faraz qilinadi.

Bu usul kalitlar to‘plami yarim gruppa bo‘lgan qism to‘plamni o‘z ichiga olgan bo‘lsa ham qo‘llanilishi mumkin. Bu usulning boshqa qo‘llanilishini to‘plam yarim gruppa bo‘lmagan hol uchun xesh-funksiyalar misolida taqdim etish mumkin.

Masalan, ERIni soxtalashtirish uchun bitta xesh qiymatga ega ikki matn topish lozim. Undan so‘ng imzolangan xabarni boshqa o‘sha xesh qiymatga ega bo‘lgan xabar bilan almashtirib qo‘yish mumkin. Bunday ikki xabarni topishni "o‘zaro uchrashish" usulida amalga oshirilsa, izlash murakkabligi $O((p\ \#\{z\})$ ga teng bo‘ladi.

Bunda $\#\{z\}$ mumkin bo‘lgan xesh qiymatlar soni. Amerikalik matematik D. Shenks tomonidan taklif etilgan bu algoritm ehtimollik algoritmi bo‘lib olingan natijalar ehtimoliy xarakterga ega.

Xesh-funksiyalar uchun kolliziya hujumi

Kriptografiyada xesh-funksiyalar quyidagi masalalarni hal qilish uchun ishlatiladi:

- ma’lumotni uzatishda yoki saqlashda uning to‘liqligini nazorat qilish uchun;

- ma’lumotning manbasini autentifikatsiya qilish uchun.

Ma’lumotni uzatishda yoki saqlashda uning to‘liqligini nazorat qilish uchun har bir ma’lumotning xesh qiymati hisoblanadi va bu qiymat ma’lumot bilan birga saqlanadi yoki uzatiladi. Ma’lumotni qabul qilgan foydalanuvchi ma’lumotning xesh qiymatini hisoblaydi va mavjud bo‘lgan nazorat qiymati bilan solishtiradi. Agar taqqoslashda bu qiymatlar mos kelmasa, ma’lumot o‘zgarganligini bildiradi.

Xesh funksiyalarga qilinadigan asosiy hujum usuli bu kolliziyani hosil qilishdir. Qabul qilingan x va $y \neq x$ matnlar uchun $N(x) \neq H(y)$ bo‘lishi kolliziyaga bardoshlilik xossasidir.

*“Tug‘ilgan kun paradoksi”*ga asoslangan kriptohujum xesh funksiyalarda kolliziyalarni topish uchun ishlatiladigan asosiy kriptohujumlardan biridir. Bu kriptohujumga asosan xesh qiymat berilganda unga mos bo‘lgan ma’lumotni tanlashning murakkabligi $O(2n)$ kattalik bilan, ma’lumot va uning xesh-qiymati berilganda, xesh-qiymati shunga teng bo‘ladigan boshqa ma’lumotni tanlashning murakkabligi $O(2^{n/2})$ kattalik bilan baholanadi. $N(x) = H(y)$ ko‘rinishdagi ikkita ma’lumotni *“o‘rtada uchrashish”* yoki Pollard usulidan foydalanib topish mumkin. Bu hesh funksiyalar uchun kolliziya hujumini ifodalaydi.

O‘rin almashtirish shifrlarining kriptoanalizi

O‘rin almashtirishga asoslangan shifrlash algoritmlari ochiq matnning alohida olingan shifr qiymatlari o‘rinlarini o‘zgartirish natijasida yoki shifr qiymatlarni guruhlab(bloklab) aralashtirish bilan amalga oshiriladi. Shifr belgilarini bloklab aralashtirish kriptografik nuqtai nazardan samarali natijalar beradi. Bloklab shifrlashda ochiq matn N ta simvoldan iborat bloklarga bo‘linib, har bir blokdagi simvollar ma’lum bir qoida(kalit) asosida almashtirilib chiqiladi. O‘rin almashtirish shifrida kalit ikki xil usul bilan qo‘llaniladi.

Kalit $K = k_1k_2k_3 \dots k_N$, ochiq matn $M = m_1m_2m_3 \dots m_N$ bo‘lsin.

1-usul: ochiq matnni shifrlash uchun uning i −simvolini k_i −o‘ringa qo‘yish kerak. Misol: $N = 7$, kalit 5312764 bo‘lsin.

Ochiq matn:“KRIPTOGRAFIYA” 7 tadan qilib bloklarga ajratiladi.

1-blok: KRIPTOG, 2-blok: RAFIYA Kriptogrammalar “IPRGKOT va FIARYA” hosil bo‘ladi.

2-usul: shifrlashda i −o‘riniga ochiq matnning k_i −simvoli qo‘yiladi.

$N = 7$; kalit 5312764 bo‘lsin.

Ochiq matn:“KRIPTOGRAFIYA ” 7 tadan qilib bloklarga ajratiladi.

1-blok: KRIPTOG, 2-blok: RAFIYA Kriptogramma “TIKRGOP” va “YAFRAI” hosil bo‘ladi.

Ixtiyoriy o‘rin almashtirishni $G =< V, E >$ graf ko‘rinishida tasvirlash mumkin, bu yerda V - grafning uchlari, E esa grafning tomonlari. O‘rin almashtirish shifrida Gamilton marshrutidan foydalanish juda qulay.

Ta’rif. Agar berilgan graf undagi barcha uchlardan faqat bir martadan o‘tadigan oddiy siklda bo‘lsa, u holda Gamilton sikli deyiladi.

Teorema. (Yetarlilik sharti) $G =< V, E >$ graf berilgan bo‘lsin. Agar berilgan grafda ixtiyoriy $u \in V$ uchun $\deg(u) \geq \frac{p}{2}$ (bu yerda p – uchlar soni) bo‘lsa, u holda graf Gamilton sikliga ega bo‘ladi.

Umumiy holda K uzunlikdagi bloklar uchun o‘rin almashtirishlar soni $K!$ bo‘ladi. Agar K kichik son bo‘lsa, bu kriptogrammani kalitni to‘liq terib chiqish usuli bilan deshifrlash mumkin, ammo kalitning uzunligi yetarlicha katta bo‘lgan o‘rin almashtirish shifrlari uchun bu katta muammo keltirib chiqaradi. Gamilton marshrutidan foydalanish o‘rin almashtirish kriptogrammalari deshifrlashini yengillashtiradi, chunki barcha kalitlar ichidan Gamilton yo‘li xossasiga ega bo‘lgan kalitlar ishlatiladi. Lekin katta bloklar uchun bu imkoniyat ham sezilarli bo‘lmaydi. Matnda harflarning juft-jufti (diagramma) bilan kelish chastotasini bilish jadvalli o‘rin almashtirish kriptogrammalarini deshifrlash imkoniyatini beradi. Jadvalli o‘rin almashtirish shifri bo‘yicha matnni nxm o‘lchovli jadvalga ustun bo‘yicha joylashtirib, ma’lum bir kalit asosida o‘rni almashtirilib, E kriptogramma hosil qilinadi:

3.1-jadval

Jadvalli o‘rin almashtirish

$e_{1,1}$	$e_{1,2}$	…	$e_{1,t}$	…	$e_{1,f}$	…	$e_{1,m}$
…	…	…	…	…	…	…	…
$e_{i,1}$	$e_{i,2}$	…	$e_{i,t}$	…	$e_{i,f}$	…	$e_{i,m}$
…	…	…	…	…	…	…	…
$e_{j,1}$	$e_{j,2}$	…	$e_{j,t}$	…	$e_{j,f}$	…	$e_{j,m}$
…	…	…	…	…	…	…	…
$e_{n,1}$	$e_{n,2}$	…	$e_{n,t}$	…	$e_{n,f}$	…	$e_{n,m}$

$p(a, c)$ deb ochiq matnda a harfdan keyin c harf kelish ehtimolligi belgilanadi. U holda $i-$ satrdan keyin $j-$ satrning ketma-ket kelish ehtimolligi quyidagicha bo‘ladi:

$$p(i,j) = \prod_{k=1}^{m} p(e_{i,k}, e_{j,k})$$

Bu formula orqali ketma-ket keluvchi barcha satrlar juftligini aniqlash mumkin. Agar ochiq matnda $i-$ satrdan keyin $j-$ satr kelsa, u holda $p(i,j) \geq p(i,k)$ bo‘ladi. Lekin har xil mavzudagi matnlar uchun diagrammalarning uchrash ehtimolligi har xil bo‘ladi. Shuning uchun birorta kriptogrammani deshifrlash uchun avvalambor uning qaysi sohaga tegishli ekanligini bilish katta ahamiyatga ega. Umumiy holda kriptogrammani deshifrlash uchun jadvalning tartibini aniqlab olib, ehtimolligi katta bo‘lgan satrlarni topishning optimal masalasini yechish kerak.

O‘rniga qo‘yish shifrlarining kriptoanalizi

Chastotaviy, ya’ni statistik xarakteristikalar usulida simmetrik yoki asimmetrik kriptotizim kriptoanalizchisi shifrmatndagi belgilar, harflar, so‘zlarning takrorlanishlari soni(chastotalari)ni hisoblab, ochiq matn qaysi tilda yozilganini aniqlaydi. So‘ngra esa, shifrmatn shifr belgilari parametrlarini ochiq matn qaysi tilda yozilgan bo‘lsa, shu tilning parametrlari bilan solishtiradi. Chastotaviy tahlil usulida ta’kidlanganidek, ingliz tilida *th, in, is, er, he, en,* bigrammalari ko‘p uchraydi. Quyidagi jadvalda ingliz tili harflarining paydo bo‘lishining nisbiy chastotasi keltirilgan (40 000 ta so‘z ichida).

Yuqorida aytib o‘tilgan prinsiplar hozirgi kunda keng tarqalgan parollarni tanlash bo‘yicha dasturlarda qo‘llaniladi. Parollarni tanlash bo‘yicha dastur avvalo ehtimolligi katta bo‘lgan parollarni tanlaydi, ehtimolligi kichik bo‘lgan parollarni keyinga olib qo‘yadi.

3.1-jadval

Ingliz tili alifbosining chastotalar jadvali

Harf	**Soni**		**Harf**	**Chastotasi**
E	21912		E	12.02
T	16587		T	9.10
A	14810		A	8.12
O	14003		O	7.68
I	13318		I	7.31
N	12666		N	6.95
S	11450		S	6.28
R	10977		R	6.02
H	10795		H	5.92
D	7874		D	4.32
L	7253		L	3.98
U	5246		U	2.88
C	4943		C	2.71
M	4761		M	2.61
F	4200		F	2.30
Y	3853		Y	2.11
W	3819		W	2.09
G	3693		G	2.03

Harf	Soni		Harf	Chastotasi
P	3316		P	1.82
B	2715		B	1.49
V	2019		V	1.11
K	1257		K	0.69
X	315		X	0.17
Q	205		Q	0.11
J	188		J	0.10
Z	128		Z	0.07

1. Shifrmatn quyidagiga teng bo‘lsin:

GBSXUCGSZQGKGSQPKQKGLSKASPCGBGBKGUKGCEUKUZKGGBSQE
ICACGKGCEUERWKLKUPKQQGCIICUAEUVSHQKGCEUPCGBCGQOEVS
HUNSUGKUZCGQSNLSHEHIEEDCUOGEPKHZGBSNKCUGSUKUASERLS
KASCUGBSLKACRCACUZSSZEUSBEXHKRGSHWKLKUSQSKCHQTXKZ
HEUQBKZAENNSUASZFENFCUOCUEKBXGBSWKLKUSQSKNFKQQKZE
HGEGBSXUCGSZQGKGSQKUZBCQAEIISKOXSZSICVSHSZGEGBSQSAH
SGKHMERQGKGSKREHNKIHSLIMGEKHSASUGKNSHCAKUNSQQKOSP
BCISGBCQHSLIMQGKGSZGBKGCGQSSNSZXQSISQQGEAEUGCUXSGBS
SJCQGCUOZCLIENKGCAUSOEGCKGCEUQCGAEUGKCUSZUEGBHSKGE
HBCUGERPKHEHKHNSZKGGKAD.

Berilgan shifrmatndagi belgilarning takrorlanish darajasi esa quyidagiga teng:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
17	20	38	2	35	3	57	23	13	1	52	10	3	13	7	7	30	7	61	1	38	3	3	8	0	19

Mos harflarning ehtimolliklari katta bo‘lganlari almashtirilgandan so‘ng, keng uchraydigan ikkiliklar (*TH*, *EA*, *OF*, *TO*, *IN*, *IT*, *IS*, *BE*, *AS*, *AT*, *SO*, *WE*, *HE*, *BY*, *OR*, *ON*, *DO*, *IF*, *ME*, *MY*, *UP*), uchliklar (*THE*, *EST*, *FOR*, *AND*, *HIS*, *ENT yoki THA*) va ma’nosidan kelib chiqqan holda so‘zlar almashtirilgandan so‘ng quyidagi ochiq matn olinadi:

THE UNITED STATES WAS AT PEACE WITH THAT NATION AND AT THE SOLICITATION OF JAPAN WAS STILL IN CONVERSATION WITH ITS GOVERNMENT AND ITS EMPEROR LOOKING TOWARD THE MAINTENANCE OF PEACE IN THE PACIFIC IN DEED ONE HOUR AFTER JAPANESE AIR SQUADRONS HAD COMMENCED XOMXING IN OAHU THE JAPANEE AMBASSADOR TO THE UNITED STATES AND HIS COLLEAGUE DELIVERED TO THE SECRETARY OF STATE A FORMAL REPLY TO A RECENT AMERICAN MESSAGE WHILE THIS REPLY STATED THAT IT SEEMED USELESS TO CONTINUE THE EXISTING DIPLOMATIC NEGOTIATIONS IT CONTAINED NO THREAT OR HINT OF WAR OR ARMED ATTACK.

Bir martalik bloknot shifrining kriptoanalizi

Bir martalik bloknot (One time pad) yoki Vernam shifri nomi bilan tanilgan kriptotizim bardoshli shifrlash algoritmi hisoblanib, tarixda turli vaqtlarda va joylarda foydalanilgan bo‘lsada, ko‘p hollarda amalga oshirishning imkoniyati mavjud emas. Bir martalik deb atalishiga asosiy sabab, undagi kalitning (bloknotning) bir marta foydalanilishi bo‘lib, shunning uchun uni aksariyat hollarda amalga oshirishning imkoni mavjud bo‘lmaydi.

Ushbu shifrlash algoritmini tushuntirish uchun 8 ta belgidan iborat bo‘lgan alfavit olingan bo‘lsin. Olingan alfavit va unga mos bo‘lgan binar qiymatlar quyidagi jadvalda keltirilgan. Shuni esda saqlash kerakki, alifbo va unga mos bo‘lgan bit qiymatlari barcha uchun ochiq va sir saqlanmaydi (ASCII jadvali kabi).

Belgilar	**P**	**I**	**N**	**1**	**3**	**4**	**8**	**9**
	000	001	010	011	100	101	110	111

Faraz qilinsin, biror qonuniy foydalanuvchi A bir martali bloknotdan foydalangan holda “PIN8893144” matnini shifrlab, o‘z sherigi B tomonga yuborishi talab etilsin. Ushbu ochiq matnni binar qiymatdagi ko‘rinishi esa quyidagicha bo‘ladi:

P	**I**	**N**	**8**	**8**	**9**	**3**	**1**	**4**	**4**
000	001	010	110	110	111	100	011	101	101

Bir martalik bloknot usulida shifrlash uchun ochiq matn uzunligiga teng bo‘lgan tasodifiy tanlangan kalit zarur bo‘ladi. Ochiq matnga kalitni XOR amalida qo‘shish orqali shifrmatn hosil qilinadi (*R – ochiq matn*, *K – kalit* va *S – shifrmatn* deb belgilansa): $C = P \oplus K$. XOR amali ($\oplus$) binar amal hisoblanib, quyida keltirilgan:

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

Yuqoridagi jadvaldan, $x \oplus y \oplus y = x$ tenglik o‘rinliligini bilish qiyin emas va shuning uchun bir martali parolda deshifrlash uchun shifrmatnga kalitni XOR amalida qo‘shishning o‘zi yetarli hisoblanadi: $P = C \oplus K$.

Faraz qilinsin A tomon yuqorida keltirilgan ochiq matn uzunligiga teng bo‘lgan quyidagi kalitga ega bo‘lsin:

$$K = \{000\ 000\ 000\ 101\ 111\ 100\ 000\ 101\ 110\ 000\}$$

Ochiq matn	**P**	**I**	**N**	**8**	**8**	**9**	**3**	**1**	**4**	**4**
	000	011	010	110	110	111	100	001	101	101
Kalit	000	000	000	*101*	*111*	*100*	*000*	*101*	*110*	*000*
Shifr matn	000	011	010	*011*	*001*	*011*	*100*	*100*	*011*	*101*
	P	**I**	**N**	**1**	**I**	**1**	**3**	**3**	**1**	**4**

Ushbu kalit asosida *A* tomon yuqorida shifrmatnni hisoblaydi.

A tomonidan yuborilgan shifrmatn *B* tomonda bir xil kalit mavjudligi sababli osongina quyidagicha deshifrlanadi.

Shifr matn	**P**	**I**	**N**	**1**	**I**	**1**	**3**	**3**	**1**	**4**
	000	011	010	*011*	*001*	*011*	*100*	*100*	*011*	*101*
Kalit	000	000	000	*101*	*111*	*100*	*000*	*101*	*110*	*000*
Ochiq matn	000	011	010	110	110	111	100	001	101	101
	P	**I**	**N**	**8**	**8**	**9**	**3**	**1**	**4**	**4**

Ushbu shifrlash algoritmi uchun quyidagi ikki holatni qarab chiqish muhim. Birinchi holatda, faraz qilinsin *A* tomoning dushmani *M* bor va u *A* tomon shifrlagan xabarni o‘qiy olmaydi, lekin o‘zgartira oladi. Ushbu imkoniyatdan foydalanib uzatilayotgan maxfiy xabarning mazmunini o‘zgartirishi mumkin. Buning uchun *M* tomon uzatilayotgan shifrmatnga o‘zining maxfiy kalitini XOR amali bo‘yicha qo‘shadi va qabul qiluvchi *B* ga uzatadi. Ushbu jarayonni quyidagicha ifodalash mumkin:

Shifr matn	**P**	**I**	**N**	**1**	**I**	**1**	**3**	**3**	**1**	**4**
	000	011	010	*011*	*001*	*011*	*100*	*100*	*011*	*101*
***M* tomonning kaliti**	*111*	*000*	*101*	*111*	*100*	*000*	*101*	*100*	*110*	*000*
***M* tomonidan shifrlangan matn**	111	011	111	100	101	011	001	000	101	101
	9	**1**	**9**	**3**	**4**	**1**	**I**	**P**	**4**	**4**

Agar *M* dushman ushbu shifrmatnni *B* tomonga qayta uzatsa, u holda *B* tomon shifrmatnni deshifrlash orqali quyidagiga ega bo‘ladi:

***M* tomonidan shifrlab yuborilgan matn**	**P**	**I**	**N**	**1**	**I**	**1**	**3**	**3**	**1**	**4**
	000	011	010	*011*	*001*	*011*	*100*	*100*	*011*	*101*
***B* tomonning kaliti**	*111*	*000*	*101*	*111*	*100*	*000*	*101*	*100*	*110*	*000*
O‘zgargan ochiq matn	111	011	111	100	101	011	001	000	101	101
	9	**1**	**9**	**3**	**4**	**1**	**I**	**P**	**4**	**4**

B tomon *M* tomonidan yuborilgan o‘zgartirilgan shifrmatnni deshifrlaydi va “PIN8893144”ga teng bo‘lgan haqiqiy xabar o‘rniga “919341IP44”ga teng bo‘lgan soxta xabarga ega bo‘ladi.

Kafolatga ega emasligi sababli, ushbu keltirilgan misollar bir martali bloknot shifrini *bardoshli* ekanini ko‘rsatadi. Bir martali bloknotda agar kalit tasodifiy tanlansa va bir marta foydalanilgan taqdirda hujumchi shifrmatndan ochiq matn haqida biror axborotga ega bo‘la olmaydi (albatta ma’lumotni uzunligidan tashqari). Ya’ni, berilgan shifrmatn uchun mos “kalit” yordamida shifrmatn uzunligidagi ixtiyoriy “ochiq matnlar”ni generatsiya qilish mumkin va bunda barcha ochiq

matnlar bir xil o‘xshashlikka ega. Shuning uchun shifrmatndan ochiq matn haqida biror foydali axborotni olishning imkoni yo‘q. Kriptografik nutqai nazardan shifrmatnlar o‘zidan ortiq ma’lumotni bera olmaydi.

Buning uchun albatta, bir martali bloknot to‘g‘ri foydalanilgan, undagi kalit tasodifiy tanlangan, bir marta foydalaniladi va faqat A va B tomonlarga ma’lum bo‘lishi talab etiladi.

Bir martali bloknot bardoshlilikni ta’minlar ekan, nima uchun har doim undan foydalanilmaydi? Buning asosiy sababi, har bir ochiq matn uchun uning uzunligiga teng bo‘lgan tasodifiy kalitni (bloknotni) generatsiya qilish va qabul qiluvchiga xavfsiz uzatish muammo tug‘diradi. Agar ochiq matn uzunligidagi kalitni (bloknotni) xavfsiz uzatishning imkoniyati mavjud bo‘lsa, u holda kalitning o‘rniga ochiq matnni uzatish foydali emasmi? Uni shifrlashdan nima ma’no? Bir martali bloknot usulidan tarixda cheklangan uzunlikdagi ma’lumotlarni shifrlash qisman foydalanilgan bo‘lsada, hozirgi kundagi katta hajmli ma’lumotlarni uzatish uchun bir martali bloknotni to‘liq amaliy tomondan qo‘llab bo‘lmaydi.

Bir martali bloknotda kalitlardan faqat bir marta foydalanish zarur hisoblanadi. Buni tushuntirish uchun faraz qilinsin, quyidagi ikki ochiq matn P_1va P_2 bitta kalit K dan foydalanib shifrlangan $C_1 = P_1 \oplus K$ va $C_1 = P_2 \oplus K$ shifrmatnlar mavjud. Kriptografiyada ushbu holatni “xavflilik” deb ataladi va bir martali bloknot xavfli holatda deb tushiniladi, ya’ni foydalanilgan kalit ortiq muammo tug‘dirmaydi:

$$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$$

Mazkur holda shifrmatn haqiqiy ochiq matn haqida ba’zi axborotni oshkor qiladi. Agar bir xil kalitdan foydalanib ko‘p marta shifrlash amalga oshirilsa bu katta xavfga olib kelishi mumkin. Mazkur holatni quyidagi misolda ko‘rib chiqish mumkin. Faraz qilinsin, quyidagi ikkita ochiq matn berilgan (belgilarning binar kodi yuqoridagi jadvaldagi kabi):

$P = LIKE = 100010011000$ va $P = KITE = 011010111000$.

Har ikkala ochiq matn yagona kalit K= 110 011 101 111 bilan shifrlangan va shifrmatnlar quyidagiga teng bo‘lgan:

$\boldsymbol{P_1}$	**L**	**I**	**K**	**E**
	100	010	011	000
$\boldsymbol{K}$	110	011	101	111
$\boldsymbol{C_1}$	010	001	110	111

va

$\boldsymbol{P_2}$	**K**	**I**	**T**	**E**
	011	010	111	000
$\boldsymbol{K}$	110	011	101	111
$\boldsymbol{C_2}$	101	001	010	111

Agar hujumchi kriptoanaliz bilan yaqindan tanish bo‘lsa, ochiq matnlardagi 2 va 4-harflarning bir xilligidan ikkala xabar ham bir xil kalit yordamida shifrlanganligini aniqlay oladi. Sababi, mos o‘rindagi shifrmatn belgilari bir xil. Bundan tashqari, hujumchi taxminiy P_1 ochiq matn oladi va uni to‘g‘riligini P_2 ochiq matn bilan tekshirib ko‘radi. Faraz qilaylik, hujumchi birinchi ochiq matn sifatida $P1 = KILL = 011\ 010\ 100\ 100$ ni olgan bo‘lsin. Bu holda u unga mos bo‘lgan

taxminiy kalitni quyidagicha hisoblaydi:

P_1	011	010	100	100
C_1	010	001	110	111
Taxminiy kalit K	001	011	010	011

Olingan kalit K yordamida esa ikkinchi shifrmatndan ochiq matnni hisoblaydi.

C_2	101	001	010	111
Taxminiy kalit K	001	011	010	111
Taxminiy ochiq matn P_2	100	010	000	100
	L	I	E	L

Hisoblangan kalit K ikkinchi ochiq matn P_2uchun mos bo‘lmagani sababli, hujumchi taxmin qilgan birinchi ochiq matni P_1 ni noto‘g‘riligini biladi. Shu tarzda hujumchi qachonki birinchi ochiq matnni P_1=$LIKE$ tarzida taxmin qilsa, ikkinchi ochiq matnni to‘g‘ri P_2=$KITE$ topa oladi.

Zimmermann telegrami

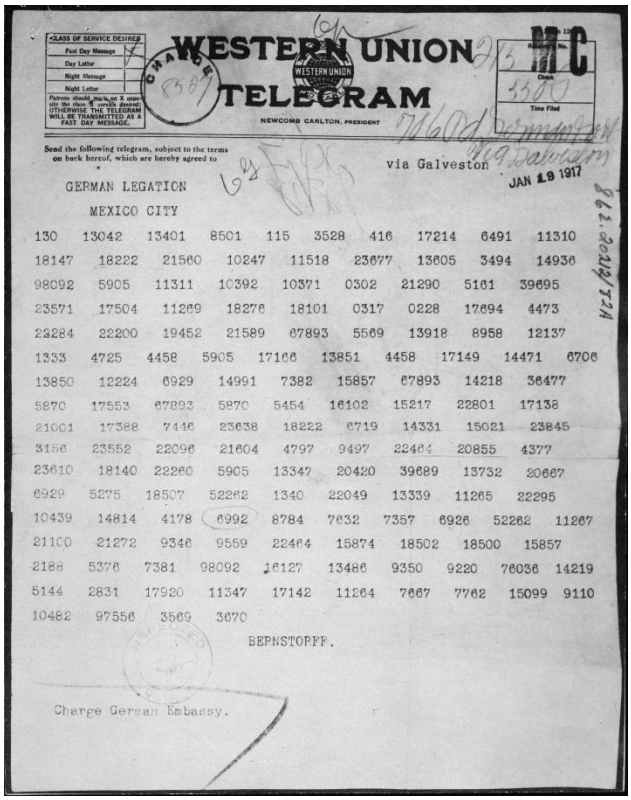
Kodlar kitobi ko‘rinishidagi klassik shifrlash usuli birinchi jahon urushi davrida ommalashgan. Kodlar kitobi lug‘atga o‘xshash kitob bo‘lib, so‘zlardan(ochiq matn so‘zlari) va unga mos bo‘lgan kod so‘zlardan(shifrmatn) tashkil topgan. Shifrlash uchun ushbu kodlar kitobidan zarur bo‘lgan so‘z aniqlanadi, va unga mos bo‘lgan kod so‘z shifrmatn sifatida olinadi. Deshifrlashda esa ushbu jarayonning teskarisi amalga oshiriladi. Ya’ni, kodlar kitobidan shifrmatndagi kod so‘z topiladi va ochiq matn sifatida unga mos bo‘lgan so‘z tanlanadi. Birinchi jahon urushi davrida nemislar tomonidan foydalanilgan kodlar kitobi na’munasi quyidagi jadvalda keltirilgan:

Ochiq Matn	**Shifrmatn**
Februar	13605
Fest	13732
Finanzielle	13850
Folgender	13918
Frieden	17142
Friedenschluss	17149
⋮	⋮

Masalan, *“Februar”* so‘zini shifrlash uchun butun so‘z 5 belgili kod so‘z *13605* bilan almashtirilgan. Yuqorida keltirilgan kodlar kitobi, shifrlash uchun foydalanilgan bo‘lib, deshifrlash uchun kod so‘zlar ustuni bo‘yicha tartiblangan ko‘rinishdagi kod so‘zlar kitobidan foydalanilgan. Kod so‘zlar kitobi o‘rniga qo‘yish akslantirishiga asoslangan bo‘lib, bunda bir belgi emas balki butun so‘z, ba’zida esa butun boshli ibora o‘rniga kod so‘z qo‘yilgan.

Yuqoridagi jadvalda keltirilgan kod so‘zlar mashhur Zimmermann telegramini shifrlash uchun foydalanilgan. 1917-yilda birinchi jahon urishi davrida, Germaniya tashqi ishlar vaziri Artur Zimmermannn Germaniyaning Meksikadagi

elchisiga shifrlangan ko‘rinishdagi telegramma yuboradi. 3.2-rasmda keltirilgan shifrlangan xabar Britaniyaliklar tomonidan tutib olinadi. Bu vaqtda Britaniya va Fransiya Germaniya bilan urushayotgan va AQSh esa betaraf holatda edi.



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

CLASS OF SERVICE DESIRED
Fast Day Message
Day Letter
Night Message
Night Letter

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3070

BEPNSTORFF.

Charge German Embassy.

3.2- -rasm. *Zimmermann telegrami*

Ruslar tomonidan Nemislar kodlar kitobining zarar yetgan versiyasi tiklanadi va Britaniyaga yuboriladi. Murakkab tahlildan so‘ng, Britaniyaliklar Zimmermann telegrami yozilgan vaqtidagi kodlar kitobidagi bo‘shliqlarni to‘ldirishadi va uni deshifrlashadi. Telegramda aytilishicha, Germaniya hukumati cheklanmagan suvosti urushi boshlanishini rejalashtirmoqda va bu AQSh bilan urushga olib kelishi mumkin degan xulosaga kelinadi. Natijada, Zimmermann o‘z elchisiga Meksikani AQShga nisbatan urushda Germaniya ittifoqchisi bo‘lishga undashi kerakligini aytadi. Xususan, Meksika Texas, Yagni Meksika va Arizona shtatlaridagi hududlarini qaytarib olishga undagan. AQShda ushbu telegramma oshkor bo‘lgandan so‘ng, jamoatchilik

We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain, and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace.
Signed, ZIMMERMANN

3.3-rasm. *Deshifrlangan ko‘rinishdagi Zimmermann telegrami*

Germaniyaga qarshi turdi va shundan so‘ng AQSh urushga kiradi. Zimmermann telegramini to‘liq deshifrlangan ko‘rinishi yuqoridagi 3.3-rasmda keltirilgan.

Zimmermann telegrami birinchi jahon urushidagi mashhur shifrlash vositasi bo‘lgan bo‘lsa, ikkinchi jahon urushida xabarlarni shifrlab uzatish uchun Enigma mashinasidan foydalanilgan. Enigma mashinasi ham o‘sha davrda to‘liq kriptoanalizga uchragan bo‘lib bu voqea urushda katta ahamiyat kasb etgan. Keyingi bo‘limda Enigma mashinasining kriptoanaliziga to‘xtalib o‘tiladi.

Enigma mashinasining kriptoanalizi

Enigmaning kriptografik muhim tashkil etuvchisi bu – stiker, uchta rotor va reflektor. Enigma kaliti bu tashkil etuvchilarning dastlabki sozlanishi bo‘lib, ular shifrlash yoki deshifrlash uchun foydalaniladi. Turli sozlanishlarni o‘z ichiga olgan kalit:

1. Rotorlarning tanlanishi;
2. Ikki o‘ng tomondagi rotorlarning har biridagi harakatlanuvchi halqaning holati, bu halqa rotorning tashqi qismiga (26 ta harf bilan belgilangan) halqaning ichki qismi (haqiqiy o‘rin almashtirish asosida bog‘langan) bilan birgalikda aylantirishga ruxsat beradi. Bu halqaning aylantirish natijasida ko‘rsatkich milometr natijasida rotordagi mos harfga siljiydi;
3. Har bir rotorning dastlabki holati;
4. Reflektorni tanlash.

Yuqorida eslatib o‘tilganidek, har bir rotor alfavitdagi 26 ta harfning o‘rin almashishini amalga oshiradi. Harakatlanuvchi halqa esa, belgiga mos holda, 26 ta holatdan biriga o‘rnatilishi mumkin.

Har bir rotor dastlab rotordagi 26 ta holatdan biriga o‘rnatilishi mumkin, bu holatlar A dan Z gacha belgilangan. Stiker eski ko‘rinishdagi telefon kommutatori kabi bo‘lib, 26 ta chuqurchadan iborat va ular harflar bilan belgilangan. Stikerda 0 dan 13 gacha kabel mavjud va har bir kabel bir juft harflarni bir biriga ulaydi. Reflektor 26 ta belgilarni o‘rin almashishini ta’minlaydi, belgi bo‘lmaganlar esa o‘ziga almashtiriladi va natijada qisqa aylanish hosil bo‘ladi. Natijada, reflektor 13 ta kabelga ega stikerga teng bo‘ladi.

Uchta rotor bo‘lganligi uchun va ularning har biri 26 ta harfning almashinishinishidan iborat bo‘lganligi uchun, bu yerda tanlash va mashinada rotorlarni joylashtirish uchun:

$$26! * 26! * 26! \approx 2^{265}$$

ta yo‘l mavjud bo‘ladi. Bundan tashqari, yo‘llar soni ikkita harakatlanuvchi halqalarga o‘rnatiladi va bu ta’sir $26 * 26 \approx 2^{9.4}$ ga teng bo‘ladi.

Har bir rotorning dastlabki holati 26 tadan biriga o‘rnatilishi mumkin va shuning uchun $26 * 26 * 26 \approx 2^{14.1}$ yo‘ldan foydalanib rotorni sozlash mumkin. Bundan tashqari, bu raqam turli dastlabki holatlar bir xil standart holda boshqa rotorlar uchun teng bo‘lganligi uchun bu hisobga teng bo‘lmasligi mumkin. Ya’ni, agar bir har bir rotorni *A* ga o‘natilgan deb faraz qilinsa, u holda, biror rotorni masalan *B* ga sozlanganligi qolgan rotorlarni *A* ga sozlanganligiga ekvivalent. Natijada, oldingi paragrafda keltirilgan faktorlashdan olingan 2^{265} qiymat barcha dastlabki rotor holatlarini o‘z ichiga oladi.

Nihoyat, stiker ko‘rib chiqilsa, stikerdagi p ta kabellarni ulanishlar sonini $F(p)$ deb belgilanadi. Ikkinchi muammodan kelib chiqib, mavjud ulanishlar

$$F(p) = \binom{26}{2p}(2p-1)(2p-3)\ldots\ldots 1$$

$F(p)$ ning barcha qiymatlari 3.2 – jadvalda keltirilgan.

3.2 – jadval

Stikerning kombinatsiyalari soni

$F(0) = 2^0$	$F(1) \approx 2^{8.3}$
$F(2) \approx 2^{15.5}$	$F(3) \approx 2^{21.7}$
$F(4) \approx 2^{27.3}$	$F(5) \approx 2^{32.2}$
$F(6) \approx 2^{36.5}$	$F(7) \approx 2^{40.2}$
$F(8) \approx 2^{43.3}$	$F(9) \approx 2^{45.6}$
$F(10) \approx 2^{47.1}$	$F(11) \approx 2^{47.5}$
$F(12) \approx 2^{46.5}$	$F(13) \approx 2^{42.8}$

Jadvalda keltirilganidek, $2^{48.9}$ dan ortiq stikerning kombinatsiyasi mavjud. Maksimum ko‘rinish 11 ta kabel orqali $F(10) \approx 2^{47.1}$ ga teng bo‘ladi. Yuqorida eslatib o‘tilganidek, Enigmaning reflektori 13 kabelga ega stikerga ekvivalent. Natijada, bu yerda turli $F(13) \approx 2^{42.8}$ reflektor mavjud.

Barcha bu natijalarni kombinatsiyasidan kelib chiqib, Enigmaning kalit maydoni taqriban quyidagiga teng:

$$2^{265} * 2^{9.4} * 2^{48.9} * 2^{42.8} \approx 2^{366}.$$

Ya’ni, nazariy tomondan Enigmaning kalit maydoni 366 bitga teng. Hattoki, zamonaviy shifrlar kamdan – kam hollarda 256 bitdan uzun kalitdan foydalanadi. Bu Nemislar uchun Enigmada buyuk ammo oxir oqibatda asossiz konfidensiallikka ega bo‘lgan ko‘rsatkichdir.

Bundan tashqari, kalitlarning bu astronomik soni adashtiruvchidir. Birinchi muammodan, Nemis harbiylari tomonidan foydalanilgan Enigma mashinasining kalitlarini amaliy tomondan 2^{77} ga tengligini ko‘rish mumkin. Shunday bo‘lsada, bu katta sondir va 1940 yildagi texnologiya orqali kalitlarni to‘liq tanlashni amalga oshirib bo‘lmasdi. Madaniyatli dunyo xalqlari baxtiga esa, bu hol uchun qisqartirilgan tahdidlar mavjud. Ammo, tahdidni tahlil qilishdan oldin, rotorni kriptografik element sifatida qisqacha ko‘rib chiqilsa quyidagi holatlar o‘rinli bo‘ladi.

Rotorlar. 20 asrning birinchi yarmi davomida ko‘plab shifrlash mashinalarida rotorlardan foydalanilgan. Enigma bularning ichida juda ham mashhuri hisoblansada, undan tashqari shifr mashinalar ham mavjud edi. Rotorli shifr mashinasiga boshqa qiziqarli misol sifatida Amerikda II jahon urushida yaratilgan Sigabani olish mumkin. Sigaba shifr mashinasi Enigmaga qaraganda yuqori xavfsizlikni ta’minlaydigan ajoyib loyihaga ega bo‘lgan.

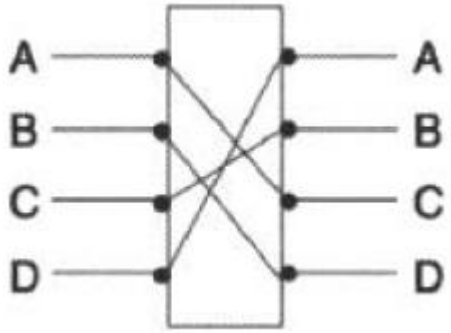
Kriptomuhandislik nuqtai nazaridan, rotorning ajoyibligi sodda elektromexanik qurilmadan bardoshli usulda katta sondagi alohida o‘rin

almashtirishlarni hosil qilishning mumkinligi. Bu qarash kompyuter erasidan oldingi era uchun juda muhim edi. Shunisi aniqki, Enigma haqiqatda qurilmaning mustahkam qismi bo‘lgan va urush holatlarida keng foydalanilgan.

Qurilmaviy rotorlar tushunish oson, ammo turli rotor holatlariga mos o‘rin almashtirishlarni ifodalashda bir oz noqulay.

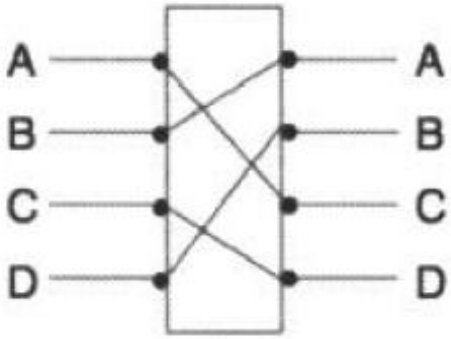
Soddalik uchun, quyida to‘rtta *A* dan *D* gacha harfdan iborat rotorning ishlash prinsipi qarab chiqiladi. Signalni chapdan o‘nga keladi deb faraz qilinsa, 3.4 – rasmda ifodalangan rotor *ABCD* kirishni *CDBA* ga almashtiradi. Ya’ni *A* belgi *C* ga, *B* belgi *D* ga, *C* belgi *B* ga va *D* belgi *A* ga almashtiriladi. Teskari almashtirish, ushbu holatda *DCAB*, chapdan o‘nga rotor o‘rniga o‘ngdan chapga yo‘nalish orqali o‘tadi. Bu xususiyat foydali bo‘lib, bir qurilmada ham shifrlash ham deshifrlash imkonini beradi. Enigma bu qadamni yanada rivojlantirgan. Ya’ni, Enigma mashinasi o‘zining teskarisiga ega, ya’ni, bir turdagi mashina bir xil sozlanish bilan shifrlash yoki deshifrlash uchun foydalanilgan.

Faraz qilinsin, 3.4 - rasmdagi rotor yagona qadamga ega. Etibor berilsa, bu yerda rotorning o‘zi aylantirish uchun to‘rtburchak shaklida ifodalangan, rotor chetlarida elektr kontakrlar yo‘q. Bu misolda, rotor “yuqoriga” harakatlansa, ya’ni, *B* belgi *A* ni o‘rniga va hokazo tartibda, *A* dan *D* gacha aylantiriladi.



3.4 – rasm. Rotor

3.4 – rasmdagi rotorning siljishi 3.5 – rasmda ifodalangan. natijaviy siljitilgan almashtirish *CADB* ga teng, balki, haqiqiy almashtirish *CDBA* ga tengligini ko‘rish qiyindir.



3.5 – rasm. Harakatlangan rotor

Odatda, o‘rin almashinishning rotor siljishini hisoblash murakkab emas. Muhim nuqta shundaki, siljishdagi aralashishni bilish. Masalan, *CDBA* o‘rin almashinishida, aralashish quyidagicha: *A* harfi *C* ga, ya’ni, ikkita qadamda

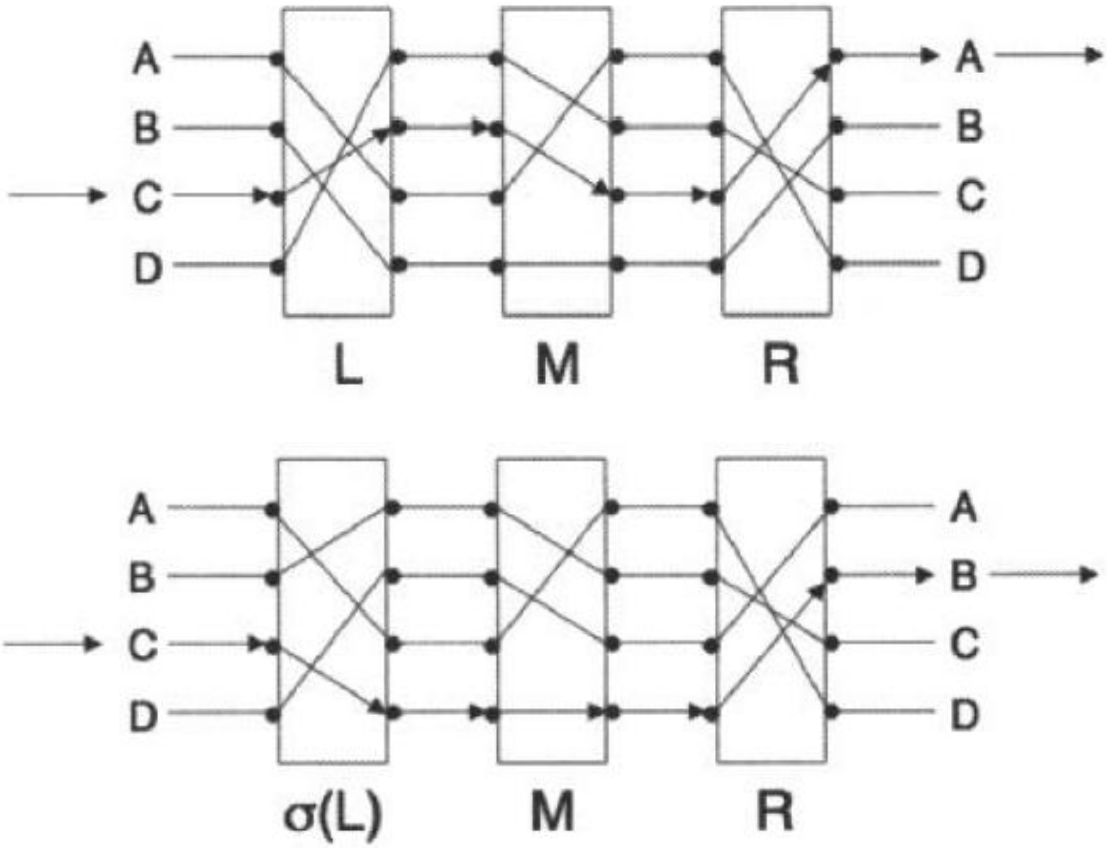
aralashdi, *B* harfi *D* ga almashdi, ya’ni, ikkita qadamda aralashdi, *C* harfi esa *B* almashdi va uchta qadam aralashdi, *D* harfi esa *A* ga almashdi, ya’ni, bitta qadamda. Ya’ni, almashtirishdagi qadamlar (2,2,3,1) ga teng. *CADB* almashtirish uchun esa bu qadamlar (2,3,1,2) ga teng va u 3.5 – rasmda keltirilgan.

Bundan tashqari, fizik rotorlar juda oddiy qurilma, ammo, abstrakt holda ba’zi tushunmovchiliklar mavjud.

Yuqorida eslatib o‘tilganidek, rotorning bir afzalligi shundaki, ular katta sondagi o‘rin almashinishlarni hosil qilish uchun sodda elektromexanik vositalar hisoblanadi. O‘rin almashinishlar sonini orttirish uchun, rotorlar kombinatsiyasi sonini oshirish kerak. Masalan, 3.6 – rasmda, *C* harfi *A* ga almashdi, *L* rotorning siljishi $\sigma(L)$ orqali ifodalanadi va *C* belgini *V* ga almashinishi aks ettirilgan. Ya’ni, bitta rotorning siljishi umumiy almashinish o‘zgarishiga ta’sir qiladi.

Uchta rotordan iborat sxemada, uchta rotor uchun 64 ni o‘rnatish orqali sodda siljitish tomonidan *ABCD* harflarning 64 ta almashinishining siklini hosil qilish mumkin.

3.6 – rasm. Uchta rotor



3.7– rasm. L rotorning qadami

Albatta, barcha almashinishlar bir xil bo‘lmaydi, ya’ni, *ABCD*, to‘rt harf uchun 24 ta almashinish mavjud. Shuningdek, rotorlar uchun turli dastlabki sozlanishlarni tanlash orqali, turli almashtirish ketma ketligini hosil qilish mumkin. Bir rotordagi kabi, bir nechta rotorlar uchun ham ularni teskarisini aniqlash oson, bu rotorlar orqali signalni teskari tartibda yuborish orqali amalga oshiriladi. Bu teskari almashtirishlar jarayoni uchun kerak.

1.3. Kriptografik algoritmlar bardoshliligi va hisoblash murakkabligi nazariyasi, kriptografik bardoshlilik tushunchasi

Kriptobardoshlilik (bardoshlilik) - deb kriptotizimning hujumlarga qarshi tura olish qobiliyatiga aytiladi. Miqdoriy jihatdan kriptobardoshlilik yetarli ehtimollik bilan kriptoanalizchini muvaffaqiyatga eltadigan eng yaxshi kriptoanaliz algoritmining murakkabligi bilan o‘lchanadi.

Kriptoalgoritmlar ular xavfsizligining isbotlana oluvchanlik darajasi bilan farqlanadi.

Kriptografik algoritmlar so‘zsiz bardoshli, isbotlanarli bardoshli va faraz bo‘yicha bardoshli kriptoalgoritmlarga ajratiladi. So‘zsiz bardoshli kriptoalgoritmlarning xavfsizligi kalitni ochish mumkin emasligini isbotlovchi teoremalarga asoslanadi. Masalan, Vernam shifri (bir marta foydalaniladigan kalitli) so‘zsiz bardoshlidir.

Isbotlanarli bardoshli kriptotizimlarning bardoshliligi barcha tomonidan murakkabligi tan olingan va ko‘plab matematiklar yechishga urinib yecha olmagan yaxshi ma’lum matematika masalasi (muammo)ning yechish murakkabligi bilan aniqlanadi. Masalan, Diffi-Xellman yoki Rayvest-Shamir-Adleman (RSA) algoritmlari shu sinfga oid. Bu algoritmlarning bardoshliligi diskret logorifmlash va butun sonni tub ko‘paytuvchilarga ajratish masalalarining murakkabligi bilan belgilanadi.

Faraz bo‘yicha bardoshli kriptoalgoritmlar bir yoki bir necha kishi urinib ko‘rgan va yaxshi o‘rganilgan masalalarga keltirilmaydigan xususiy matematika masalalariga asoslanadi. Lekin, kriptoalgoritmlarda bo‘sh joylar payqalganda ulardan voz kechmay buni hisobga olib yana qo‘shimcha ishlash ko‘p vaqtni olmaydi. Masalan, DES, GOST 28147-89, FEAL, IDEA va boshqalar.

Isbotlanarli bardoshli kriptoalgoritmlarning xavfsizligi ular asosiga olingan masalalarning yaxshi o‘rganilganligidadir. Kamchiligi zarurat tug‘ilganda kriptoalgoritmni tezkor tarzda qayta qurish imkoniyati yo‘qligidadir. Ular "qattiq" tizimlar bo‘lib, ularning bardoshliligini oshirishga matematik masala o‘lchamlarini oshirish yoki almashtirish orqali erishiladi. Bu albatta, shifrlangan apparatdagina emas, balki unga qo‘shni jihozlarda ham o‘zgarishlarni yuzaga keltiradi.

Faraz bo‘yicha bardoshli kriptoalgoritmlar tegishli matematika masalalarining nisbatan kam o‘rganilganligi bilan xarakterlanadi.

Bundan tashqari kalit bardoshliligi, kalitsiz o‘qishga bardoshlilik, imitobardoshlilik (taqlidga bardoshlilik) va yolg‘on axborotni tiqishtirish tushunchalarini farqlash lozim.

Kalit bardoshliligi - bu eng yaxshi ma’lum algoritm bilan kalitni topish murakkabligi bilan o‘lchanadi.

Imitobardoshlilik - bu eng yaxshi ma’lum algoritm yordamida yolg‘on axborotni ro‘kach qilishdir.

Shunga o‘xshash, kriptoalgoritmning o‘z bardoshliligi, protokol bardoshliligi, kalitlar hosil qilish algoritmi va tarqatish bardoshliligi farqlanadi.

Bardoshlilik sathi kriptoanalizchining imkoniyatlariga va foydalanuvchiga bog‘liq.

Kalitlar bardoshliligi sathlari berilgan kriptotizim uchun quyidagi tartibga bo‘ysunadi:

Kalitning matnlar asosida tahlilga nisbatan bardoshliligi B_{tm} asl (ochiq) matn asosida tahlil B_m dan, B_m esa shifrlangan matn asosida tahlildagi kalit bardoshliligi B_{shm} dan oshmaydi

$$B_{tm} \leq B_m \leq B_{shm}.$$

Ayrim hollarda kriptograf hatto raqib tomon kriptoanalizchisi kriptotizimga aralashishi, ya’ni "o‘ziniki" bo‘lishi mumkin deb hisoblagan hol uchun ham bardoshililigi yetarli kriptotizim yarata oladi.

Odatda yaratiladigan kriptoalgoritmlar tanlangan ochiq matnga asoslangan kriptoanalizga nisbatan bardoshli qilib yaratiladi. Bardoshlilik ta’rifida kalitni topishdagi “eng yaxshi” algoritm tushunchasi konstruktiv bo‘lmagani uchun uning talqini subyektivdir. Qaysidir kriptoalgoritmni eng yaxshi algoritm sifatida qarashda kalitni oddiy qarab chiqish orqali topishga nisbatan solishtiriladi.

Foydalanilayotgan birorta kriptoalgoritm uchun kalitni topishning eng yaxshi algoritmi aniqlanmagan, zero bunday eng yaxshi algoritmni topish murakkab masaladir. Shu tufayli amaliyotda bardoshlilikni baholashda ma’lum yoki tadqiqotlar davomida aniqlangan kriptoanaliz algoritmidan foydalaniladi. Shunday qilib, amaliyotda kriptoanalizchiga yangi, samaraliroq tahlil usulini topish tadqiqot yo‘nalishlaridan biri bo‘lib qoladi.

Kalitni topishning yangi samarali usulini yaratish yoki kriptoalgoritmni zaiflashtirishning boshqa usulini yaratish mazkur kriptoalgoritmdan foydalanuvchilarga zarar keltirishi borasida katta imkoniyatlar yaratadi. Bunday tadqiqotlarni e’lon qilish yoki yashirish jamiyatning ochiqlik darajasiga ham bog‘liq. Oddiy foydalanuvchi buzg‘unchining kalitni buzib ochishiga hech qanday qarshilik qila olmaydi.

Ma’lumki, “eng yaxshi” algoritm tushunchasi mutlaq emas. Ertaga kriptoanalizda yangi samarali algoritmini yaratilmasligiga hech kim kafolat bera olmaydi. Bunda kriptoalgoritm iste’moldan chiqadi. Matematika fanining va hisoblash texnikasining taraqqiyoti oshib borgan sari kriptoalgoritmning bardoshliligi kamayib boraveradi. Kriptoalgoritmni o‘z vaqtida almashtirmaslikdan mumkin bo‘lgan zararning oldini olish uchun kriptoalgoritm bardoshliligini davriy tarzda qayta tekshirib borish maqsadga muvofiqdir. Yangidan ishlab chiqilgan kriptoalgoritmning bashorat qilib bo‘lmaydigan kriptobardoshlilik ehtimolini pasaytirish uchun kriptografik tadqiqotlar olib borish zarurdir.

Yuqorida aytilganlardan kelib chiqadiki, kriptotizim bardoshliligi ko‘p qirrali tushunchadir. Bardoshlilik nafaqat ishlab chiquvchidan, balki boshqaruv va aloqa tizimida mazkur kriptoalgoritmdan foydalanish xususiyatlariga, kriptotizimning fizikaviy amalga oshirilishiga hamda matematika va hisoblash texnikasining kelajakdagi yutuqlariga bog‘liq.

Ko‘p tizimlarning bardoshliligi ishonchli sur’atda ko‘plab yaxshi ma’lum masalalarning yechila olmasligiga suyanadi va vaqt o‘tishi bilan ba’zi kriptotizimlarning buzilishi prinsipial mumkin emasligini isbotlashga asoslanadi.

Ammo, kriptografiya masalalarini yaxshi o‘rganilgan matematik masalalarga keltirish orqali isbotlanadigan bardoshlilikka erishish o‘zini oqlanmadi, buning aksi yuz berdi. Xuddi shu kriptografiya masalalarini murakkab matematik masalasiga keltirish ko‘p kriptotizimlarning buzilishiga olib keldi. Hozirgi kunda an’anaviy bir marta foydalaniladigan kalitli algoritmlar(masalan Vernam shifri) so‘zsiz bardoshli shifrlash tizimi bo‘lib qolmoqda.

Ideal tarzda biror ochiq kalitli kriptotizimning bardoshliligini isbotlash uchun bu tizimni ochishning hisobga olishga arziydigan ochish ehtimoliga ega bo‘lgan har qanday algoritmi amalga oshirib bo‘lmaydigan katta hisoblashlar bilan bog‘liqligini isbotlashga keltirilishi kifoya. Ko‘plab ishlab chiqilgan tizimlarga nisbatan ularning bardoshliligi ayrim ahamiyatli va deyarli barcha tomonidan juda murakkab deb tan olingan masalani yechish murakkabligiga ekvivalentligi isbotlangan. Butun sonlarni tub ko‘paytuvchilarga ajratish va diskret logarifmlash masalalari shular jumlasidandir. Shuning uchun ham Diffi Hellman kalitni almashish tizimi, RSA va El Gamal kriptotizimlari bardoshliligi isbotlanadigan kriptotizimlar sinfiga mansubdir. Keyingi o‘n yilliklar davomida kriptografiya va hisoblash murakkabligi nazariyasi sohasida olib borilgan tadqiqotlar zamonaviy kriptoanalizchiga u ishlab chiqqan kriptotizimni bardoshliligini nima pasaytirishi sabablarini chuqurroq tushunishga yordam beradi.

Ko‘pdan beri mavjud bo‘lgan va yaqinda yuzaga kelgan kriptotizimlar uchun kriptoanaliz olib borish juda dolzarb masaladir. Chunki shundagina berilgan kriptotizimning bardoshli emasligi haqida o‘z vaqtida fikr bildirish mumkin bo‘lib, uni yaxshilash yoki boshqasiga almashtirish imkoni tug‘iladi. Bardoshsiz kriptotizimlarni o‘z vaqtida payqash uchun esa har doim ma’lum bo‘lgan kriptoanaliz usullarini mukammallashtirish va yangilarini topish lozim bo‘ladi.

Hisoblash murakkabligi nazariyasi

Murakkablik nazariyasi kriptoanaliz algoritmlarining hisoblash murakkabliklari bilan shug‘ullanadi. Har xil kriptografik tahlillash algoritmlarining hisoblash murakkabliklarini solishtirib, kriptografik algoritmlarning ishonchlilik - bardoshlilik darajasi aniqlanadi.

Algoritmning murakkabligi shu algoritmni to‘la amalga oshirish uchun bajarilishi nazarda tutilgan barcha amallar soni bilan aniqlanadi. Algoritmning hisoblash murakkabligi odatda ikkita parametr algoritmda ko‘rsatilgan amallarni bajarishga sarflanadigan *vaqt bilan aniqlanadigan murakkablik* T va hisoblash qurilmasida algoritm parametrlari ustida amallar bajarishda kerak bo‘ladigan registrlar soni bilan aniqlanadigan *hisoblash qurilmasi xotirasining hajmi bilan bog‘liq bo‘lgan murakkablik* S bilan aniqlanadi.

Bu T va S parametrlar algoritm xususiyatlaridan kelib chiqib boshlang‘ich qiymatlarning n o‘lchamiga bog‘liq holda, ya’ni, $T = f(n)$ va $S = s(n)$ funksiyalar bilan aniqlanadi.

Algoritmning hisoblash murakkabligi “O” belgisi bilan ifodalanadi hamda bu belgi n parametr qiymatining ortishi bilan murakkablik funksiyasi ifodasi ichida qiymati eng tez o‘sadigan hadni ifodalab, boshqa hadlarni hisobga olmaydi. Masalan, algoritmning vaqt bilan aniqlanadigan murakkabligi $T = f(n) = 5n^2 +$

$6n + 11$ bo‘lsa, u holda uning $n^{\,2}$ tartibli hisoblash murakkabligi $O(n^2)$ ko‘rinishda ifodalanadi.

Hisoblash murakkabligi baholari boshlang‘ich qiymatlarni, algoritmning xususiyatlaridan kelib chiqqan holda, algoritmni amalga oshirish uchun sarflanadigan vaqt va hisoblash qurilmasi xotirasiga qo‘yiladigan talablarni yaqqol namoyon etadi. Masalan, $T = O(n)$ bo‘lsa, boshlang‘ich qiymat o‘lchamining ikki marta o‘sishi vaqtning ham ikki marta o‘sishiga olib keladi; agarda $T = O(2^n)$ bo‘lsa, boshlang‘ich qiymat o‘lchamiga bitta bitning qo‘shilishi algoritmni amalga oshirish uchun sarflanadigan vaqtni ikki baravar ortishini bildiradi.

Algoritmlar vaqt va hisoblash murakkabliklariga ko‘ra quyidagi sinflarga ajratiladi:

1. Algoritm *doimiy* deyiladi, agarda uning murakkablik qiymati boshlang‘ich qiymat o‘lchamiga bog‘liq bo‘lmasa, ya’ni $O(1)$.

2. Algoritm *chiziqli* deyiladi, agarda uning murakkabligi qiymatining tartibi $O(n)$ bo‘lsa.

3. Algoritm *polinomial* deyiladi, agarda uning murakkabligi qiymatining tartibi $O(n^m)$ (bu yerda $m > 1$) bo‘lsa.

4. Algoritm *eksponensial* deyiladi, agarda uning murakkabligi qiymatining tartibi $O(t^{f(n)})$ (bu yerda $const = t\ > 1$ va $f(n)$ – boshlang‘ich qiymat o‘lchami n ga nisbatan polinomial funksiya) bo‘lsa.

5. Murakkabligi qiymatining tartibi $O\left(t^{f(n)}\right)$ bo‘lgan *eksponensial* algoritmlar to‘plamiga qism to‘plam bo‘ladigan algoritmlar *superpolinomial* deyiladi, agarda $f(n)$ – polinomial funksiya t o‘zgarmasga nisbatan tezroq, lekin chiziqli funksiyaga nisbatan sekinroq o‘ssa, misol uchun: $O(t^{\sqrt{n}})\ \ , 1 < t < \sqrt{n}$ bo‘lsa.

Shu yerda ta’kidlash joizki, kriptoalgoritmlar natijasiga ko‘ra uning noma’lum parametrlarini topishning mavjud algoritmlari superpolinomial murakkablikka ega bo‘lib, ularning polinomial murakkablikka ega bo‘lgan algoritmlarini topish mumkin emasligi isbot qilinmagan. Ya’ni biror algoritmning noma’lum parametrini polinomial murakkablikka ega bo‘lgan algoritmlarini topish mumkinligi uning kriptobardoshsiz bo‘lib qolganligini bildiradi.

Masalaning (muammoning) murakkabligi. Biror masalani yechish algoritmining murakkabligidan tashqari, masalaning o‘zining murakkabligi tushunchasi ham mavjud. Masalaning murakkabligi nazariyasi yechilishi eng murakkab bo‘lgan masalani *Tyuring mashinasi* deb ataluvchi – *nazariy kompyuterda* yechish uchun sarflanadigan minimal vaqt va xotira hajmini baholashga teng deb olinadi. Tyuring mashinasi – o‘qish va yozish uchun cheksiz xotiraga ega bo‘lgan chekli sondagi amallarni bajaruvchi hisoblash qurilmasidan iborat.

Polinomial murakkablikka ega bo‘lgan algoritmlar bilan yechiladigan masalalarni *yechish mumkin bo‘lgan* masalalar deyiladi, ya’ni bular boshlang‘ich kiritiladigan qiymatlarning biror chekli n-o‘lchamida qoniqarli vaqt birligi ichida yechilishi mumkin polinomial murakkablikka ega bo‘lgan masalalar bo‘lsa. Polinomial vaqt birligi ichida yechilmaydigan masalalarni *qiyin yechiladigan* yoki *qiyin* masalalar deyiladi, ya’ni bu holda boshlang‘ich kiritiladigan qiymatlarning

biror yetarli kichik chekli n-o‘lchamidan boshlab yechish uchun bajarilishi kerak bo‘lgan amallar sonining yetarli darajada tez o‘sib ketishiga olib kelib, bu amallarning barchasini amalga oshirish imkoni bo‘lmasa. Boshlang‘ich kiritiladigan qiymatlarning nisbatan yetarli kichik chekli n o‘lchamida super polinomial murakkablikka ega bo‘lgan algoritmlar bilan yechiladigan masalalarni *hisoblanishi qiyin* bo‘lgan masalalar deyiladi.

Yechish algoritmlari yaratilmagan (yoki qanday yaratilish asoslari zamonaviy ilm-fan yutuqlariga mantiqan ma’lum bo‘lmagan) masalalar – *yechilmaydigan* masalalar deyiladi.

Ikkilik sanoq tizimining so‘zlari deb ataluvchi $\{0;\ 1\}$ belgilaridan iborat barcha:

$$0; 1; 00; 01; 10; 11; 000; 001;\ \dots\ ; 111; \dots; 00 \dots 0; 00 \dots 1; \dots; 11 \dots 1;$$

chekli sondagi 0 va 1 belgilarning ketma-ketliklari bloklaridan (vektorlaridan) tuzilgan to‘plamni Σdeb belgilanadi. Barcha o‘lchami n ga teng bo‘lgan ikkilik sanoq tizimining so‘zlari to‘plamini Σ^n deb belgilanadi. Murakkablik nazariyasida $\Sigma$to‘plamga qism bo‘lgan to‘plamlar $L \in \Sigma$- tillar deyiladi deb qabul qilingan.

Agar Tyuring mashinasi M da u ixtiyoriy chekli n o‘lchamli boshlang‘ich kirish qiymatiga (so‘ziga) bog‘liq bo‘lgan $r(p)$ – ko‘phadning (eng katta) qiymatidan ko‘p bo‘lmagan amallarni bajargandan so‘ng to‘xtasa, u polinomial vaqt birligi ichida ishlaydi (yoki polinomial) deyiladi.

M Tyuring mashinasi L tilni tushunadi (qabul qiladi) deyiladi, agarda u L tilga tegishli bo‘lgan ixtiyoriy kirish so‘zida, ya’ni $\forall x \in L$ bo‘lganda, amallarni bajarib, yana qabul qilish holatida hamda, $\forall x \notin L$ bo‘lganda, amallarni bajarib rad etish holatida to‘xtasa.

Polinomial vaqt birligi ichida ishlaydigan Tyuring mashinasi M qabul qiladigan barcha tillar sinfi R – sinf deb belgilanadi.

Agarda funksiya f uchun polinomial Tyuring mashinasi mavjud bo‘lib, boshlang‘ich qiymat - kirish $x \in \Sigma$ so‘zida amallarni bajarib, to‘xtaganda $f(x)$ qiymatni bersa, u $f: \Sigma \to \Sigma$ polinomial vaqt birligi ichida hisoblanadi deyiladi.

Agarda polinomial vaqt birligi ichida hisoblanadigan $R(x,u)$: $\Sigma \times \Sigma \to \{0,1\}$ – funksiya (predikat) mavjud bo‘lib, boshlang‘ich kirish qiymatlari o‘lchamiga nisbatan aniqlanuvchi murakkablik polinomi $r \in L = \{x|\ \exists y\ P(x,y) \& |y| \leq r(|x|)\}$ bo‘lsa, L til NP to‘liq sinfga tegishli bo‘ladi. Ya’ni, L til NP to‘liq sinfga tegishli bo‘ladi, agarda ixtiyoriy p-o‘lchami $x \in L$ so‘z uchun unga mos $r(|x|) = r(n)$ polinomial uzunlikka ega bo‘lgan y satrni ko‘rsatish mumkin bo‘lib, ko‘rsatilgan satrni to‘g‘ri yoki noto‘g‘riligi $R(x,u)$ predikat orqali aniqlangan. Yuqoridagi fikr va mulohazalardan $R \subseteq NP$ ekanligi kelib chiqadi. Bu tegishlilik munosabati qat’iy, ya’ni: $R \subset NP$ va $P \neq NP$ ekanligi to‘g‘risida hozirgi kunda biror isbot qilingan dalil mavjud emas.

NP to‘liq sinfdan eng katta polinomial murakkablikka ega bo‘lgan tillarning qism sinfi ajratilgan, ya’ni ixtiyoriy $L \in NP$ to‘liq til polinomial vaqt birligi ichida tushunilishi (qabul qilinishi) uchun $P = NP$ bo‘lishi zarur va yetarli.

Yuqorida kiritilgan Tyuring mashinasi tushunchasidan tashqari Tyuringning ehtimollik mashinasi tushunchasi ham mavjud. Bu tushunchalarning farqi

quyidagicha izohlanadi. Tyuring mashinasining keyingi (yangi) holati uning bundan oldingi holati bilan to‘liq aniqlanadi. Tyuring ehtimollik mashinasining keyingi (yangi) holati uning bundan oldingi holati va yana 0 hamda 1 qiymatlarni ½ ehtimollik bilan qabul qiluvchi tasodifiy miqdorning qiymati bilan birgalikda aniqlanadi. Ya’ni, Tyuringning ehtimollik mashinasi uning holatini ifodalovchi qo‘shimcha tasodifiy miqdorning 0 va 1 qiymatlari cheksiz ketma-ketligi satrining holatiga ham bog‘liq.

Tabiiy ravishda savol tug‘iladi: ushbu $P \neq NP$ tengsizlik bardoshli kriptografik tizimlar mavjudligining zaruriy va yetarlilik shartini ifodalaydimi?

Haqiqatan ham bu shartning zaruriyligi bardoshli kriptotizimlar uchun $P \neq NP$ shartining bajarilishiga bevosita ishonch hosil qilish mumkinligidadir. Yuqorida ko‘rilgan misolga qaytgan holda, ushbu

$$L = \{(k_1, d, i) | \exists \text{ma’lumot } t\text{: } d = E_{k_1}(m) \text{ va } m_i = 1\}$$

til aniqlanadi. Ya’ni to‘plam $L \subset \Sigma^n$ biror p-o‘lchamli barcha $m = (m_1, m_2, .. m_i, .. m_n \in \sum_1^n m_i)$ so‘zlardan, i–biti 1 ga teng $m_i = 1$ bo‘lganlari bo‘lib (ularning soni 2^{n-1} ta), ularni k_1 –kalit bilan E - bir tomonlamalik xususiyatiga ega bo‘lgan algoritmdan foydalangan holda shifrlanganda $d = E_{r_1}(m)$ tenglikni qanoatlantiradi. Ushbu $k_1$va d parametrlarni hamda E-algoritmni bilgan holda $d = E_{r_1}(m)$ va $m_i = 1$ tengliklarni qanoatlantiruvchi barcha $m = (m_1, m_2, .. m_i, .. m_n \in L \subset \sum_1^n m_i$ topish eksponensial murakkablikka ega. Bunday aniqlangan til $L \in NP$ bo‘lib, eksponensial vaqt birligi ichida bu tilda shunday t matnlarni ko‘rsatish mumkinki, bu matnlar uchun $d = E_{r_1}(m)$ va uning (m ning) i–biti *1* ga teng, ya’ni $m_i = 1$. Agar shunday bo‘lsa, kirish so‘zi (k_1, d, i) qabul qilinadi, aks holda rad etiladi.

Agarda $P=NP$ deb faraz qilinsa, L tilni tushunuvchi (qabul qiluvchi) polinomial murakkablikka ega bo‘lgan E algoritm mavjud bo‘lib, k_1 va d parametrlarni ma’lum bo‘lib, bu algoritmdan foydalangan holda $d = E_{k_1}(m)$ va m_i *=1* shartlarni qanoatlantiruvchi $m = (m_1, m_2, .. m_i, .. m_n \in L \subset \sum_1^n m_i$ ochiq matnlarni hisoblash mumkin. Bunday xususiyatga ega bo‘lgan algoritmlar kriptobardoshsiz bo‘ladi.

Ushbu $P \neq NP$ tengsizlik o‘rinli bo‘lganda, NP to‘liq masala asosida yaratilgan har qanday algoritm maxfiy parametrlarini aniqlash har doim ham NP to‘liq masala bo‘ladimi, ya’ni eksponensial murakkablikka ega bo‘ladimi? Bunday savolga javoblar asimmetrik kriptografik algoritmlarni tahlil qilish orqali qidirilgan hamda NP to‘liq masala asosida yaratilgan har qanday kriptoalgoritm maxfiy parametrlarini aniqlash har doim ham NP to‘liq masala bo‘lavermasligiga ishonch hosil qilingan. NP to‘liq masala unga faqatgina boshlang‘ich kiritiladigan qiymatlarning biror chekli n o‘lchami biror qiymatdan kichik bo‘lmagandagina qiyin yechiladigan masala bo‘lishi aniqlangan. Bundan kelib chiqadiki, $P \neq NP$ shartning bajarilishi kriptobardoshlilik uchun yetarli emas. Shuning uchun ham kriptobardoshli algoritmlar asosida bir tomonlamalik xususiyatiga ega bo‘lgan akslantirishlar yotadi.

Nazorat savollari:

1. Kriptografiyaning asosiy tushunchalariga ta’rif berish. Bu tushunchalarning bir-biridan farqi nimada?
2. Kriptoanaliz deganda nimani tushunasiz, kriptoanalizchining maqsadi nima?
3. Kriptoanalizning zarurati nimada?
4. Kriptografik algoritmlar bardoshliligi tushunchasi va kriptobardoshlilik deganda nima tushunasiz?
5. Kiriptografik algoritmlarning bardoshliligini baholashdagi hisoblash murakkabligi nazariyasi nimalarga asoslanadi?
6. Qanday kriptotahlil turlarini bilasiz?
7. Klassik kriptoanaliz usullarini sanab bering
8. To‘liq tanlash usuli va uning mohiyatini tushuntirib bering
9. Chastotaviy tahlil usulida ochiq matnni topish nimaga asoslanadi?
10. «O‘rtada uchrashish» hujum usulini tushuntirib bering.
11. Xesh-funksiyalar uchun kolliziya hujumi usuli haqida ma’lumot bering.
12. O‘rin almashtirishga asoslangan shifrlash usullarining kriptoanalizi haqida ma’lumot bering.
13. O‘rniga qo‘yishga asoslangan shifrlash usullarining kriptoanalizi haqida ma’lumot bering.
14. Bir martali bloknot shifri nima va uning kriptoanalizi qanday amalga oshiriladi?
15. Zimmermann telegrami nima?
16. Enigma mashinasi qachon yaratilgan va uning vazifasi nimadan iborat bo‘lgan
17. Enigma mashinasining kriptoanalizi qanday amalga oshirilgan?
18. Enigma mashinasida shifrlangan axbotning kriptobardoshliligi qanday bo‘lgan?

Adabiyotlar va internet resurslar:

1. Xasanov P.F., Xasanov X.P., Axmedova O.P., Davlatov A.B. Kriptotahlil va uning maxsus usullari, O‘quv qo‘llanma, Toshkent, 2010
2. Akbarov D.YE. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanishlari. Toshkent. ”O‘zbekiston markasi“, 2009
3. Л.К.Бабенко, Е.А.Ищукова. Современные алгоритмы блочного шифрования и методы из анализа: учеб. пособие для студентов вузов, обучающихся по группе специальностей в обл. информ. безопасности – М.: Гелиос АРВ, 2006. – 376 с.
4. M.Stamp. Applied cryptanalysis: Breaking Ciphers in the Real World. John Wiley & Sons, Inc, 2007, -P. -417.
5. Б.Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – Москва: ТРИУМФ, 2002.
6. Xasanov P., Xasanov X., Axmedova O., Davlatov A. Kriptotahlil va

uning maxsus usullari. O‘quv qo‘llanma.– Toshkent, 2010.

7. O.P.Axmedova, Z.T.Xudoykulov, O. Allanov, I.M.Boyquziyev Kriptoanaliz. O‘quv qo‘llanma. T.: “Iqtisod-Moliya”, 2022. 171 b.

8. Kuryazov D.M., Sattorov A.B., Axmedova B.B. Blokli simmetrik shifrlash algoritmlari bardoshligini zamonaviy kriptotahlil usullari bilan baholash. O‘quv qo‘llanma. T.: “Aloqachi”. 2017, 228 bet.

9. http://jnicholl.org/Cryptanalysis/Tools/
10. https://www.cryptool.org/en/cto/
11. https://resources.infosecinstitute.com/topic/cryptanalysis-tools/
12. http://rumkin.com/tools/cipher/
13. https://blackarch.org/crypto.html
14. https://www.guballa.de/vigenere-solver
15. https://www.simonsingh.net/The_Black_Chamber/substitutioncrackingtool.html
16. https://www.guru99.com/how-to-make-your-data-safe-using-cryptography.html
17. https://www.cs.bu.edu/~goldbe/teaching/CS558S17/Lab1.pdf

2-ma’ruza. “Simmetrik blokli shifrlar kriptotahlilida statistik usullar (2 soat)

Simmetrik blokli shifrlash algoritmlariga nisbatan chiziqli, differensial va chiziqli-differensial kriptotahlil usullari. Korrelyatsion matritsa va ayirma matritsani hisoblash.

Reja:

2.1. Simmetrik blokli shifrlash algoritmlariga nisbatan chiziqli kriptotahlil usuli
2.2. Simmetrik blokli shifrlash algoritmlariga nisbatan differensial kriptotahlil usuli
2.3. Simmetrik blokli shifrlash algoritmlariga nisbatan chiziqli-differensial kriptotahlil usuli

Tayanch iboralar: *chiziqli krtiptotahlil, korrelyatsion matrisa, chetlanish, fidderensial kriptotahlil, ayirma matritsa, ChDK, DES. Tiny DES*

2.1. Simmetrik blokli shifrlash algoritmlariga nisbatan chiziqli kriptotahlil usuli

Zamonaviy chiziqli kriptoanaliz usuli Yaponiyalik kriptograf M.Matsui tomonidan 1993-yilda DES shifrlash algoritmiga qarshi hujum turi sifatida ishlab chiqilgan.

Ushbu kriptoanaliz usulining mohiyati tanlab olingan ochiq matn *M* va mavjud shifrmatn *C* larning bitlarini *XOR* amali yordamida qo‘shish va natijada kalit bitlarini aniqlashdan iborat:

$$M[i_1, i_2, \dots . i_n) \oplus C[j_1, j_2, \dots . j_n] = K[k_1, k_2, \dots . k_n],$$

bu yerda $M[i_1, i_2, \dots . i_n) = M[i_1) \oplus M[i_2) \oplus \dots . M[i_n)$

$$S[i_1, i_2, \dots . i_n) = S[i_1) \oplus S[i_2) \oplus \dots . S[i_n)$$

$$K[i_1, i_2, \ldots . i_n) = K[i_1) \oplus K[i_2) \oplus \ldots . K[i_n)$$

Natijada yuqoridagi tenglikdan eng yaqin chiziqli approksimatsiyani aniqlash, ya'ni tahlil qilinayotgan algoritm akslantirishlari xossalaridan kelib chiqib, eng samarali chiziqli bog'lanishni tanlashdan iborat. Tanlangan approksimatsiya tenglamalarida tenglikning chap tomonining qiymati *0* yoki *1* ga teng ekanligini aniqlash uchun yetarlicha ko'p miqdordagi ochiq matn va shifr matn juftliklari ustida statistik tahlil olib borish kerak bo'ladi. Natijada, faqat kalit bitlari ishtirok etgan tenglamalar sistemasiga ega bo'linadi. Ushbu tenglamalar sistemasini yechish orqali kalit bitlarini aniqlash mumkin bo'ladi.

Simmetrik blokli shifrlash algoritmlarida chiziqsiz akslantirishlar S-bloklar bo'lib hisoblanadi. Demak S-bloklarini kriptoanaliz qilish asosida algoritmning kriptobardoshliligi xususida xulosa bildirish mumkin. S–bloklarni chiziqli kriptoanaliz qilish uchun chiziqli approksimatsiya tenglamalarini tuzish kerek. Bunda "korrelyatsion matritsa" jadvalidan foydalanish samarali usul hisoblanib, aynan ushbu jadval chiziqli kriptoanalizning asosiy xarakteristikasi hisoblanadi.

Korrelyatsion matritsani tuzish quyidagicha amalga oshiriladi. Masalan, shifrlash algoritmida $Y = \varphi(X): GF(2^n) \to GF(2^m)$ chiziqsiz akslantirish bajarilgan bo'lsin. Ya'ni, $X[x_1, x_2, \ldots . x_n)$ – akslantirishga kiruvchi bitlarni, $Y[y_1, y_2, \ldots . y_n)$–akslantirishdan chiquvchi bitlarni ifodalaydi.

Ta'rif. $Y = \varphi(X)$ - akslantirishga nisbatan korrelyatsion matritsa deb, har bir (*i,j*) - elementi quyidagi tenglik bilan aniqlanuvchi *C* – jadvalga aytiladi:

$$C(\mathrm{i,j}) = \#\{X < X, i >= Y < Y, j >\} \text{ bu yerda}$$
$$i \in 2^n, j \in 2^m,$$
$$< X, i > [x_1 i_1 \oplus x_2 i_2 \oplus, \ldots . x_n i_n),$$
$$< Y, i > [y_1 i_1 \oplus y_2 i_2 \oplus, \ldots . y_n i_n)$$

Ta'rifdan korrelyatsion matritsa akslantirishga kiruvchi va chiquvchi bitlar turli xil pozitsiyalarining o'zaro bog'lanishlarini, ya'ni kiruvchi *i*–bitlarni *XOR* amali yordamida yig'indisining chiquvchi *j*–bitlarni *XOR* amali yordamida yig'indisiga necha marta teng bo'lishini ifodalaydi.

Chiziqli tahlilning maqsadi nochiziqli qismlarni chiziqli tenglamalar bilan taxminiy ifodalashga qaratiladi. Matematiklar uchun chiziqli tenglamalarni yechish oson, agar shunday ehtimolliklar topilsa, bu hujumni shifrmatnga qaratish mumkin. DES algoritmining nochiziqli qismi bu S-bloklardir, shuning uchun chiziqli kriptoanaliz S-bloklar ustida amalga oshiriladi.

Ya'ni, 4.1-jadvaldagi S-blokni ko'rib chiqilsa, uchta kirish bitlarini x_0, x_1, x_2 va ikkita chiqish bitlarini y_0, y_1 kabi belgilab olinadi. Jadvalning satri x_0 qiymatni, ustuni x_1, x_2 qiymatlarini belgilaydi. Ajratilmagan satrdagi belgilar y_0, y_1 chiqish qiymatlarini ifodalaydi. Masalan S-blokga $x_0 x_1 x_2 = 000$ qiymati kiritilganda undan $y_0 y_1 = 10$ ga teng qiymat chiqadi va hakozo.

4.1-jadval

3 bit kirish qiymatini 2 bit chiqishga akslantiruvchi S blok

Satr	**Ustun**			
	00	**01**	**10**	**11**
0	10	01	11	00

1	00	10	01	11

Chiziqli kriptoanalizning asosiy g‘oyasi nochiziqli S-bloklardan chiqish qiymatilarining kirish qiymatlariga bo‘g‘liqligidan kalit qiymatini aniqlash hisoblanadi. Shundan kelib chiqib ushbu kriptoanaliz usulida kirish bitlarining chiqish bitlarini bilan bo‘g‘liqligini ifodalovchi 4.3-jadvaldagi kabi korrelyatsion matrisa tuziladi. Korelyatsion matrisa jadvalini tuzish quyidagicha amalga oshiriladi. Kirish va chiqish bitlarining bog‘liqligi jadvali tuzib olinadi:

Kirish bitlaring barcha kirish qiymatlari $000_2=0_{10}$ dan $111_2=8_{10}$ ga 4.1-jadvaldagi chiqish qiymatlari mosligini quyidagi 4.2-jadvaldagi kabi yozib olinadi.

4.2-jadval

x_0	x_1	x_2	y_0	y_1
0	0	0	1	0
0	0	1	0	1
0	1	0	1	1
0	1	1	0	0
1	0	0	0	0
1	0	1	1	0
1	1	0	0	1
1	1	1	1	1

Kriptoanalizda 0 ga teng kirish va 0 ga teng chiqish qiymatlari kalit bitlarini aniqlashda yordam bermaganligi sababli ularning qiymati olib tashlanadi va quyidagi 4.3-jadvaldagi kabi 7x3 o‘lchamdagi korelatsion matrisa tuziladi. Korelatsion matrisaning jadvali quyidagicha to‘ldiriladi. Masalan jadvalning 2 satr va 2 ustuni kesishmasida joylashgan 6 ga teng qiymat quyidagicha hisoblangan:

$2_{10}=01_2=0^* x_0 \oplus 1^* x_1 = x_1$ qiymatning $2_{10}=01_2=0^* y_0 \oplus 1^* y_1 = y_1$ qiymatga 4.2-jadval asosida 6 marta tengligini ko‘rsatadi;

$7_{10}=111_2=1^* x_0 \oplus 1^* x_1 \oplus 1^* x_2 = x_0 \oplus x_1 \oplus x_2$ qiymatning $7_{10}=111_2=1^* y_0 \oplus 1^* y_1 \oplus 1^* y_2 = y_0 \oplus y_1 \oplus y_2$ qiymatga 4.2-jadval asosida 2 marta tengligini ko‘rsatadi va hakozo.

4.3-jadval

4.1-jadvaldagi S-blokning korrelatsion matritsa jadvali

Krish bitlari	***Chiqish bitlari***		
	y_0	y_1	$y_0 \oplus y_1$
x_0	4	4	4
x_1	4	6	2
x_2	4	4	4
$x_0 \oplus x_1$	4	2	2
$x_0 \oplus x_2$	4	4	4

$x_1 \oplus x_2$	4	6	6
$x_0 \oplus x_1 \oplus x_2$	4	6	2

Yuqoridagi 4.3-jadval natijalari shuni ko‘rsatadiki, masalan, $y_1=x_1$,ya’ni y_1 ning x_1 ga teng bo‘lish imkoniyati 8 ta dan 6 ta holatda bajarilgan. Bu tenglamaning ¾ ehtimollik bilan bajarilishini bildiradi. $x_0 \oplus x_1 \oplus x_2 = y_0 \oplus y_1$ tenglik 4.2-jadvalga asosan 8 ta holatdan 2 ta holatda qanoatlangan. Bu tenglikni bajarilish ehtimolligi ¾ ga teng. Demak bu tenglikning teskarisi bajarilishi ehtimolligi katta. Unga 1 ni XOR amali bilan qo‘shib bemalol 1 qiymatga amashtirish mumkin. 4.3-jadvalda kirish va chiqish bitlarining teng bo‘lish ehtimolligi ko‘rib chiqilgan. Jadvalda “4” ga teng bo‘lmagan qiymatlar tasodifiy bo‘lmagan, ya’ni chiqish bitining tasodifiy almashmaganini bildiradi.

Ushbu ma’lumotlardan foydalanib, S-bloklarni chiziqli funksiyalar bilan almashtirib tahlil qilish mumkin. Natijada nochiziqli S-bloklardan chiziqli tenglamalarni hosil qilib olish, bu yerda chiziqli tenglamalar aniqlilikka asoslangan bo‘lishi shart emas, lekin bu tenglamalarni muhim bo‘lmagan ehtimolliklar bilan bajarish imkoniyati mavjud.

Bu chiziqli ehtimollik tenglamalaridan DES shifrlash bloklariga hujum foydaliroq bo‘lishi uchun bu yodashuvni kengaytirishga harakat qilish kerak. Natijada kalitni topishga qaratilgan chiziqli tenglamalarni yechish imkoniyatiga ega bo‘linadi. Xuddi differensial tahlilda bo‘lgani kabi barcha raundlar uchun “ketma-ketlik zanjiri” kabi bog‘langan tenglamalar sistemasini hosil qilish mumkin.

Chiziqli funksiyalar bilan DES algoritmi S-bloklarining qanchalik yaqin ehtimollik bilan ifodalash mumkin. DES algoritmining har bir S-bloki nochiziqli kombinatsiyalar asosida loyihalashtirilgani uchun kirish bitlari chiqish bitiga yaxshi ehtimollik bilan almashadi. Biroq, kirish bitlarining chiziqli kombinatsiyasi orqali taxmin qilingan chiqish bitlarining chiziqli kombinatsiyasini aniqlash mumkin. Natijada DES algoritmini muaffaqiyatli chiziqli kriptoanaliz qilish mumkin.

Chiziqli kriptoanalizni ko‘rsatish uchun, DES algoritmiga o‘xshash Tiny(sodda) DES algoritmi haqida quyida ma’lumot beriladi. Keyin TDES algoritmining chiziqli va differensial kriptoanalizi keltiriladi.

Tiny DES algoritmi

Tiny DES yoki TDES algoritmi, bu DES algoritmiga nisbatan oson va oddiy kriptoanaliz qilinadigan sodda shifrlash algoritmi. TDES algoritmi chiziqli va differensial kriptoanalizni amalga oshirish uchun yaratilgan sodda shirflash algoritmi. Shunga qaramay bu tahlillarni amalga oshirish uchun DES algoritmiga o‘xshashdir. TDES quyidagilardan tarkib topgan DES algoritmining soddalashtirilgan variantidir:

- blok uzunlidigi 16-bit
- kalit uzunligi 16-bit
- to‘rtta raund
- ikkita S-blok, xar biri 6 bit kirish 4 bit chiqish
- har bir round uchun 12-bitli qism kalit

TDES algoritmida boshlangich va oxirgi o‘rniga qo‘shish amalini bajaruvchi

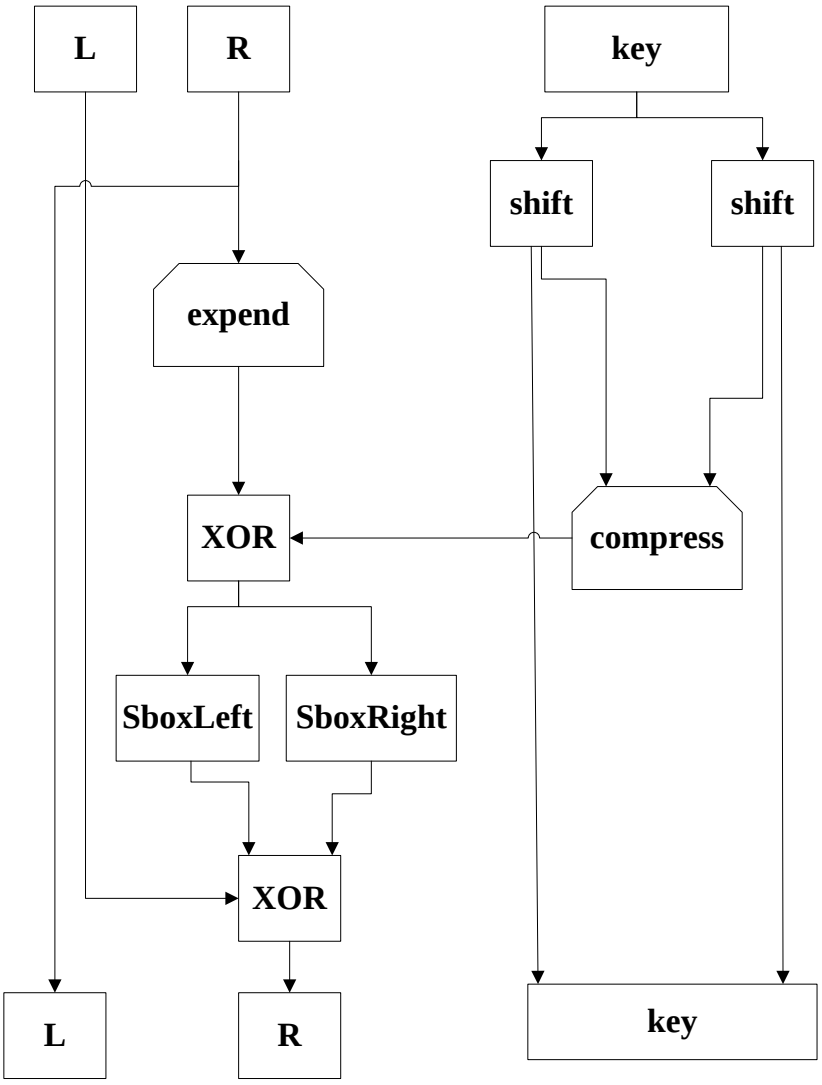
P-blok yo‘q. Asosan, bunda DES algoritmiga tegishli barcha xavfsizlik xususiyatlariga katta ta’sir qilmagan holda, blok va kalit uzunliklari kamaytirilgan.

Kalit va blok uzunligining kichikligi TDES algoritmining xavfsizlikni ta’minlay olmasligini bildiradi va tahlil natijasi qanday bo‘lishidan qat’iy nazar kerakli algoritm bo‘lolmasligini bildiradi. Shunga qaramay, TDES algoritmini chiziqli va differensial tahlilda hamda simmetrik blokli shifrlarning boshqa muammolarini yechishda sodda algoritm sifatida foydalanish mumkin.

TDES algoritmida Feystel tarmog‘iga asosan ochiq matn (L_0, R_0) qismlarga ajratiladi. Keyin to‘rtta $(for\ i = 1,2,3,4)$ raundlar uchun quyidagi almashtirish bajariladi:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

oxirida shifrlangan matn (L_4, R_4) ga teng bo‘linadi. TDES algoritmining bir raundi quyida 4.1-rasmda tasvirlangan. Bu yerda har bir satrda bitlar nomerlarda ko‘rsatilgan.



4.1-rasm. Tiny DES algoritminining bir raundi

TDES algoritmida ikkita S-blok, $SboxLeft(X)$ va $SboxRight(X)$ bor. Har ikkisi ham DES algoritmidagidek 6 bit kirish 4 bit chiqishga ega. TDES algoritmida kriptoanaliz uchun muhim jihat

S-bloklar va ularga kirish qiymatlari hisoblanadi. Tizimni soddalashtirish uchun F funksiya aniqlanadi

$$F(R,K) = Sboxes(expand(R) \oplus K) \quad (4)$$

Bu yerda

$$Sboxes(x_0x_1x_2..x_{11}) = (SboxLeft(x_0x_1..x_5), SboxRight(x_6x_1x_7..x_{11})).$$

Bunda kengaytirish o‘rniga qo‘yish quyidagicha amalga oshiriladi

$$expand(R) = expand(r_0r_1..r_7) = (r_7r_7r_2r_1r_5r_7r_0r_2r_6r_5r_0r_3).$$

Quyida TDES algoritmining chap $SboxLeft(X)$ S-blokini keltirilgan. Bunda S-blok 16 lik sanoq sistemasida ifodalangan:

	$x_1x_2x_3x_4$															
x_0x_5	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	6	9	A	3	4	D	7	8	E	1	2	B	5	D	F	0
1	9	E	B	A	4	5	0	7	8	6	3	2	C	C	1	F
2	8	1	C	2	D	3	E	F	0	9	5	A	4	B	6	7
3	9	0	2	5	A	D	6	E	1	8	B	C	3	4	7	F

Bu yerda o‘ng $SboxRight$ (X), S-bloki quyidagicha:

	$x_1x_2x_3x_4$															
x_0x_5	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	C	5	0	A	E	7	2	8	D	4	3	9	6	F	1	B
1	1	C	9	6	3	E	B	2	F	8	4	5	D	A	0	7
2	F	A	E	6	D	8	2	4	1	7	9	0	3	5	B	C
3	0	A	3	C	8	2	1	E	9	7	F	6	B	5	D	4

DES algoritmida bo‘lgani kabi, TDES algoritmida ham S-bloklar almashtirishlari 16 lik sanoq sistemasida ifodalangan, ya’ni *0,1,2,...,E,F*. TDES algoritminig kalit hosil qilish jarayoni juda oddiy. 16 bitli dastlabki kalit olinadi:

$$K = k_0k_1k_2k_3k_4k_5k_6k_7k_8k_9k_{10}k_{11}k_{12}k_{13}k_{14}k_{15}$$

va yordamchi kalitni quyidagicha hosil qilinadi:

1. Dastlabki kalit o‘rtasidan teng ikkiga LK chap va RK o‘ng qism kalitga ajratiladi

$$LK = k_0k_1k_2k_3k_4k_5k_6k_7$$
$$RK = k_8k_9k_{10}k_{11}k_{12}k_{13}k_{14}k_{15}$$

2. Har bir raund $(i = 1,2,3,4)$ uchun qism kalitlar chap tomonga quyidagicha siklik suriladi

$$LK = rotate\ LK\ (2\ birlik\ chapga\ surish)$$
$$RK = rotate\ RK\ (1\ birlik\ chapga\ surish)$$

3. Hosil bo‘lganlardan (LK, RK) tartibida 16-bitli kalit yasaladi. Yasalgan kalitni 12 bitga siqish uchun uning *0,2,3,4,5, 7,9,10,11,13,14 va 15* tartibidagi bitlaridan yangi qism kalit hosil qilinadi.

K_i raund kalitlari quyidagicha ifodalanishi mumkin:

$$K_1 = k_2k_4k_5k_6k_7k_1k_{10}k_{11}k_{12}k_{14}k_{15}k_8$$
$$K_2 = k_4k_6k_7k_{10}k_1k_3k_{11}k_{12}k_{13}k_{15}k_8k_9$$
$$K_3 = k_6k_0k_1k_2k_3k_5k_{12}k_{13}k_{14}k_8k_9k_{10}$$
$$K_4 = k_0k_2k_3k_4k_5k_7k_{13}k_{14}k_{15}k_9k_{10}k_{11}$$

Keyingi bo‘limda TDES algoritmi chiziqli kriptoanaliz qilinadi. Undan keyin TDES algoritmiga qaratilgan differensial kriptoanaliz ko‘rib chiqiladi. Ushbu ma’lumotlar DES va boshqa blokli shifrlash algoritmlari uchun differensial va chiziqli kriptoanalizni amalga oshirishga taalluqli muhim prinsiplarni aks ettiradi.

TDES algoritmining chiziqli kriptoanalizi

TDES algoritmini chiziqli kriptoanalizi differensial kriptoanaliziga nisbatan soddaroq hisoblanadi. Quyida TDESning algoritmining chiziqli kriptoanalizi chap S-blokiga qaratilgan.

Quyidagi belgilar bilan berilgan:

$$y_0y_1y_2y_3=Sboxleft(x_0\ x_1x_2x_3x_4x_5).$$

TDES algoritmining chap S-blokini chiziqli approksiomatiya tenglamalari

$$y_1= x_2 \text{ va } y_2=x_3 \qquad (4.1)$$

¾ ehtimollik bilan bajariladi. Bunga o‘xshash approsiya tenglamalariga asoslangan chiziqli tahlilni rivojlantirish uchun ushbu usulni barcha roundlarga ketma-ket qo‘llash shart.

	$x_1x_2x_3x_4$															
x_0x_5	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	6	9	A	3	4	D	7	8	E	1	2	B	5	D	F	0
1	9	E	B	A	4	5	0	7	8	6	3	2	C	C	1	F
2	8	1	C	2	D	3	E	F	0	9	5	A	4	B	6	7
3	9	0	2	5	A	D	6	E	1	8	B	C	3	4	7	F

Ochiq matn $P=(L_0,R_0)$dan $R_0=r_0r_1r_2r_3r_4r_5r_6\ r_7$ o‘ng qismi tanlab olinadi. Keyin kengaytirish funksiyasidan quyidagiga ega bo‘linadi:

$$expend(R_0)= expend\ (r_0r_1r_2r_3r_4r_5r_6\ r_7)= r_4r_7r_2r_1r_5r_7r_0\ r_2\ r_6r_5r_0\ r_3. \quad (4.2)$$

4.2-tenglamadagi F funksiyaning ta’rifidan, S-blokga birinchi raunddagi kirish qiymatini $expand(R_0) \oplus K_1$ tenglikdan olish mumkin. Keyin, 4.2-tenglama va K_1 round kaliti ta’rifidan, chap S-blokga birinchi raundda kirish qiymatini quyidagiga tengligini ko‘rish mumkin:

$$r_4r_7r_2r_1r_4r_5\ r_7 \oplus k_2k_4k_5k_6k_7k_1.$$

Demak $y_0y_1y_2y_3$ chap S-blokdan birinchi raundda chiqish qiymatlari deb qaraladi. Keyin yuqoridagi 4.1-tenglama quyidagini nazarda tutadi:

$$y_1= r_2 \oplus k_5 \text{ va } y_2= r_1 \oplus k_6\ , \qquad (4.3)$$

bu yerdagi har bir tenglikning bajarilish ehtimolligi ¾ ga teng. Boshqa so‘z bilan aytganda, chap S-blok uchun, chiqishdagi 1-indeksdagi bit kirishdagi 2-indeksdagi bit hisoblanadi. XOR amali bilan hisoblanganda, chiqish bitining 2-raqami kirish bitining 1-raqamiga teng bo‘lishi ¾ ehtimollik bilan hisoblanadi.

TDES algoritmida (DES algoritmida bo‘lgani kabi) S-blokdan chiqish qiymatlari oldingi qadamdagi chap yarim bloki bilan XOR amali bilan qo‘shiladi. Demak $L_0=l_0l_1l_2l_3l_4l_5l_6l_7$ va $R_1=r'_0r'_1r'_2r'_3r'_4r'_5r'_6r'_7$ bo‘lsin, keyin bu S-blokdan birinchi roundda chiqish qiymatlari $r'_0r'_1r'_2r'_3$ ni chap blok $l_0l_1l_2l_3$ bilan XOR amali orqali qo‘shiladi. Ushbu belgilarni 4.3-tenglama orqali birlashtirib, quyidagiga ega bo‘linadi:

$$r'_1=r_2 \oplus k_5 \oplus l_1 \text{ va } r'_2=r_1 \oplus k_6 \oplus l_2, \qquad (4.4)$$

bu tenglamalarning har biri ¾ ehtimollik bilan bajariladi. Xuddi shunga o‘xshash

natijalar keyingi raundlarda takrorlanadi, bu yerda maxsus kalit bitlari qism kalit K_i ga bog‘liq.

4.4-tenglama natijasida, barcha raundlar uchun 4.3-tenglamadagidek chiziqli approksiya tenglamalarini tuzish mumkin. Ular quyida 4.2-jadvalda tasvirlangan. Chiziqli kiriptotahlil bu ochiq matnni bilish hujumi (known plaintext attack) bo‘lgani uchun, bunda hujumchi ochiq matnni $P = p_0p_1..p_{15}$ va shunga mos shifrmatnni $C=c_0c_1c_2..c_{15}$ biladi. 4.3-jadvalning oxirgi satrida $L_4=c_0c_1c_2c_4c_5c_6c_7$ ekanligi keltirilgan.

Ushbu tenglamalarni quyidagicha qayta yozish mumkin:

$$k_0 \oplus k_1=c_1 \oplus p_{10} \qquad (4.5)$$

va

$$k_7 \oplus k_2=c_2 \oplus p_{9.} \qquad (4.6)$$

Yuqoridagi tenglamalarning har ikkalasi ham $(¾)^3$ ehtimollik bilan bajariladi. c_1, c_2, p_9 va p_{10} ma’lumligidan, k_0, k_1, k_2 va k_7 kalit bitlari haqida ba’zi ma’lumotlarga ega bo‘linadi.

4.3-jadval

TDES algoritmining chiziqli tahlili

$(L_0,R_0) =(p_0…p_7,p_8…p_{15})$	**1 va 2 bitlar (raqamlar 0 dan boshlangan)**	**Bajarilish ehtimolligi**
$L_1=R_0$	p_9,p_{10}	1
$R_1=L_0 \oplus F(R_0 ,K_1)$	$p_9 \oplus p_{10} \oplus k_5$, $p_2 \oplus p_9 \oplus k_6$	¾
$L_2=R_1$	$p_1 \oplus p_{10} \oplus k_5$, $p_2 \oplus p_9 \oplus k_6$	¾
$R_2=L_1 \oplus F(R_1 ,K_2)$	$p_9 \oplus k_6 \oplus k_7$, $p_1 \oplus k_5 \oplus k_0$	$(¾)^2$
$L_3=R_2$	$p_2 \oplus k_6 \oplus k_5$, $p_1 \oplus k_5 \oplus k_0$	$(¾)^2$
$R_3=L_2 \oplus F(R_2 ,K_3)$	$p_{10} \oplus k_0 \oplus k_1$, $p_9 \oplus k_7 \oplus k_2$	$(¾)^3$
$L_4=R_3$	$p_{10} \oplus k_0 \oplus k_1$, $p_9 \oplus k_7 \oplus k_2$	$(¾)^3$
$R_4=L_3 \oplus F(R_3 ,K_4)$		
$C=(L_4,R_4)$	$c_1=p_{10} \oplus k_0 \oplus k_1$, $c_2=p_9 \oplus k_7 \oplus k_2$	$(¾)^3$

4.3-jadval natijalariga asoslangan holda chiziqli hujumni amalga oshirish sodda hisoblanadi. Ma’lum ochiq matn $P =p_0p_1p_2..p_{15}$ va unga mos shifrmat $C=c_0c_1c_2..c_{15}$ berilgan bo‘lsin, har bir juftlik uchun inkrement qiymatini quyidagilarga qarab mos ravishda amalga oshirib, ushbu

$$c_1 \oplus p_{10}=0 \text{ yoki } c_1 \oplus p_{10}=1$$

tenglik yoki quyidagi tenglama bajariladi:

$$c_2 \oplus p_9=0 \text{ yoki } c_2 \oplus p_9=1.$$

Quyida 100 ta tanlab olingan ochiq matnlardan foydalanilganda quyidagi natijalar olingan:

$c_1 \oplus p_{10}=0$ -38 marta bajarildi

$c_1 \oplus p_{10}=1$ -62 marta bajarildi

$c_2 \oplus p_9=0$ -62 marta bajarildi

$c_2 \oplus p_9=1$ -38 marta bajarildi.

Ushbu holatdan, quyidagi xulosaga kelish mumkin. 4.5-tenglamadan kelib chiqib katta 62% li ehtimollikni inobatga olib

$$k_0 \oplus k_1=1$$

va 4.6-tenglama katta 62% li ehtimollik bilan quyidagiga teng:

$$k_7 \oplus k_2 = 0.$$

Ushbu misolda haqiqiy kalit

$$K = 1010\ 0011\ 0101\ 0110,$$

va bundan $k_0 \oplus k_1 = 1$ yoki $k_0 \oplus k_1 = 0$ osonlik bilan aniqlanadi.

Yuqoridagi chiziqli kriptoanalizda kalit ma'lumotining ikki bitini tiklash keltirilgan. Butun K kalitni qayta tiklash uchun qolgan noma'lum bitlarni ham to‘liq aniqlash kerak. Bu taxminan 2^{13} ta shifrlashni bajarish va chiziqli kriptoanalizni amalga oshirishni talab qiladi. Bu hujum juda muhim ahamiyatga ega bo‘lmasa ham samarali hujum hisoblanadi. Shuning uchun qilingan tahlil TDES algoritmining xavfsiz algoritm emasligini ko‘rsatadi.

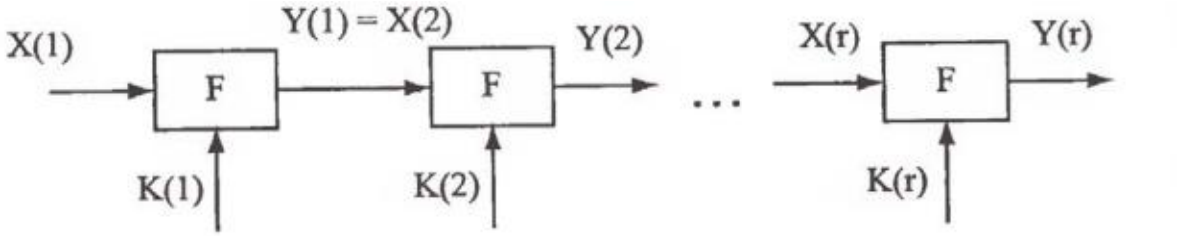
2.2. Simmetrik blokli shifrlash algoritmlariga nisbatan differensial kriptotahlil usuli

Differensial kriptoanaliz (DK) usuli Isroil kriptograflari E.Biham va A.Shamir tomonidan 1990-yilda DES algoritmiga qarshi hujum turi sifatida ishlab chiqilgan. DK usulida shifrlash algoritmi, unga mos tanlab olingan ochiq matn va shifr matn ma'lum deb qaraladi. Mazkur kriptoanaliz usuli 16-raundli DES algoritmini amaliy jihatdan to‘liq ochish imkoniyatini bermasa ham(2^{47} ta matn kerak bo‘ladi), qisqartirilgan raundli masalan, 8-raundli, 6-raundli DES algoritmini muvaffaqiyatli ochish imkonini beradi.

DK usulining mohiyati biror algoritmga kiruvchi X, X' va ularning differensiali ΔX, chiquvchi Y, Y' hamda uning differensiali ΔY qiymatlardan foydalanib kalitni topishdan iborat. Mazkur usulni amaliyotda qo‘llash murakkabligi shundan iboratki, yetarlicha ko‘p miqdordagi ochiq matn va shifr matn juftliklari ustida tahlil olib borish kerak bo‘ladi.

DK usulini ifodalash uchun blok uzunligi N ga teng bo‘lgan shifrator quyidagi 4.2–rasmda ko‘rsatilgan sxemadagidek tasvirlanadi.

4.2-rasm. Blokli shifrlash sxemasi



Bu yerda $K = (K(1), K(2), \dots, K(r))$ kalitlar K_0 kalitdan biror qonuniyat asosida yasalgan yoki xar bir raund uchun alohida tanlangan kalitlar, $X(1)$ va $X'(1)$ ochiq matn juftliklari.

Quyidagi farqlar ko‘rib chiqiladi:

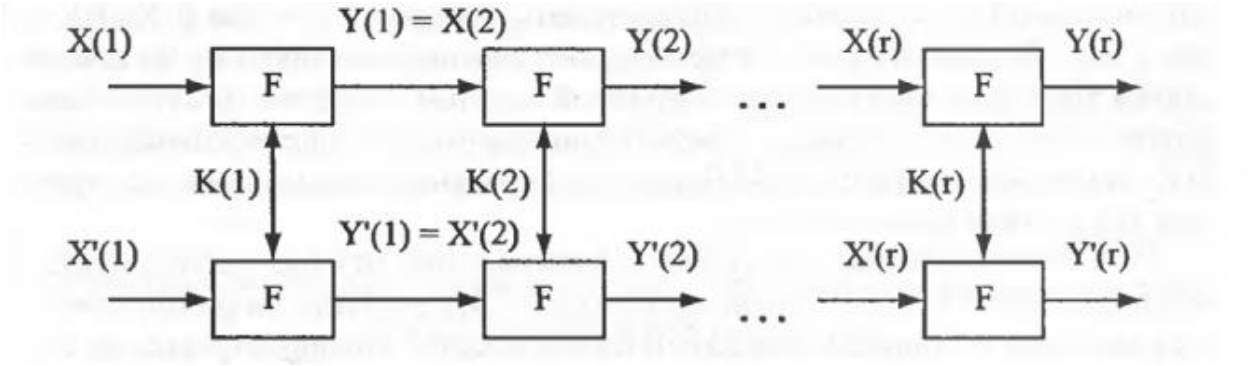
$$\Delta X(1) = X(1) \oplus X'(1);$$
$$\Delta Y(i) = Y(i) \oplus Y'(i).$$

Differensial kriptoanalizning vazifasi, $X(1), K(1), K(2), \dots, K(r-1)$ ma'lumotlarni $1/(2^N)$ ehtimollik bilan tanlash orqali $\Delta Y(r-1)$ shifrmatn farqiga mos ΔX(1) ochiq matnlar farqini topishdan iborat.

(α, β) juftlik $(\Delta X(1), \Delta Y(i))$ vektorlarning $i-$sikldagi differensiali

deyiladi.

Shunda differensial kriptoanalizni quyidagi 4.3–rasmda ko‘rsatilgan modeldek tasvirlash mumkin.



4.3-rasm. Differensial kriptoanaliz modeli

Shifrning oxirgi raund kalitini quyidagi algoritmlar ketma-ketligi asosida topiladi:

1. $P(\Delta X(1)) = \alpha, \Delta Y(r-1) = \beta$ katta ehtimolliklar uchun, $(r-1)$ siklning differensiali (α, β) tanlanadi;
2. $X(1)$ tasodifiy tanlanadi. Ma’lum $Y(r), Y'(r)$ va $\Delta X(1) = \alpha$ tenglik asosida $X'(1)$ tanlanadi;
3. Taxmin qilingan $\Delta Y(r-1) = \beta$ va ma’lum $Y(r), Y'(r)$ lardan foydalanib $K(r)$ topiladi;
4. Ikkinchi va uchinchi qadamlar kalitlar kesishmasi yagona elementni qabul qilmaguncha davom ettiriladi.

Differensial kriptoanalizning g‘oyasi kirish va chiqishdagi ma’lumot bitlaridagi farqlarni taqqoslashga asoslanadi. Buni sodda tushuntirish uchun, avvalo soddalashtirilgan S-blokdan foydalanish maqsadga muofiq. Masalan DES yoki shunga o‘xshash shifrlash algoritmi uchun 3-bit kirish va 2-bitli chiqishdan iborat S-blok ishlatilgan bo‘lsin:

4.4-jadval

3-bit kirish va 2-bitli chiqishdan iborat sodda S-blok

Satr	**Ustun**			
	00	**01**	**10**	**11**
0	10	01	11	00
1	00	10	01	11

$$010 = X_1 \oplus X_2 = Sbox(X_1) \oplus Sbox(X_2) = 01$$

1. $010 = 000 \oplus 010 = 10 \oplus 11 = 01$
2. $010 \oplus 000 = 11 \oplus 10 = 01$
3. $001 \oplus 011 = 01 \oplus 00 = 01$
4. $011 \oplus 001 = 00 \oplus 01 = 01$
5. $100 \oplus 110 = 00 \oplus 01 = 01$
6. $110 \oplus 100 = 01 \oplus 00 = 01$
7. $101 \oplus 111 = 10 \oplus 11 = 01$
8. $111 \oplus 101 = 11 \oplus 10 = 01$

bu yerda, $x_1x_2x_3$ kirish bitlari bo‘lib, bunda x_1 jadvalning satr qismi bo‘lsa, x_2x_3 ustun qismdagi elementlar hisoblanadi. Masalan, *Sbox (010)=11*, chunki satrdagi biti 0 va ustundagi bitlari 10 bo‘lgan umumiy 010 kirish bitining S-blokdan chiqish qiymati 11 ni tashkil qiladi.

Ikkita kirish ma’lumoti ko‘rib chiqilsa, bunda $X_1=110$ va $X_2=010$ va kalitni $K=011$ deb olinsin. Keyin $X_1 \oplus K=101$ va $X_2 \oplus K=001$ amallarni bajarib quyidagilarga ega bo‘linadi:

$$Sbox(X_1 \oplus K)=10 \text{ va } Sbox(X_2 \oplus K)=01 \qquad (4.7)$$

4.7-tenglamada K kalitning qiymatini noma’lum deb tasavvur qilinsa, lekin bunda kirish qiymatlari ma’lum, ya’ni $X_1=110$ va $X_2=010$. Bu yerda S-blokdan chiqish qiymatlari ma’lum, ya’ni 2-tenglamadan $Sbox(X_1 \oplus K)=10$ va $Sbox(X_2 \oplus K)=01$. Yuqoridagi birinchi S-blokdan qaysi joylarda 2-tenglikning chiqish qiymatlari $Sbox(X_1 \oplus K)=10$ va $Sbox(X_2 \oplus K)=01$ teng bo‘lgan holatlarni topish mumkin. Bunda $X_1 \oplus K \in \{000,101\}$ bo‘lgan holatlarda S-blokdan “10”, $X_2 \oplus K \in \{001,110\}$ bo‘lgan holatlarda S-blokdan “01” qiymatlar chiqishini ko‘rish mumkin. Yuqoridagi ifodalarga mos holda X_1 va X_2 larni XOR amali bo‘yicha qo‘shish orqali K kalit tegishli bo‘lgan oraliqlar quyidagicha bo‘lishi mumkin:

$$K \in \{110,011\} \cap \{011,100\}$$

ushbu kesishmadan $K=011$ ekanligi kelib chiqadi. Yuqoridagi “hujum” kriptoanalizchiga tanlangan ochiq matn va shifrmatn ma’lum bo‘lgan holda, noma’lum K kalitni aniqlash uchun oddiy S-blokga qaratildi. DES algoritmining yaxlit S-blokiga qaratilgan hujum ham yuqoridagidek amalga oshiriladi.

Biroq, DES algoritmining bitta S-blokiga bir raundda qilingan hujum natijasi yetarli bo‘lmaydi. Bundan tashqari, kriptoanalizchi birinchi raunddan boshqa roundlarga kirish ma’lumotini bilmaydi va oxirgi raunddan boshqa roundlardan chiquvchi ma’lumotni bilmaydi. Kriptoanalizchiga oraliq raundlardagi kirivchi va chiqiuvchi ma’lumotlar noma’lum bo‘ladi.

Ushbu yondoshuv DES algoritmini krioptotahlil qilishda foydaliligini ko‘rsatish uchun, tahlilni bitta raundda to‘liq amalga oshirish kerak, bunda sakkizta S-blokni bir vaqtning o‘zida ko‘rib chiqish kerak. Tahlil bir raundga uzaytirildimi, demak tahlilni bir necha raundlarga uzaytirish mumkin. Tashqaridan bu ikkala vazifa ham qiyin bo‘lib ko‘rinadi. Biroq, kirish va chiqishdagi farqlarga qarab, qaysi S-bloklar “faol” qaysilari “faolmas” ligini aniqlash oson . Natijada, ayrim hollarda “faolmas” S-bloklarni tahlil qilmasdan hujumni bir raundga qisqartirishga erishish mumkin. Shundan keyin tahlilni bir necha raundaga kengaytirib, kirish va chiqishdagi farqni topishish mumkim va bu farq keyingi raund uchun kirish ma’lumoti vazifasini o‘taydi. Buning murakkabligi S-blokning o‘ziga xos xususiyatlari va shu bilan birga har bir roundda amalga oshiriladigan chiziqli almashtirishlarga bog‘liq.

Bu yerda asosiy e’tibor sifatida kirish va chiqishda bitlaridagi farqlarga qaraladi. Masalan X_1 va X_2 kirish qiymatlari ma’lum. Keyin X_1 kirish uchun, S-blokga kiruvchi xaqiqiy qiymat $X_1 \oplus K$ va X_2 uchun S-blokga kiruvchi xaqiqiy

qiymat $X_2 \oplus K$, lekin bu yerda kalit nima ekanligini noma'lum. Farqlar, kirish parametrlarini "modul2" bilan qo'shilgandagi natija bilan teng, yani XOR amali orqali qo'shish. Shundan S-blokdagi kirishlar farqi quyidagiga teng bo'ladi:

$$(X_1 \oplus K) \oplus (X_2 \oplus K) = X_1 \oplus X_2$$

Yuqoridagidan shunga e'tibor qaratish kerakki kirishdagi farq K kalitga bog'liq emas. Bu differensial kriptoanalizni amalga oshirishdagi asosiy jihat hisoblanadi. Demak chiqish qiymatlari mos holda $Y_1=Sbox\ (X_1 \oplus K)$ va $Y_2=Sbox\ (X_2 \oplus K)$. Keyin raunddan chiquvchi $Y_1 \oplus Y_2$ farq keyingi raund uchun kirish farqi qiymati bo'ladi. Bundan maqsad kirish ma'lumoti farqini qurish va boshqa raundlar uchun ham bu farqlarni topishni davom ettirib "ketma-ketlik zanjirini" hosil qilish kerak. Kirish farqlari K kalitdan mustaqilligi sababli va differensial tahlilchining ochiq matnni tanlay olishini inobatga olib, kirish farqini ixtiyoriy tanlash imkniyatiga ko'ra ularni ixtiyoriy tanlab va turli xildagi chiqish farqlariga ega bo'lish mumkin.

Differensial hujumning yana bir muhim elementi S-blokga kirish farqining nolga tengligi, har doim chiqish farqining nolga tengligiga olib keladi. Kirish farqlari nolga tengligi faqat kirish qiymatlari teng degan ma'noni anglatadi, demak X_1 va X_2 ning qiymatlari teng bo'lganda ularni XOR amali bilan qo'shilgan farqlar qiymati nolga teng bo'ladi. Bu holat chiqishdagi farqlar ham bir biriga tengligini anglatadi. Sababi chiqish qiymatlari ham bir biriga teng bo'lganda ularning farqi $Y_1 \oplus Y_2=0$ nolga teng bo'ladi. Shuning uchun ushbu elementlarni o'zgartiruvchi S-bloklarni "faolmas" qilib ularni diferensial tahlil qilmaslik mumkin. Sababi kirish va chiqishdagi farqlar bir xil nolga teng bo'lib o'zgarish kuzatilmaydi.

So'ngi kuzatuv shuni ko'rsatadaki, hodisalar aniq sodir bo'lishi shart emas. Boshqa so'z bilan aytganda, ba'zi kirish farqlari chiqishda ehtimollikka asosan o'zgaradi, shunga ko'ra ehtimollikka asoslangan hujumni davom ettirish va undan kalitni tiklab olish mumkin bo'ladi.

Masalan S-blok berilgan, uni quyidagiga asoslanib kirish farqlarini tahlil qilish mumkin. Har bir mumkin bo'lgan kirish qiymati X uchun, barcha X_1 va X_2 juftliklarni

$$X=X_1 \oplus X_2$$

va tegishli chiqish farqlarini

$$Y=Y_1 \oplus Y_2$$

deb belgilanadi. Bu yerda

$$Y_1=Sbox\ (X_1)\ va\ Y_2=Sbox\ (X_2)$$

Yuqoridagi 4.4-jadval uchun tahlil natijalari quyidagi 4.5-jadvaldagi qiymatlarni beradi.

4.5-jadval

S-blokning differensial tahlili

$X_1 \oplus X_2$	$Sbox\ (X_1) \oplus Sbox\ (X_2)$			
	00	01	10	11
000	8	0	0	0
001	0	0	4	4
010	0	8	0	0

$X_1 \oplus X_2$	$Sbox\ (X_1) \oplus Sbox\ (X_2)$			
	00	01	10	11
011	0	0	4	4
100	0	0	4	4
101	4	4	0	0
110	0	0	4	4
111	4	4	0	0

Har qanday S-blok uchun, “000” farqli kirish qiymati muhim emas, chunki kirish qiymatlari bir xil va S-bloki "faol emas" (farqlarga nisbatan), chunki chiqish qiymatlari bir xil bo‘lishi kerak. Masalan 4.5-jadvaldan kirishdagi farq 010 bo‘lganda chiqish qiymati 01 teng bo‘lgan imkoniyatlar soni eng ko‘p va 8 ta. Yuqoridagi 3-tenglamadan qayd qilinganidan $X_1 \oplus X_2=010$ bo‘lsa, S-blok uchun haqiqiy kirish farqi ham 010 ga teng bo‘ladi, chunki kirishdagi farqlarni aniqlashda XOR amali orqali qo‘shilganda K kalit yo‘qolib ketadi.

DES algoritmining differensial kriptoanalizi juda murakkab. Ushbu tahlilni aniqroq ko‘rsatish uchun, DES algoritmiga xos bo‘lgan murakkabliklardan voz kechish maqsadida, Tiny DES yoki TDES deb ataladigan DESning soddalashtirilgan versiyasini tanlab, keyin TDES algoritmida differensial kriptoanalizni amalga oshirilsa oson va maqsadga muvofiq bo‘ladi.

TDES algoritmining differensial tahlili

Ushbu differensial kriptoanaliz TDES algoritmining yuqorida ko‘rsatilgan o‘ng S-blokiga qaratiladi. Masalan $X1 \oplus X2=001000$ shartni qanoatlantiruvchi X_1 va X_2 barcha kiruvchi juftliklar uchun $SboxRight(X_1) \oplus SboxRight(X2)$ tenglikning bajarilish ehtimolligi topiladi

$$X_1 \oplus X_2 =001000 => SboxRight(X_1) \oplus SboxRight(X_2)=0010 \quad (4.7)$$

tenglikning bajarilish ehtimolligi ¾ . Har qanday S-blok uchun quyidagi tenglik o‘rinli:

$$X_1 \oplus X_2 =000000 => SboxRight(X_1) \oplus SboxRight(X_2)=0000 \quad (4.8)$$

Bundan maqsad ushbu kuzatuvlardan TDES algoritmini differensial tahlil qilishni rivojlantirishdir.

Differensial kriptoanaliz bu ochiq matnni tanlash hujumi(chosen plaintext attack)dir. Masalan ikkita ochiq matn bloklari shifrlandi, $P=(L,R)$ va $P'=(L',R')$, ularning XOR amalidagi yig‘indisini quyidagiga teng deb olinsin:

$$P \oplus P' = (L, R) \oplus (L', R') = 0000\ 0000\ 0000\ 0010 = 0x0002. \quad (4.9)$$

Keyin P va P' larning bir biti orasidagi farq bitta bitda farq qildi va boshqa barcha bitlari bir xil bo‘ldi. Demak, P va P' ning TDES bilan shifrlangandagi bitlari orasidagi farqni ko‘rib chiqilsa:

$$F(R, K) \oplus F(R', K)=Sboxes(expand(R \oplus K) \oplus boxes(expand(R') \oplus K).$$

Yuqoridagi 4- tenglikdan foydalanib quyidagiga ega bo‘lish mumkin

$$expand(0000\ 0010) = 000000\ 001000.$$

Chunki chiziqli kengayririshdan oldin $X_1 \oplus X_2$= 0000 0010 bo‘lgan bo‘lsa, keyin

$$expand(X_1) \oplus expand(X_2)=expand(X_1 \oplus X_2)=$$

$$expand(0000\ 0010)=000000\ 001000 \qquad (4.10)$$

10-tenglikdagi tanlangan ochiq matn bitlari farqidan ushbu $R \oplus R' = 0000\ 0010$ tenglikka ega bo‘lish mumkin. Keyin yuqoridagi 4.10-tenglikdan quyidagi tengliklar kelib chiqadi:

$$F(R, K) \oplus F(R', K) = Sboxes(expand(R \oplus K) \oplus Sboxes(expand(R' \oplus K) = (SboxLeft(A \oplus K), SboxRight(B \oplus K)) \oplus (SboxLeft(A' \oplus K), SboxRight(B \oplus K)) = (SboxLeft(A \oplus K) \oplus SboxLeft(A' \oplus K)), (SboxRight(B \oplus K) \oplus SboxRight(B' \oplus K)),$$

Bu yerda $A \oplus A' = 000000$ va $B \oplus B' = 001000$. Bu natija bilan birga 4.7 va 4.8-tenglamalar orqali quyidagi tenglik

$$F(R,K) \oplus F(R',K) = 0000\ 0010$$

¾ ehtimollik bilan bilan bajariladi.

Xulosa qilib aytganda, agar $R \oplus R' = 0000\ 0010$ bo‘lsa, ixtiyoriy (noma’lum) qism kalit K uchun

$$F(R,K) \oplus F(R',K) = 0000\ 0010 \qquad (4.11)$$

tenglik ¾ ehtimollik bilan bajariladi. Boshqacha qilib aytganda ma’lum kirish qiymatlari farqi chiqish farqiga katta ehtimollik bilan teng bo‘ladi. Endi ushbu natijani TDES algoritmining barcha raundlariga qo‘llash keltirib o‘tiladi.

Chunki, differensial kiptotahlil bu tanlangan ochiq matn hujumi(chosen plaintext attack) bo‘lgani uchun 4.10-tenglikni qanoatlantiruvchi P va P' ochiq matnlar tanlanadi. 4.6-jadvalda TDESning ochiq matn qiymatlarini shifrlash bosqichlarini tahlil qilindi. Tanlagan P va P' ochiq matnlardan quyidagilarga ega bo‘linadi:

$$R_0 \oplus R'_0 = 0000\ 0010 \text{ va } L_0 \oplus L_0 = 0000\ 0000.$$

Keyin 4.11-tenglikdan

$$R_1 \oplus R'_1 = 0000\ 0010$$

tenglikning bajarilish ehtimolligi ¾ . Bu natija shuni anglatadiki

$$\begin{aligned} R_2 \oplus R'_2 &= (L_1 \oplus F(R_1, K_2)) \oplus (L'_1 \oplus F'(R'_1, K_2)) \\ &= (L_1 \oplus L'_1) \oplus (F(R_1, K_2) \oplus F(R', K_2)) \\ &= (R_0 \oplus R'_0) \oplus (F(R_1, K_2) \oplus F(R'_1, K_2)) \\ &= 0000\ 0010 \oplus 0000\ 0010 \\ &= 0000\ 0000 \end{aligned}$$

$(3/4)^2 = 4/16 = 0.5625$ ehtimollik bilan bajariladi. Quyidagi 4.6-jadvalda $R_3 \oplus R'_3$ va $R_4 \oplus R_4$ uchun berilgan natijalar ham xuddi yuqoridagidek hisoblangan.

4.6-jadval

TDES ning differensial tahlili

$(L_0, R_0) = P$	$(L'_0, R'_0) = P'$	$(L_0, R_0) = P$	**Bajarilish ehtimolligi**
$L_1 = R_0$ $R_1 = L_0 \oplus F(R_0, K_1)$	$L'_1 = R'_0$ $R'_1 = L'_0 \oplus F(R'_0, K_1)$	$(L_1, R_1) \oplus$ $(L_1, R_1) = 0x0202$	¾
$L_2 = R_1$ $R_2 = L_1 \oplus F(R_1, K_2)$	$L'_2 = R'_1$ $R'_2 = L'_1 \oplus F(R'_1, K_2)$	$(L_2, R_2) \oplus$ $(L'_2, R'_2) = 0x0200$	$(¾)^2$
$L_3 = R_2$ $R_3 = L_2 \oplus F(R_2, K_3)$	$L'_3 = R'_2$ $R'_3 = L'_2 \oplus F(R'_2, K_3)$	$(L_3, R_3) \oplus$ $(L'_3, R'_3) = 0x0002$	$(¾)^2$

$(L_0, R_0) = P$	$(L'_0, R'_0) = P'$	$(L_0, R_0) = P$	**Bajarilish ehtimolligi**
$L_4 = R_3$ $R_4 = L_3 \oplus F(R_3, K_4)$ $C = (L_4, R_4)$	$L'_4 = R'_3$ $R'_4 = L'_3 \oplus F(R'_3, K_4)$ $C = (L'_4, R'_4)$	$(L_4, R_4 \oplus)$ $(L'_4, R'_4) = 0x0202$ $C \oplus C' = 0x0202$	$(¾)^3$

4.6-jadvaldan ba'zi noma'lum kalit bitlarini aniqlash algoritmini chiqarib olish mumkin. *P* va *P'* ochiq matnlarni 10-tenglik bo'yicha tanlab, ularga mos C va C' shifrmatlar olinadi. Chunki TDES algoritmi Feystel tarmog'iga asoslanar ekan

$$R_4 = L_3 \oplus F(R_3, K_4) \text{ va } R'_4 = L'_3 \oplus F(R'_3, K'_4).$$

Qo'shimcha blok $L_4 = R_3$ va $L'_4 = R'_3$ ga teng. Natijada

$$L_3 = R_4 \oplus F(L_4, K_4) \text{ va } L'_3 = R'_4 \oplus F(L'_4, K_4).$$

Tenglamani quyidagicha qayta yozib olish mumkin

$$L_3 = R_4 \oplus F(L_4, K_4) \text{ va } L'_3 = R'_4 \oplus F(L'_4, K_4).$$

Agar

$$C \oplus C = 0x0202 \qquad (4.12)$$

bo'lsa, 4.6-jadvaldan $L_3 \oplus L'_3 = 0000\ 0000$ ekanligi deyarli aniq va bu $L_3 = L'_3$ ekanligini anglatadi. Bu quyidagini keltirib chiqaradi:

$$R_4 \oplus F(L_4, K_4) = R'_4 \oplus F(L'_4, K_4).$$

O'zgaruvchilarni tenglikning ikki tomoniga o'zgartirib tenglamani qayta yozib olish mumkin

$$R_4 \oplus R'_4 = F(L_4, K_4) \oplus F(L'_4, K_4) \qquad (4.13)$$

E'tibor berilsa, 4.13-tenglikda faqat K_4 ning qiymati noma'lum. Endi K_4 kalit bitlari topish uchun yuqoridagi natijadan qanday foydalanish kerakligi ko'rib chiqiladi.

4.9-tenglikka mos keluvchi ochiq matn juftliklarini, 4.12-tenglikni qanoatlantirsa, bundan 4.13-tenglikka ega bo'linadi. Shundan keyin

$$C \oplus C' = (L_4, R_4) \oplus (L'_4, R'_4) = 0x0202,$$

Bizga ma'lumki

$$R_4 \oplus R'_4 = 0000\ 0010 \qquad (4.14)$$

va yuqoridan quyidagi ham ma'lum

$$L_4 \oplus L_4 = 0000\ 0010. \qquad (4.15)$$

Demak

$$L_4 = l_0 l_1 l_2 l_3 l_4 l_5 l_6 l_7 \text{ va } L'_4 = l'_0 l'_1 l'_2 l'_3 l'_4 l'_5 l'_6 l'_7$$

Keyin 4.15-tenglikda i = 0,1,2,3,4,5, 7 lar uchun $l_i = l'_i$ tenglik o'rinli, faqat $l_6 \neq l'_6$.

Shuning uchun 4.14-ifodaning qiymatini 4.13-ifodaning mos tomoni bilan almashtirish orqali *F* ni kengaytirib quyidagi topilpdi

$$0000\ 0010 = (SboxLeft(l_4 l_7 l_2 l_1 l_5 l_7 \oplus k_0 k_2 k_3 k_4 k_5 k_7), SboxRight(l_0 l_2 l_6 l_5 l_0 l_3 \oplus k_{13} k_{14} k_{15} k_9 k_{10} k_{11})) \oplus (Sboxleft(l'_4 l'_7 l'_2 l'_1 l'_5 l'_7 \oplus k_0 k_2 k_3 k_4 k_5 k_7), SboxRight(l'_0 l'_2 l'_6 l'_5 l'_0 l'_3 \oplus k_{13} k_{14} k_{15} k_9 k_{10} k_{11}) \qquad (4.16)$$

4.16-ifodaning chap qismidagi 4 ta bitlari quyidagini beradi

$$0000 = (SboxLeft(l_4 l_7 l_2 l_1 l_5 l_7 \oplus k_0 k_2 k_3 k_4 k_5 k_7) \oplus (SboxLeft(l'_4 l'_7 l'_2 l'_1 l'_5 l'_7 \oplus k_0 k_2 k_3 k_4 k_5 k_7$$

$l_i = l'_i$ tengligidan va 4.16 ifodadan $k_0k_2k_3k_4k_5k_7$ kalit bitlari farqi 0 ga tengligidan bu K_4 qism kalit bitlarini aniqlashning imkoni yo‘qligi kelib chiqadi.

Boshqa tomondan olib qaralganda, 4.16-ifodaning o‘ng tomondagi 4 biti bizga quyidagini beradi

$$0010=SboxRight(l_0l_2l_6l_5l_0l_3 \oplus k_{13}k_{14}k_{15}k_9k_{10}k_{11}) \oplus SboxRight(l'_0l'_2l'_6l'_5l'_0 l'_3 \oplus k_{13}k_{14}k_{15}k_9k_{10}k_{11}) \quad (4.17)$$

Bundan $k_{13}k_{14}k_{15}k_9k_{10}k_{11}$ qism kalit bitlarini moslarini tanlab olish mumkin va bunda qism kalit bitlarini noto‘g‘ri tanlash ehtimolligi ham bor. Chunki chap S-blokning L_4 va L'_4 ning bitlarining qiymatlari ma’lum, 4.17-ifodadan noma’lum kalit bitlarini aniqlash mumkin. Ushbu kalit bitlarni tiklash algoritmi 4.7-jadvalda keltirilgan.

4.7-jadval

Raund kalitini aniqlash algoritmi

```
count[i] = 0, for i = 0 , 1 , . . . , 63
for i = 1 to iterations
    Choose P and P with P⊕P = 0x0002
    Obtain corresponding C = c0 c1 ...c15 and C'=c'0 c'1 ...c'15
    if C⊕C = 0x0202 then
    li =ci and l'i =c'i for i = 0 , 1 , . . . , 7
        for K = 0 to 63
    if 0010 = = 0010=SboxRight (l0l2l6l5l0l3⊕K)
    ⊕SboxRight(l0l2l6l5l0l3⊕K)   then
                increment count [K]
            end if
        next K
    end if
next i
```

4.7-jadvaldaning pastki qismidagi sikl har safar bajariladi, $K= k_{13}k_{14}k_{15}k_9k_{10}k_{11}$ qism kalit bitlari to‘g‘ri topilganda count[K] bittaga oshiriladi, aks holda K ning indeksi bittaga oshiriladi. Natijada, maksimal indeksli qism kalit round kaliti bo‘lish ehtimolligi yuqori bo‘ladi. Bunday maksimal qiymatli indeksli qism kalitlar ko‘p bo‘lishi mumkin, ammo yetarli miqdorda takrorlanishlar, bunday sonlar kam bo‘lishini ta’minlaydi.

4.7-jadvalda berilgan algoritm uchun alohida holatlarda, P va P’ ochiq matnlarning $P \oplus P = 0x0002$ shartni qanoatlantiruvchi 100 ta jufti generatsiya qilindi. Olingan matn juftliklarining 47 tasida $C \oplus C = 0x0202$ tenglik qanoatlandi va shu vaqtda barcha 64 siklda qism kalit qabul qilgan 6-bitli raund kalitining qiymatlari qarab ko‘rildi. Ushbu tajribada ochiq matn va shifrmatn juftliklari mos kelgan 47 ta siklda to‘rtta raunda kalitlarining qiymatlarini eng ko‘p uchraganlari 000001, 001001, 110000, va 000111. Boshqa hech qaysi qiymatlarning uchrash ehtimolligi 39 tadan yuqori bo‘lmaydi. Shundan xulosa qilish mumkinki K_4 raund kalitining qiymatlari yuqorida ko‘rsatilgan qiymatlardan biriga teng bo‘lishini anglatadi. Keyin K_4 kelib chiqish tarifidan foydalanib quyidagini yozish mumkin

$$k_{13}k_{14}k_{15}k_9k_{10}k_{11} \in \{000001,001001,110000, 000111\}$$

bunga ekvavalent

$$k_{13}k_{14}k_{15}k_9k_{10}k_{11} \in \{00001, ,11000\} \qquad (4.18)$$

Bunday holatda, kalit

K = 1010 1001 1000 0111

shuning natijasida 4.18- tenglamadan kutilganidek $k_{13}k_{14}k_{15}k_9k_{10}k_{11}$= 11000.

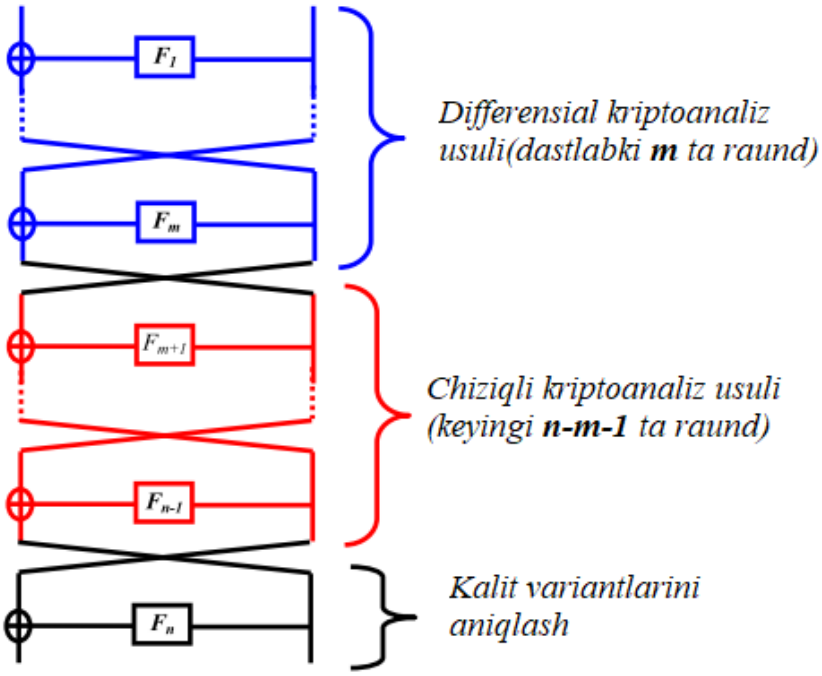
Albatta, agar biz hujumchi bo‘lsak, kalitni bilmaymiz, shuning uchun K ni qayta tiklashda 2^{11} ta qadamda noma’lum kalit qidirishimiz kerak va ularning har biri uchun 18-tenglikning har ikkala tomoni imkoniyatini sinab ko‘rishimiz kerak. Ushbu 2^{12} ta K kalit koeffitsientlarining har biri uchun, biz shifrmatnni deshifrlaymiz va kalit to‘g‘ri kelgan holatda ochiq matn qayta tiklanadi. Ushbu natija hisoblashning boshida yoki oxirida, xullas yarmida sodir bo‘lishi mumkinligini hisobga olib $2^{12}/2=2^{11}$ siklda tekshirib ko‘ramiz.

Ushbu usul bilan butun K ni qayta tiklash uchun kutilgan jami hisoblashlar soni taxminan 2^{11} ta shifrlashni amalga oshiramiz, shuningdek taqqoslaganda juda muhim bo‘lmagan differemsial hujum ham talab qilinadi. Natijada, biz butun 16-bit kalitni topishimiz uchun kalitni to‘liq qidiruv usuli $2^{16}/2=2^{15}$ dan ko‘ra ancha yaxshi bo‘lgan 2^{11} marta shifrlash jarayonini amalga oshirish orqali topishimiz munkin. Bu TDES algoritmi uchun qisqartirilgan hujum mavjudligini ko‘rsatadi va natijada uni xavfsiz algoritm deb hisoblab bo‘lmaydi degan xulosa berishga asos bo‘ladi.

2.3. Simmetrik blokli shifrlash algoritmlariga nisbatan chiziqli-differensial kriptotahlil usuli

Chiziqli-differensial kriptoanaliz usuli 1994-yilda Martin Xellman va Syuzen Langford tomonidan DES shifrlash algoritmiga qarshi hujum turi sifatida ishlab chiqilgan. Ushbu usul tanlangan ochiq matnga asoslangan bo‘lib, g‘oya mualliflari tomonidan chiziqli-differensial kriptoanaliz (ChDK) usulini qo‘llab, 512 ta ochiq matn yordamida DES shifrlash algoritmida foydalanilgan maxfiy kalitning 10 bitini 80% ehtimollik bilan aniqlashga erishilgan. Ochiq matn sonini 768 taga oshirish orqali bu ehtimollik qiymatini 95% gacha yetkazish mumkin.

(ChDK) usuli qurilish tamoyili chiziqli kriptoanaliz (ChK) hamda differensial kriptoanaliz (DK) usullarini umumlashtirishga asoslangan bo‘lib, Feystel tarmog‘iga asoslangan n raundli shifrlash algoritmi uchun uning umumiy qo‘llanilish sxemasi 4.4-rasmda keltirilgan.



4.4-rasm. ChDK usulining umumiy qo‘llanish sxemasi

Ya’ni, kriptoanalizning dastlabki qadamida kiruvchi (1-raundga kiruvchi) ayirmani bilgan holda m - raunddan chiquvchi ayirma qiymati DK usuli orqali aniqlanadi, keyingi qadamda $n-1$ - raunddan chiquvchi ayirma qiymati ChK usuli orqali aniqlanadi. So‘nggi qadamda esa oxirgi raund funksiyasiga kiruvchi va funksiyadan chiquvchi ayirma va shifr matn qiymatlarini bilgan holda so‘nggi raund funksiyasida foydalanilgan kalit variantlari statistika o‘tkazish (tekshirib ko‘rish) orqali aniqlanadi.

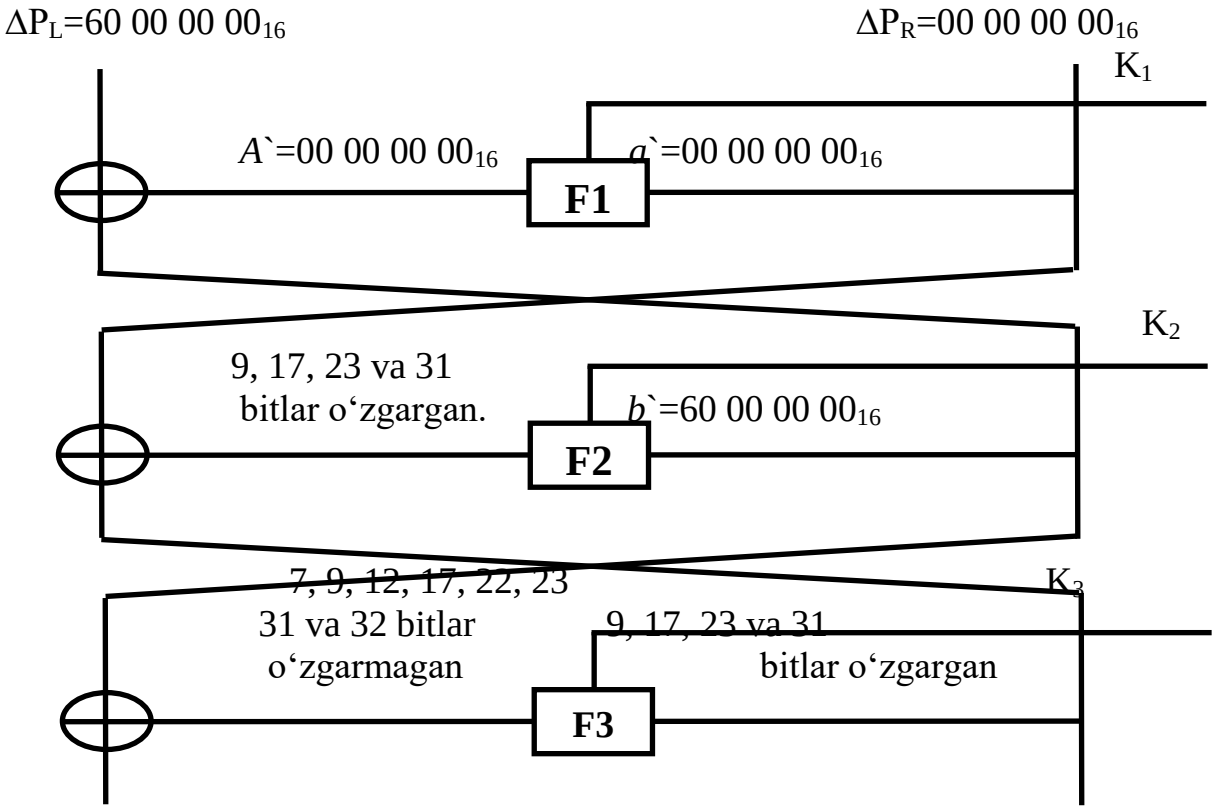
Kriptoanaliz samaradorligi ham aynan DK va ChK usullari samaradorligiga ya’ni, ular orqali aniqlangan so‘nggi raund funksiyasidan chiquvchi ayirma qiymatining to‘g‘ri aniqlanganligiga bog‘liqdir.

Chiziqli – differensial kriptoanaliz usuli chiziqli hamda differensial hujum turlarini umumlashtirishga asoslangan. Ya’ni biror feystel tarmog‘iga asoslangan *n* raundli shifrlash algoritmi tahlil qilinayotgan bo‘lsa, dastlabki *m* raundiga differensial, keyingi *n-m-1* raundiga chiziqli kriptoanaliz usulini qo‘llash hamda *n*-raundda foydalanilgan kalit bitlarini aniqlash tamoyiligi asoslanadi. Qolaversa chiziqli hamda differensial kriptoanaliz usullari kabi ChDK usulida ham dastlab *n*-raund kalit bitlari so‘ngra *n-1*-raund kalit bitlari va hokazo *1*-raund kalit bitlari aniqlab boriladi.

Quyida 7 raundan iborat bo‘lgan DES shifrlash algoritmiga ChDK usuli qo‘llanishi ko‘rib chiqiladi. Bu holda shifrlash algoritmining daslabki 3 (1 dan 3 gacha) raundiga differensial kriptoanaliz usuli, keyingi 3 raundiga (4 dan 6 gacha) esa chiziqli kriptoanaliz usuli qo‘llaniladi. Boshlang‘ich IP va oxirgi IP^{-1} o‘rin almashtirish akslantirishlari shifrlangan ma’lumotning kriptobardoshligiga ta’siri yo‘qligi uchun, ularni tashlab o‘tish mumkin. Kriptoanalizchini kiruvchi ma’lumotning chap qism qiymatlari, ikkinchi yoki uchinchi, yoki birgalikda ikkinchi va uchinchi bitlar farqli bo‘lgan holatlar qiziqtiradi. Shunga asosan S_1 akslantirish

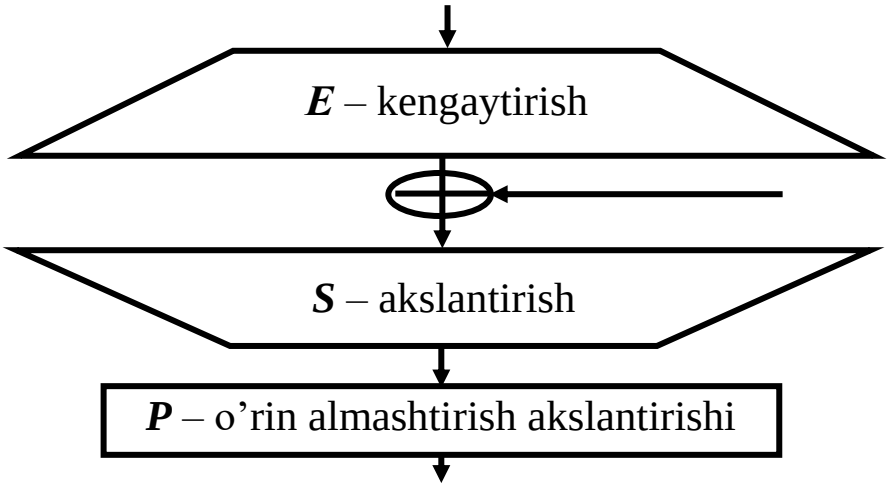
blokining kirishiga faqatgina ushbu ayirma kiritilgan holat e’tiborga olinadi, qolgan bloklar kirishiga esa nolga teng bo‘lgan ayirma beriladi. Ushbu holatda ayirmani chap qismi, ikkinchi va uchinchi (ikkita ma’lumotning XOR yig‘indisi bo‘lgan) o‘rinlardan tashqari nollardan iborat bo‘ladi. O‘ng qismda esa kiruvchi ma’lumotlar farqli bo‘lmagani tufayli ularning ayirmasi nolga teng bo‘ladi.

4.5-rasmda birinchi hamda ikkinchi raund *F* funksiyalari kirishiga berilayotgan ayirmalarni mos ravishda *a`* va *b`* orqali, birinchi raund *F* funksiyadan chiquvchi ayirmani esa *A`* orqali ifodalangan.



4.5-rasm. DES shifrlash algoritmining dastlabki 3 ta raund xususiyati

Kiruvchi nollik ayirmalar chiqishda ham doimo noldan iborat bo‘ladi, shuning uchun 2 – raund *F* shifrlash funksiya kirishiga 1 – raundga kiruvchi ayirmaning chap qismi beriladi. DES shifrlash algoritmining *F* – feystel funksiya



4.6–rasmda ifodalangan akslantirishlarni o‘z ichiga oladi.

4.6-rasm. DES shifrlash algoritmining *F* – feystel funksiyasi

bu yerda: *E* – kengaytiruvchi o‘rin almashtirish, *R* – o‘rin almashtirish hamda *S* - blok akslantirishlari quyidagi 4.7–4.16 jadvallar orqali amalga oshiriladi:

4.7 – jadval

Kengaytiruvchi o‘rin almashtirish jadvali

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

4.8 – jadval

P – o‘rin almashtirish jadvali

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

4.9 – jadval

S_1 - akslantirish bloki

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

4.10 – jadval

S2 - akslantirish bloki

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

4.11– jadval

S_3 - akslantirish bloki

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

4.12– jadval

S_4- akslantirish bloki

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

4.13– jadval

S_5- akslantirish bloki

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

4.14– jadval

S_6- akslantirish bloki

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

4.15– jadval

S_7- akslantirish bloki

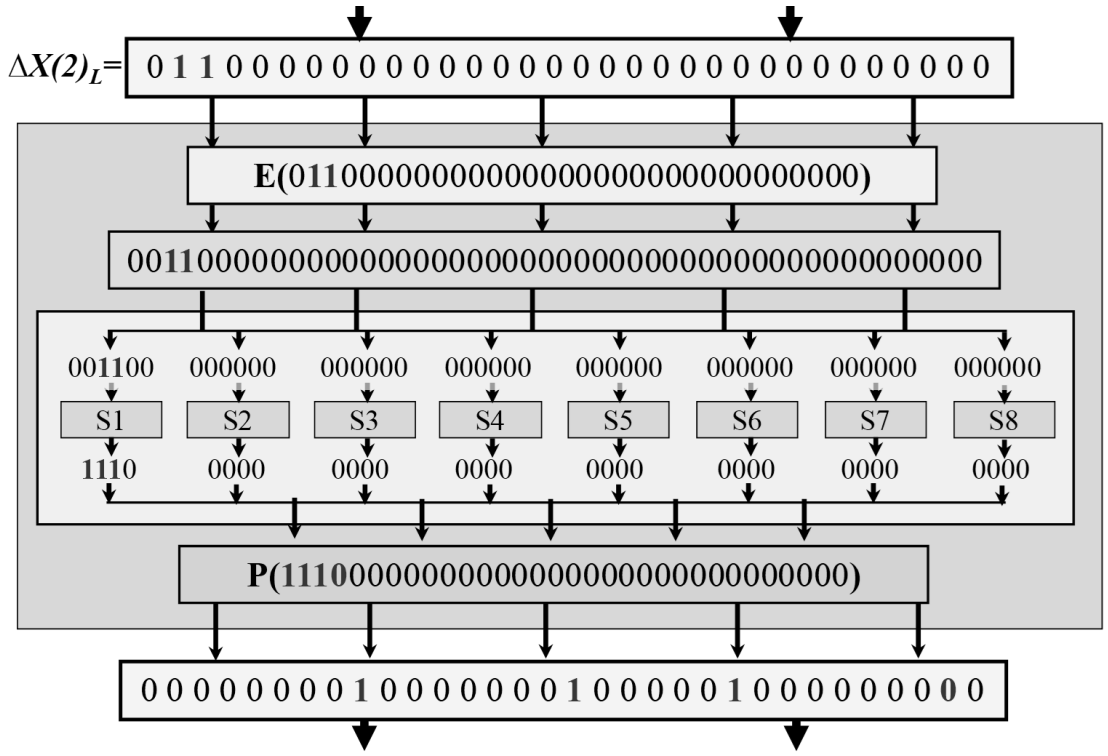
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

4.16– jadval

S_8- akslantirish bloki

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

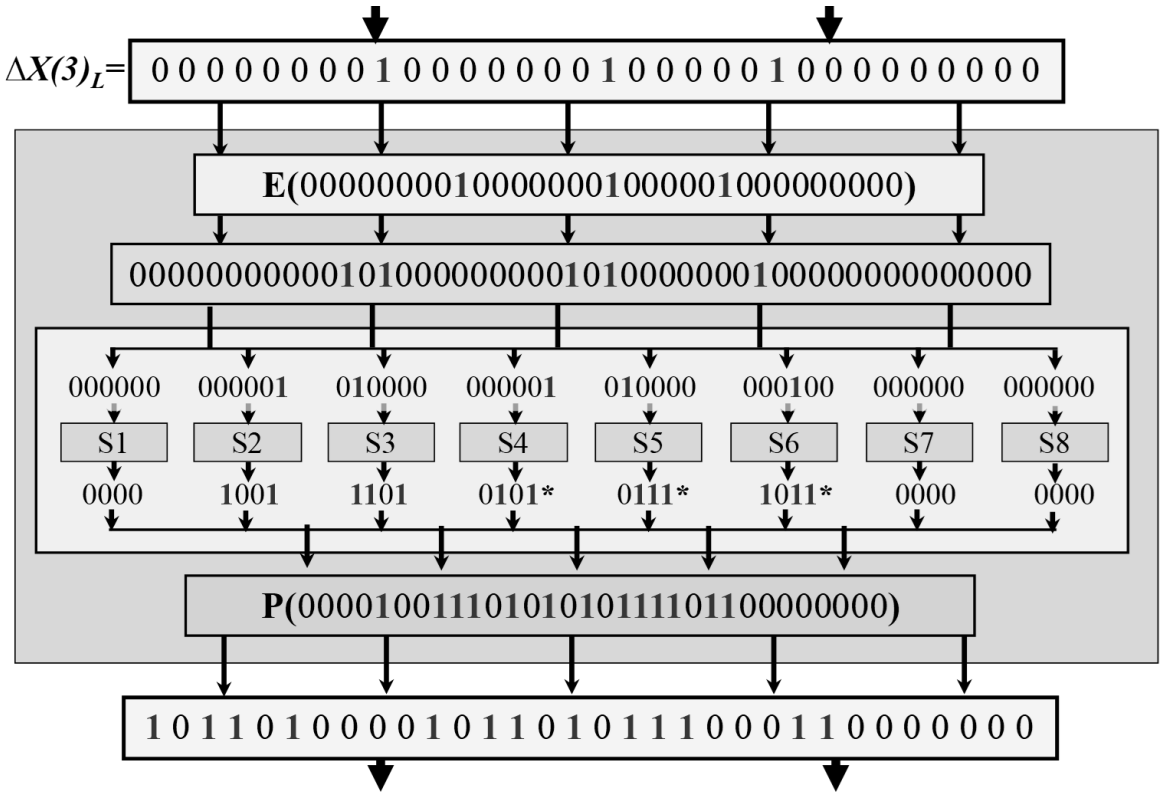
Ikkinchi raund *F* funksiyasiga kiruvchi *b`=60000000* orttirmani *F* funksiya *E, S, P* – akslantirishlaridan so‘ng o‘zgarishi 4.7 – rasmda ifoda etilgan.



4.7-rasm. *F(2)* – funksiyaga kiruvchi orttirmaning o‘zgarish jarayoni

Demak, 4.7 – rasmda ko‘rsatilgan akslantirishlar natijasiga ko‘ra, 2–raund F–funksiya chiqishida Δ=00000000**1**00000000**1**00000**1**0000000**0**0 orttirma hosil bo‘ladi, ya’ni chiquvchi orttirmaning 9, 17, 23 va 31 o‘rinlari o‘zgargan va qolgan o‘rinlari o‘zgarmaganligi kuzatiladi. Bu chiquvchi orttirma qiymatlari albatta S akslantirish bloki xususiyatiga bog‘liq holda qandaydir *p* ehtimollik bilan hosil bo‘ladi.

U xolda DES shifrlash algoritmi ikkinchi raund *F* funksiya chiqishidagi 9, 17, 23 va 31 o‘rinlarida farqli bo‘lgan ayirma hosil bo‘lishi mumkin. Bu ayirma avvalgi raunddan chiqqan nollik ayirma bilan mod2 bo‘yicha qo‘shishdan so‘ng o‘zgarmay qoladi va uchinchi shifrlash raund *F* funksiyaning kirish ayirmasi bo‘ladi. Uchinchi shifrlash raund *F* funksiyasiga kiruvchi ayirmaning o‘zgarishi 4.8 – rasmda ifoda etilgan.



4.8-rasm. *F(3)* – funksiyaga kiruvchi orttirmaning o‘zgarish jarayoni

Uchinchi shifrlash raund *F* funksiyasiga kiruvchi ayirma 4.4 – rasmga ko‘ra kengaytirish amalidan o‘tgandan keyin 9, 17, 23 va 31 – bitlar, S_1 va S_7 bloklardan tashqari barcha *S* akslantirish bloklarining kirish ayirmasida hosil bo‘ladi (9 – bit S_2 va S_3 bloklarni kirish ayirmasida, 17 – bit S_4 va S_5, 23 – bit S_5, 31 esa S_8 blokda hosil bo‘ladi). Demak 1 - va 7 - bloklarning chiqishlarida nollik ayirmalar hosil bo‘ladi. Qolgan akslantirish bloklarining chiqishlari ma’lum emas. Avvalgi raundda kuzatilgan jarayonga o‘xshab o‘rinalmashtirish amalidan so‘ng S_1 blok chiqishlari 9, 17, 23 va 31 – bitlarida hosil bo‘ladi, S_7 – blokning chiqishlari esa 32, 12, 22 va 7 – o‘rinlarida hosil bo‘ladi. O‘rin almashtirishdan so‘ng uchinchi shifrlash raund *F* funksiyasining chiqish ayirmasi daslabki 4 bitlarda noma’lum bo‘lgan qiymatlardan iborat bo‘ladi (7, 9, 12, 17 ,22 , 23, 31, 32 – bitlar o‘zgarmasdan qoladi). Bundan kelib chiqadiki uchinchi shifrlash raund *F* funksiyasidan chiquvchi ayirmani oldingi raundning *b*`=60 00 00 00 chiqishi bilan mod2 buiycha qo‘shganimizda hech qanday o‘zgarishlar bermaydi, chunki *b*` ning 7, 9, 12, 17, 22, 23, 31, 32 - bitlarida nollar mavjud. Demak, shifrlar jarayonining 3 raundidan so‘ng chiquvchi ayirmaning chap qismi 7, 9, 12, 17, 22, 23, 31, 32 o‘rinlarida doimiy o‘zgarmas qiymatga (qaralayotgan misolda bu nolga teng) ega bo‘ladi. Chiqish ayirmaning o‘ng qismi esa 9, 17, 23 va 31 o‘rinlarda o‘zgargan bo‘lishi ehtimoli bor (ya’ni chiqish ayirmaning o‘ng qismidagi qolgan barcha bitlar kirish ayirmaga mos ravishda nol qiymatiga ega bo‘ladilar).

Demak 7 raundli DES shifrlash algoritmining 1 – 3 rundiga differensial kriptoanaliz usulini qo‘llab, kiruvchi orttirmani qandayligini bilgan holda, 3 – raunddan chiquvchi orttirmani qanday o‘zgarish mumkinligi aniqlandi.

Tahlilning keyingi qismida navbatdagi 3 raundga (4 dan 6 gacha) chiziqli kriptoanaliz usuli ChDK usulida qanday qo‘llanishini ko‘rib chiqiladi. Shunga ko‘ra,

S_5 – blok korrelyatsion jadvali qiymatlarining yuqori chetlanish qiymati $S_5(i^*,j^*)=12$, $i^*=(0,1,0,0,0,0)$, $j^*=(1,1,1,1)$ ga teng. Bu qiymat esa r=12/64=3/16 ehtimollik bilan bajariluvchi quyidagi 4.19 – aproksimatsiya tenglamasini beradi.

$$X_2 \oplus Y_1 \oplus Y_2 \oplus Y_3 \oplus Y_4 \oplus = K_2, \quad (4.19)$$

4.19–aproksimatsiya tenglamasining chetlanish qiymati $\Delta = |1-2r| = |1-2(3/16)| = 5/8$ ga teng bo‘ladi. Hosil qilingan aproksimatsiya tenglamasini kengaytirish hamda o‘rinalmashtirish akslantirishlarini hisobga olgan holda 4 – raund kirish va chiqishiga ko‘ra ifodalasak, quyidagi 4.20 – aproksimatsiya tenglamasiga ega bo‘lamiz.

$$X(4)_{17} \oplus Y(4)_3 \oplus Y(4)_8 \oplus Y(4)_{14} \oplus Y(4)_{25} = K(4)_{26}, \quad (4.20)$$

bu tenglamadagi $(N)_m$ ifodada, N – raund qiymatini, m – bit pozitsiyasini anglatadi.

4 – raund uchun hosil qilingan aproksimatsiya tenglamasi kabi 6 – raund uchun ham aynan S_5 – blokiga nisbatan aproksimatsiya tenglamasini tuzib, hamda 3 raund uchun statistik analog tenglamasini qurish teoremasiga qo‘ra 3 – 6 – raund uchun umumiy aproksimatsiya tenglamasi tuzilsa, quyidagi 4.21 – aproksimatsiya tenglamasiga ega bo‘linadi.

$$X(4)_{17} \oplus Y(4)_3 \oplus Y(4)_8 \oplus Y(4)_{14} \oplus Y(4)_{25} \oplus X(6)_{17} \oplus Y(6)_3 \oplus Y(6)_8 \oplus Y(6)_{14} \oplus Y(6)_{25} = K(4)_{26} \oplus K(6)_{26}, \quad (4.21)$$

4.21–aproksimatsiya tenglamasining chetlanish qiymati $\Delta = \Delta_1 * \Delta_2 = (5/8) * (5/8) = 25/64$ ga, bajarilish ehtimolligi esa $r = (1-\Delta)/2 = (1-25/64)/2 = 39/128$ ga teng bo‘ladi. Tahlil jarayonida 2 ta kiruvchi X va $X`$ ma’lumotlar orttirmasini (XOR yig‘indi) ko‘rib chiqayotganligi uchun, har bir kiruvchi ma’lumot uchun aproksimatsiya tenglamasi tuzilib, hosil bo‘lgan ikki tenlamani mod2 bo‘yicha o‘zaro qo‘shilsa quyidagi, chap qismi modul 2 bo‘yicha mos bitlarni yig‘indisiga va o‘ng qismi nolga teng bo‘lgan, 4.22 – tenglikka ega bo‘linadi.

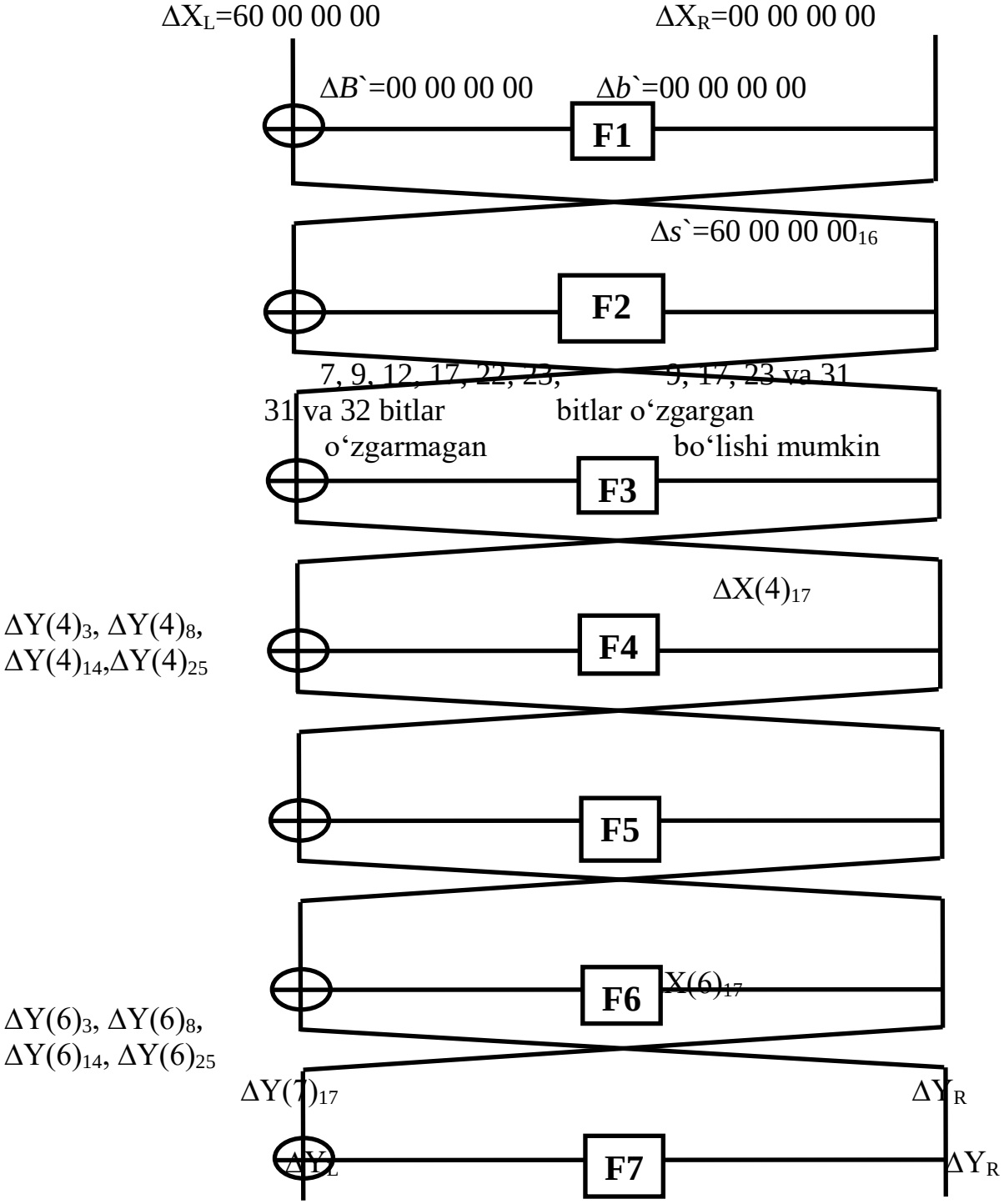
$$\Delta X(4)_{17} \oplus \Delta Y(4)_3 \oplus \Delta Y(4)_8 \oplus \Delta Y(4)_{14} \oplus \Delta Y(4)_{25} \oplus \Delta X(6)_{17} \oplus \Delta Y(6)_3 \oplus \Delta Y(6)_8 \oplus \Delta Y(6)_{14} \oplus \Delta Y(6)_{25} = 0 \quad (4.22)$$

X va $X`$ ma’lumotlar K kalit yordamida shifrlanganligi sababli, tenglamani o‘ng qismlari nolga teng bo‘ladi.

Yuqorida shifrlash algoritmining dastlabki 3 raundiga differensial kriptoanaliz usulini qo‘llab, 3 – raunddan chiquvchi orttirmani chap 17 – biti o‘zgarmay (qaralayotgan bisolda bu nolga teng) qolishligi aniqlangan edi. Uchinchi raunddan chiquvchi ayirmaning chap qismi to‘rtinchi raundga kiruvchi ayirmaning o‘ng qismi bo‘lganligi sababli, $\Delta X(4)_{17}$ orttirma qiymati ma’lum. Qolaversa uchinchi shifrlash raundidan chiquvchi ayirmaning o‘ng qismi 9, 17, 23 va 31 – o‘rinlaridan tashqari barcha o‘rindagilarni o‘zgarmay qolishligini ham aniqlash mumkin. Uchinchi shifrlash raundidan chiquvchi ayirmaning o‘ng qismi to‘rtinchi shifrlash raundiga kiruvchi ayirmaning chap qismi bo‘lganligi, qolaversa uchinchi shifrlash raundidan chiquvchi ayirmaning chap qismi to‘rtinchi shifrlash raundiga kiruvchi ayirmaning o‘ng qismi bo‘lganligi sababli, $\Delta Y(4)_3$, $\Delta Y(4)_8$, $\Delta Y(4)_{14}$ va $\Delta Y(4)_{25}$ ifodalarning qiymatlarini ham aniqlab olishimiz mumkin.

Ya’ni 4 – raundga kiruvchi orttirmaning mumkin bo‘lgan variantlari ma’lum bo‘lganligi uchun, ularni S bloklarga tuzilgan ayirma matritsa jadvallaridan

foydalangan holda funksiya chiqishida qanday qiymatga akslanishini kuzatish mumkin.



4.9-rasm. DES shifrlash algoritmining dastlabki 7 ta raundi uchun chiziqli – differensial kriptoanaliz usulining qo‘llanilishi.

Bu chiquvchi orttirmaning 3, 8, 14, 25 – bitlariga 4 – raundga kiruvchi chap orttirmaning 3, 8, 14, 25 – bitlari mod2 bo‘yicha qo‘shilsa: $\Delta Y(4)_3$, $\Delta Y(4)_8$, $\Delta Y(4)_{14}$ va $\Delta Y(4)_{25}$ orttirma qiymatlari hosil bo‘ladi. Albatta bunday hujum turini qo‘llashda kriptoanalizchi shartli ravishda shifr ma’lumot va o‘nga mos ravishda ochiq ma’lumotni biladi deb qaraladi. Shuning uchun X – ochiq va o‘nga mos ravishda Y – shifr ma’lumot hamda $X`$ – ochiq va o‘nga mos ravishda $Y`$ – shifr ma’lumot oldindan ma’lum, demak, ularning ΔY ayirmasi ma’lum. Oltinchi raunddan

chiquvchi ayirmaning chap qismi yetinchi raundga kiruvchi ayirmaning hamda ΔY shifr ma'lumotning o'ng qismi bo'lganligi sababli, $\Delta Y(6)_3$, $\Delta Y(6)_8$, $\Delta Y(6)_{14}$ va $\Delta Y(6)_{25}$ ifodalarning qiymatlari ma'lum.

Demak 1.4 – tenglama bitta $\Delta X(6)_{17}$ noma'lumga bog'liq bo'lgan tenglamani ifodalagani uchun, $\Delta X(6)_{17}$ orttirma qiymatini oson aniqlash mumkin. 1.4 – tenglikning ehtimolligi X va $X`$ ma'lumotlar uchun tuzilgan aproksimatsiya tenglamalar ehtimolligi ko'paytmasiga teng, ya'ni: p=(39/128)* (39/128)≈0,0928

Nazariy savollari:

1. Chiziqli kriptoanaliz usulining mohiyatini tushuntirib bering
2. TDES algoritmi qanday maqsadlarda ishlatiladi?
3. Simmetrik blokli shifrlash algoritmlariga differensial kriptoanaliz usuli qanday qo'llaniladi?
4. Chiziqli-differensial kriptoanaliz usuli qanday amalga oshiriladi?

Adabiyotlar va internet resurslar:

1. Xasanov P.F., Xasanov X.P., Axmedova O.P., Davlatov A.B. Kriptotahlil va uning maxsus usullari, O'quv qo'llanma, Toshkent, 2010
2. Akbarov D.YE. Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanishlari. Toshkent. "O'zbekiston markasi", 2009
3. Л.К.Бабенко, Е.А.Ищукова. Современные алгоритмы блочного шифрования и методы из анализа: учеб. пособие для студентов вузов, обучающихся по группе специальностей в обл. информ. безопасности – М.: Гелиос АРВ, 2006. – 376 с.
4. M.Stamp. Applied cryptanalysis: Breaking Ciphers in the Real World. John Wiley & Sons, Inc, 2007, -P. -417.
5. Б.Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – Москва: ТРИУМФ, 2002.
6. Xasanov P., Xasanov X., Axmedova O., Davlatov A. Kriptotahlil va uning maxsus usullari. O'quv qo'llanma.– Toshkent, 2010.
7. O.P.Axmedova, Z.T.Xudoykulov, O. Allanov, I.M.Boyquziyev Kriptoanaliz. O'quv qo'llanma. T.: "Iqtisod-Moliya", 2022. 171 b.
8. Kuryazov D.M., Sattorov A.B., Axmedova B.B. Blokli simmetrik shifrlash algoritmlari bardoshligini zamonaviy kriptotahlil usullari bilan baholash. O'quv qo'llanma. T.: "Aloqachi". 2017, 228 bet.
9. http://jnicholl.org/Cryptanalysis/Tools/
10. https://www.cryptool.org/en/cto/
11. https://resources.infosecinstitute.com/topic/cryptanalysis-tools/
12. http://rumkin.com/tools/cipher/
13. https://blackarch.org/crypto.html

14. https://www.guballa.de/vigenere-solver
15. https://www.simonsingh.net/The_Black_Chamber/substitutioncrackingtool.html
16. https://www.guru99.com/how-to-make-your-data-safe-using-cryptography.html
17. https://www.cs.bu.edu/~goldbe/teaching/CS558S17/Lab1.pdf

3-ma’ruza. “Simmetrik blokli shifrlar kriptotahlili (2 soat)

Reja:

2.1. Simmetrik blokli shifrlash algoritmlariga nisbatan algebraik kriptotahlil usuli
2.2. Simmetrik blokli shifrlash algoritmlariga nisbatan integral kriptotahlil usuli
2.3. Simmetrik blokli shifrlash algoritmlariga nisbatan “Slaydli hujum” kriptotahlil usuli
2.3. Simmetrik blokli shifrlash algoritmlariga nisbatan apparat xatoliklarni generatsiyalashga asoslangan kriptotahlil usuli

Tayanch iboralar: *algebraik krtiptotahlil, integral matrisa, chetlanish, “Slaydli hujum”, apparat xatoliklarni generatsiyalashga asoslangan kriptotahlil usuli*

2.1. Simmetrik blokli shifrlash algoritmlariga nisbatan algebraik kriptotahlil usuli

Algebraik kriptoanaliz (AK) usulining mohiyati shifrlash algoritmini ifodalovchi chekli maydonda aniqlangan algebraik tenglamalar sistemasini tuzish va shu tenglamalar sistemasini yechish orqali shifrlash kalitini topishdan iborat .

AK usuli ochiq va shifr matn asosidagi hujum turiga tegishli bo‘lib, uning murakkabligi mumkin bo‘lgan barcha tenglamalar sistemasi(TS)ni qurish va yechish hisoblanadi. Shuning uchun AK jarayonida algebraik chiziqsizlik darajalari past tenglamala sistemasini kurish va ularni yechishning optimal yo‘llarini topish muhim sanaladi.

Kriptoanalizning shifrlash algoritmini tenglamalar sistemasi orqali ifodalash bosqichi quyidagi qadamlar asosida amalga oshiriladi:

a) *shifrlash algoritmini dekompozitsiyalash*; ya’ni, shifrlash algoritmining tashkil etuvchilarini imkon qadar kichik va alohida elementlar (chiziqli, chiziqsiz va boshqa akslantirishlar)ga ajratish;

b) *har bir elementni algebraik ifodalash*; ya’ni, har bir akslantirish uchun, ularni kirishi va chiqishini bog‘lovchi imkoniyat darajasida minimal algebraik chiziqsizlik darajasiga ega bo‘lgan TS hosil qilinadi. Bir turga mansub bo‘lgan akslantirishlar uchun TS hosil qilish bir xil tarzda amalga oshiriladi. Mazkur TS faqat noma’lumlari bilan farqlanadi;

c) *har bir elementning kirishi va chiqishini boshqa elementlar hamda kalit, ochiq matn va shifr matn bitlari bilan bog‘lash*.

Ta’kidlash lozimki, TS qurish jarayoni tahlil qilinayotgan shifrlash algoritmi

tuzilishi va uning tashkil etuvchi elementlari xususiyatlariga bog‘liq holda amalga oshirilib, ixtiyoriy shifr uchun TS qurishning universal va optimal yechimi mavjud emas. Biroq bugungi kunda chekli maydonda aniqlangan chiziqsiz tenglamalar sistemasini yechishga qaratilgan ko‘plab usullar (masalan: Buxberger, F4, F5, F5C, G2V, GVW, SAT-solvers, XL, XL2, XLF, XSL, FXL, XFL, WXL, HXL, MutantXL va MXL2) taklif etilgan va ulardan AK o‘tkazishda bevosita foydalanib kelinmoqda.

Algebraik tenglamalar sistemasini tuzish

Algebraik kriptoanaliz usulining dastlabki bosqichi, shifrlash algoritmini ifodalovchi *algebraik tenglamalar sistemasini tuzish* hisoblanadi. Ushbu sistema elementlari «Algebraik tenglama» bo‘lib, u quyidagicha ta’riflanadi.

Ta’rif. Algebraik tenglama deb, quyidagi:

$$f(x_1,x_2,x_3,\ldots,x_n) = 0$$

ko‘rinishidagi tengamaga aytiladi. Bu yerda, f – noma’lum x_1, x_2, x_3,…, x_n o‘zgaruvchilardan iborat bo‘lgan ko‘phad.

Odatda f ko‘phad koeffitsientlari biror F maydondan olinadi va shunga ko‘ra ifoda F maydonda aniqlangan algebraik tenglama deb yuritiladi. Algebraik tenglama darajasi f ko‘phad darajasini anglatadi. Masalan, quyidagi:

$$y^4 + \frac{xy}{2} + y^2z^5 + x^3 - xy^2 + \sqrt{3}x^2 - \sin 1 = 0$$

tenglama haqiqiy sonlar maydoni ustidagi, 3 o‘zgaruvchili (noma’lum), 7-darajali (ya’ni chiziqsiz) algebraik tenglama hisoblanadi.

Algebraik tenglamalar sistemasini tuzishda qaralayotgan shifrlash algoritmi chiziqsiz akslantirishining algebraik strukturasiga asoslaniladi. Kriptoanaliz jarayonining 2-bosqichi samarali o‘tishi uchun, akslantirishni algebraik ifodalovchi *minimal darajadagi hadlardan (termlardan) iborat bo‘lgan maksimal sondagi tenglamalarni hosil qilish* talab etiladi. Ya’ni, ushbu tenglamalar sistemasi qaralayotgan akslantirishni to‘liq ifodalashi talab etiladi.

Ko‘plab simmetrik blokli shifrlash algoritmlarida chiziqsiz akslantirish sifatida S – blok jadvalidan foydalaniladi. Bu turdagi shifrlash algoritmlarini kriptoanaliz qilishda, avvalo S – blok akslantirishi uchun tenglamalar sistemasini tuzish ko‘rib o‘tiladi. Ushbu xolda, ixtiyoriy S – blok akslantirishiga kiruvchi (x) va chiquvchi (u) bitlarni bog‘lovchi tenglamalarni algebraik normal forma (Jegalkin ko‘phadi) ko‘rinishida bir qiymatli ifodalash mumkin. Lekin, mazkur tenglamalar kam miqdorda va ularning algebraik chiziqsizlik darajalari *(deg)* yuqori bo‘lganligi bois kriptoanaliz jarayoni uchun yetarli hisoblanmaydi. Shuning uchun, tenglamalar sistemasini shakllantirishda ikki noma’lum ko‘paytmasidan iborat bo‘lgan birhadlarni ko‘rish bilan chegaralanadi.

Umumiy holda, ixtiyoriy S – blokni ifodalovchi tenglamalarni quyidagi (4.20) ifoda ko‘rinishida shakllantirish mumkin [1, 5]:

$$\sum a_{ij}x_ix_j \oplus \sum \beta_{ij}y_iy_j \oplus \sum \gamma_{ij}x_iy_j \oplus \sum \delta_{ij}x_i \oplus \sum \varepsilon_{ij}y_i \oplus \eta = 0 \qquad (4.20)$$

bu yerda, x_i va y_j – mos ravishda S blokga kiruvchi va chiquvchi bitlar, x_ix_j – S

blokga kiruvchi bitlar kombinatsiyasi, y_iy_j – S blokdan chiquvchi bitlar kombinatsiyasi, x_iy_j – S blokga kiruvchi va chiquvchi bitlar kombinatsiyasi, $\alpha_{ij}, \beta_{ij}, \gamma_{ij}, \delta_{ij}, \varepsilon_{ij}, \eta$ – 0 yoki 1 qiymat qabul qiluvchi koeffitsientlar.

Tenglamalar sistemasini tuzishda, ushbu birhadlarni mumkin bo‘lgan barcha kombinatsiyalarini ko‘rib chiqish kerak bo‘ladi. *s* bit o‘lchamga ega bo‘lgan S – blok akslantirishi uchun 2^t ta tenglama tuzish mumkin. *t* – tenglamada ishtirok etuvchi birhadlar soni bo‘lib, u quyidagi (4.21) formula orqali hisoblanadi:

$$t = \binom{2s}{2} + 2s + 1 \qquad (4.21)$$

Ya’ni, $2s$ – S blokka kiruvchi va chiquvchi bitlar soni, $\binom{2s}{2}$ – S blokga kiruvchi va chiquvchi bitlarning mumkin bo‘lgan barcha ko‘paytmalari soni va 1 ta η – koeffitsient.

Tuzilgan barcha kombinatsiyadagi tenglamalarning aksariyati noto‘g‘ri tenglama bo‘lib, ularning berilgan S – blok akslantirishiga muvofiqligini, ya’ni to‘g‘ri tenglama ekanligini tekshirish uchun S – blok chinlik jadvalini (tekshiruv jadvali) tuzib chiqish kerak bo‘ladi. Ushbu chinlik jadvalining umumiy ko‘rinishi 4.23-jadvalda keltirilgan bo‘lib, 2^s ta satr va *t* ta ustundan iborat.

4.23-jadval

Tekshiruv jadvali

	S – blokka kiruvchi qiymatlar			**S – blokdan chiquvchi qiymatlar**			**S – blokka kiruvchi va chiquvchi qiymatlarning barcha brikmalari**									
S – blokka kiruvchi barcha mumkin bo‘lgan qiymatlar (0 dan 2^s gacha)	x_s	…	x_1	y_s	…	y_1	x_sx_{s-1}	..	x_2x_1	y_sy_{s-1}	..	y_2y_1	x_sy_s	…	x_2y_1	η
	0	...	0	1	...	0										1
	...															
	1	...	1	0	…	1										1

Tekshiruv jadvalidagi S – blokka kiruvchi (x_i) va unga mos chiquvchi (y_i) qiymatlar S – blokka muvofiq tarzda aniqlanadi, qolgan barcha birxadlarning (x_ix_j, x_ky_z) qiymati esa, mos elementlarni ko‘paytirish asosida aniqlanadi.

Tekshirish jarayoni, tenglamada qatnashgan barcha birxadlar o‘rniga ularning satr bo‘yicha chinlik jadvalidagi qiymatlarini qo‘yish va modul 2 bo‘yicha qo‘shish (XOR) hamda natijani 0 bilan taqqoslash asosida amalga oshiriladi. Shu tarzda, har bir tenglama uchun 2^s marta (umumiy holda $2^t \cdot 2^s$) tekshirish jarayoni bajariladi. Agarda, biror bir kombinatsiya asosida tuzilgan tenglama chinlik jadvalining barcha satr qiymatlari uchun o‘rinli bo‘lsa, ushbu tenglama qaralayotgan S – blok

akslantirishini qanoatlantiradi va bu tenglamani izlanayotgan tenglamalardan biri sifatida e'lon qilinadi.

Barcha tekshiruvlar natijasida olingan to'g'ri tenglamalarning ayrim qismi o'zaro chiziqli bog'liqli bo'ladi. Kriptoanaliz jarayonida esa, chiziqli bog'liqsiz (erkli) bo'lgan tenglamalar bilan ish ko'riladi. Chiziqli bog'liqsiz bo'lgan tenglamalarni ajratib olish uchun Gauss usulidan, ularni minimal sonini aniqlashda esa quyidagi teoremadan foydalanish mumkin.

Teorema 4.1. nxm – o'lchovli ixtiyoriy $F(x_1,..,x_n) \rightarrow (y_1,..y_m)$ – akslantirish bloki va barcha mumkin bo'lgan *t* ta birxadlarning ixtiyoriy *T* to'plami uchun, agar $t>2^n$ shart bajarilsa, u xolda *T* to'plam birxadlaridan iborat bo'lgan va *r=1* ehtimollik bilan bajariluvchi kamida $t-2^n$ ta chiziqli bog'liqsiz tenglamalar mavjud.

Demak, ushbu teoremaga ko'ra *sxs* o'lchamli S – blok akslantirishi uchun chiziqli bog'liqsiz tenglamalar soni $r \geq t-2^s$ tani tashkil etadi.

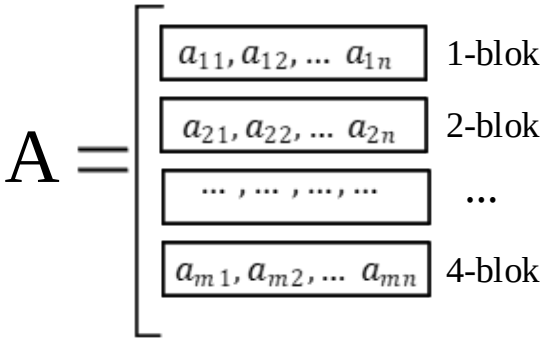
Ushbu bosqich natijasida hosil qilingan tenglamalar soni kriptoanalizning keyingi bosqichi uchun har doim ham yetarli bo'lmaydi. Ularga qo'shimcha ravishda boshqa tenglamalarni, tenglama tuzishning yuqorida keltirilgan usulidan farqli tarzda tuzish mumkin. Bu jarayon, qaralayotgan akslantirish xususiyatiga ko'ra turli yondashuvlar asosida amalga oshiriladi.

2.2. Simmetrik blokli shifrlash algoritmlariga nisbatan integral kriptotahlil usuli

Integral kriptoanaliz usulini biror-bir blokli simmetrik shifrlash algoritmiga qo'llash uchun, tanlab olingan ochiq matnlar va ularga mos shifrmatnlarning maxsus to'plami hamda shifrlash algoritmi ma'lum bo'lishi lozim.

Kriptoanaliz uchun ochiq matnlar to'plamini (A) tanlash quyidagi tartibda amalga oshiriladi (4.14-rasm).

Ushbu rasmda, *m* – tanlab olinuvchi bloklar soni va $m=2^N$, *N* – a_{ij} elementni bitlar soni, *n* – qaralayotgan algoritm kiruvchi blok uzunligiga bog'liq.



4.14-rasm. Ochiq matnlar to'plami

Ushbu A – ochiq matnlar to'plami quyidagicha aniqlanuvchi *aktiv* va *passiv* elementlardan tashkil topishi kerak, ya'ni:

– agar $j=1..n$ uchun $a_{1,j} \neq a_{2,j} \neq a_{3,j} ... \neq a_{m,j}$ bajarilsa, ochiq matnlardagi $a_{i,j}$ *(i=1…m, j=const)* elementlar *aktiv elementlar* hisoblanadi;

– agar $j=1..n$ uchun $a_{1,j}=a_{2,j}=a_{3,j}...=a_{m,j}$ bajarilsa, ochiq matnlardagi $a_{i,j}$ *(i=1…m, j=const)* elementlar *passiv elementlar* hisoblanadi.

1. **Teorema.** Ushbu tanlab olingan A – ochiq matnlar to‘plami elementlari uchun quyidagi tenglik o‘rinli:

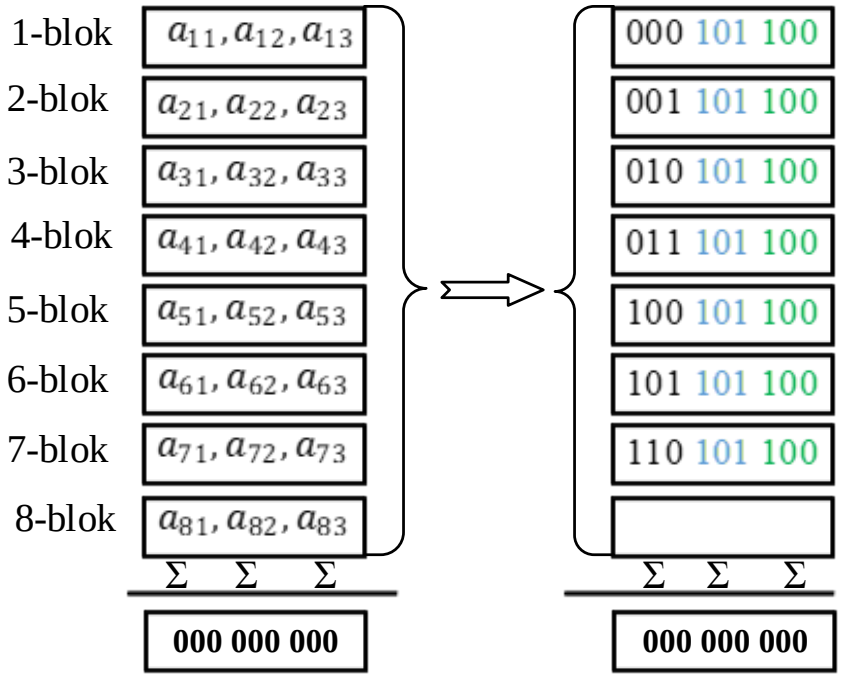
$$\sum_{i=1}^{m} a_{ij} \qquad (4.22)$$

bu yerda *j=1,2,3,…, n.*

Ochiq matnlar to‘plamini tanlab olishni quyidagi misolda ko‘rishimiz mumkin.

Aytaylik a_1, a_2, a_3, a_4 – biror shifrlash algoritmi uchun kiruvchi blok hamda a_i – yarim bayt (bitlar soni 4 ta) bo‘lsin, u holda tanlab olinuvchi bloklar soni 16 ta ($m=2^4=16$) bo‘ladi.

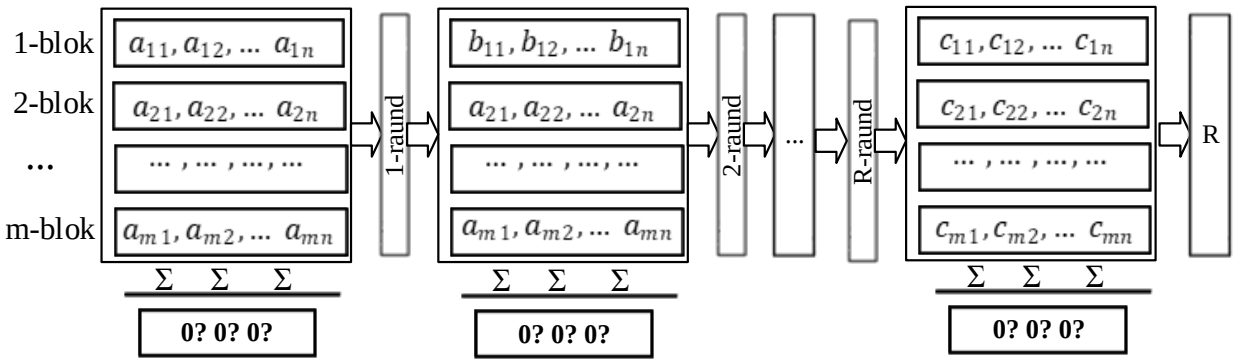
Ushbu bloklarni yuqoridagi talablar asosida quyidagicha shakllantirish mumkin (4.15-rasm):



4.15-rasm. Ochiq matnlar to‘plami

Ushbu tanlab olingan ochiq matnlar to‘plami uchun yuqoridagi teorema shartlari qanoatlantiradi. Ya’ni, har bir ochiq matnlar blokining mos elementlari yig‘inidisi (*XOR*) nolga teng bo‘ladi. Shuningdek, ushbu ochiq matnlar to‘plamida mos ravishda birinchi elementlari aktiv, qolgan elementlari esa mos ravishda passiv elementlar hisoblanadi.

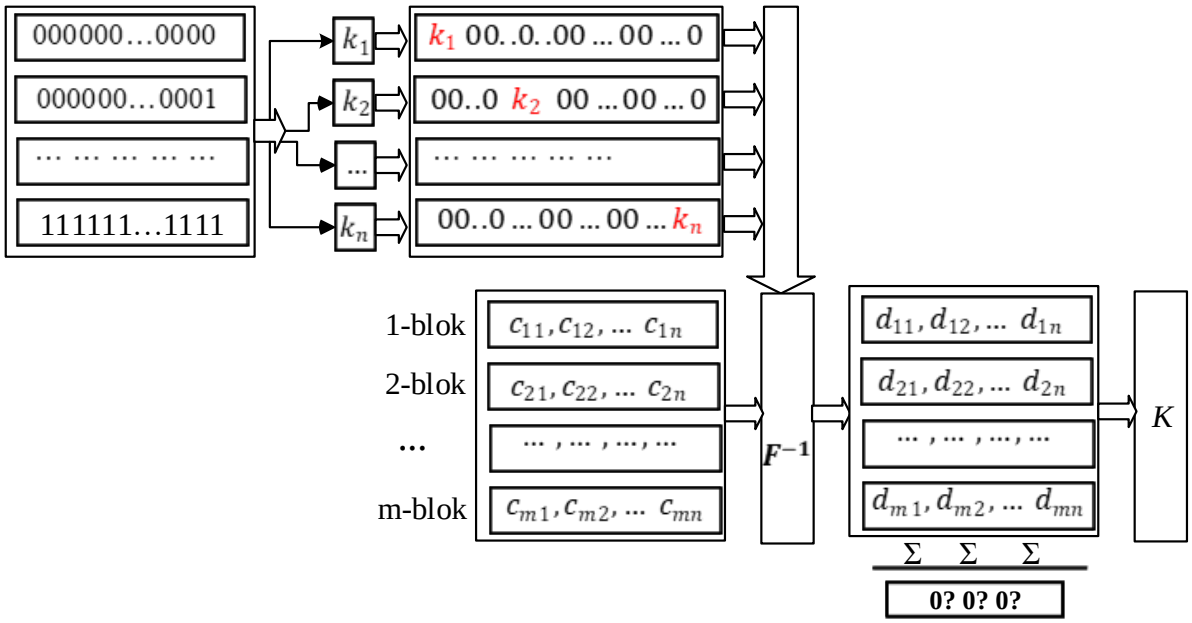
Kriptoanaliz jarayonida, tanlab olingan A to‘plam xususiyatining shifrlash algoritmi raundlaridan o‘tganda qanday o‘zgarishi bo‘yicha tadqiqot olib boriladi (4.16 -rasm). Agar kuzatilayotgan ochiq matnlar to‘plamining biror *R*-raunddan chiqish xolatida balanslashganlik xususiyati buzulib, hamda aktiv yoki passiv baytlar mavjud bo‘lmasa, u holda *R* raundli shifrlash algoritmining so‘ngi raundida foydalanilgan maxfiy kalitni topish imkoniyati tug‘iladi.



4.16-rasm. Ochiq matnlar to‘plamini kuzatish sxemasi

Demak, ochiq matnlar to‘plamini kuzatishda aktiv yoki passiv baytlarning mavjudligi qanchalik ko‘p raundda saqlanib, balanslashganlik xususiyati bajarilsa, shifrlash algoritmining integral kriptoanaliz usuliga kriptobardoshligi ham shu qadar past bo‘ladi.

Shifrlash algoritmining so‘ngi raundida foydalanilgan kalit qiymatini aniqlash esa, so‘ngi raundga kiruvchi to‘plamda aktiv (yoki passiv) bayt mavjudligini hamda so‘ngi raunddan chiquvchi ma’lumotni bilgan holda, statistika o‘tkazish yo‘li orqali amalga oshiriladi. Quyidagi 4.17-rasmda, ushbu jarayonni amalga oshirishning funksional sxemasi keltirilgan.



4.17-rasm. Kalit qiymatini aniqlashning funksional sxemasi

Ya’ni, tanlab olingan ochiq matnlarga mos shifr matnlarni biror tanlab olingan kalit asosida bir raund deshifrlanadi. Agar deshifrlashdan hosil bo‘lgan matnlar uchun yuqoridagi teorema sharti bajarilsa, ushbu kalit nomzod kalitlar ro‘yxatiga qo‘shiladi. Ushbu jarayon, barcha tanlab olingan kalitlar ustida amalga oshiriladi.

Ayni vaqtda standart shifrlash algoritmlari muhim kamchiliklaridan biri ularning real texnik kriptoanaliz usullariga nisbatan bardoshsiz ekanligini ko‘rsatmoqda, xususan “apparat xatoliklarini generatsiyalashga asoslangan kriptoanaliz” usullariga. Bu usulning mohiyati, algoritm akslantirishlarining ma’lum joylaridagi ayrim bitlarini o‘zgartirishga erishish maqsadida, himoya apparatiga issiqlik, yuqori chastotali, ionizatsiyalash va boshqa tashqi ta’sir usullaridan

foydalangan holda ta’sir etishdir. Bunday o‘zgartirish kiritishga asoslangan tahlil usuli ma’lumotni o‘zgartirish kiritilgunga qadar va o‘zgartirilganidan so‘ng ega bo‘lgan ma’lumotlarini solishtirish orqali oxirgi raund kaliti va keyinchalik barcha raund kalitlari to‘g‘risida qiymatlar topishga qaratilgan.

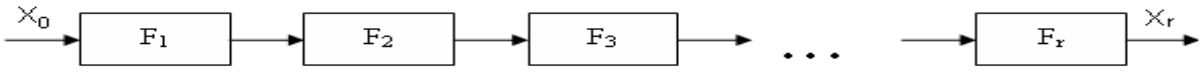
2.3. Simmetrik blokli shifrlash algoritmlariga nisbatan “Slaydli hujum” kriptotahlil usuli

Slaydli hujum kriptoanaliz usuli asosan Feystel tarmog‘iga asoslangan shifrlash algoritmlariga qaratilgan. Agar Feystel tarmog‘i bo‘yicha qurilgan shifrlash algoritmlarining kirishiga n bitli ma’lumot kelib tushadigan bo‘lsa, unda qism kalitning uzunligi $n/2$ bitni tashkil qiladi. Shu bois ham shifrlash algoritmida foydalanilgan maxfiy kalitning uzunligi $n/2$ ni tashkil etadi.

Quyida keltirilgan 4.10-rasmda n bitli x_0 ochiq matnni shifrlash jarayoni ko‘rsatilgan, uning natijasida x_r shifrmatn hosil bo‘ladi. Bu yerda x_j j-chi raundan keyingi berilganlarning oraliq qiymatini belgilaydi, $x_j = F_j(x_{j-1}, k_j),\ j = 1,2,3,...,r$.

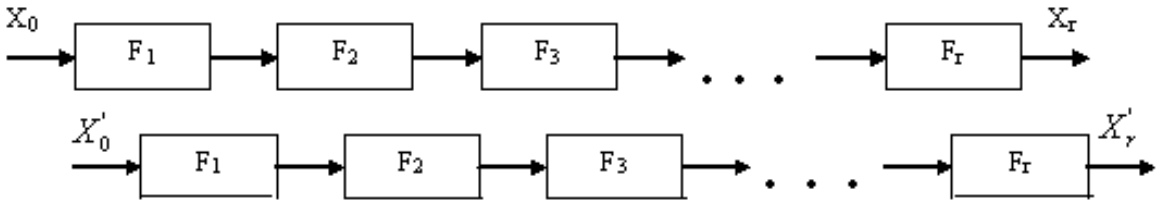
Keyinchalik, ba’zan F funksiyani belgilashda k qiymatni tushurib qoldiramiz $F(x,k)$ yoki $F_j(x,k)$ o‘rniga $F(x)$ yoki $F_j(x)$ deb yozish mumkin.

4.10 - rasm. Oddiy blokli shifrlash algoritmi sxemasi



<u>*Ta’rif.*</u> F funksiya “kuchsiz” deb ataladi, agar ma’lum $F(x_1,k) = y_1$ va $F(x_2,k) = y_2$ ikki tenglikda k kalitni aniqlash oson bo‘lsa.

Quyidagi 4.11- rasmda bunday turdagi shifrlash algoritmlari uchun slaydli hujumni qo‘llanilishi mumkinligi ko‘rsatilgan.



4.11- rasm. Oddiy slaydli hujum sxemasi

Slaydli hujum usulining g‘oyasi shundaki, jarayonlardan birini ikkinchisidan bir raundga kechiktirib, ikkita shifrlash jarayonini o‘zaro mos qo‘yish asos qilib olinadi. Shunday qilib, jarayonlardan biri ikkinchisidan bir raundga ortda qoladi.

Aytaylik, x_0 va $x_0^{'}$ boshlang‘ich ochiq matnlar va ularning mos ketma-ketliklari $x_j = F_j(x_{j-1})$ va $x_j^{'} = F_j(x_{j-1}^{'}),\ j = 1,...,r$ berilgan bo‘lsin.

1. *Tasdiq*. Agar $x_1 = x_0^{'}$ qiymatlar juftligiga ega bo‘linsa, u holda ularga mos $x_r = x_{r-1}^{'}$ qiymatlar juftligiga ham ega bo‘linadi.

Aytaylik, $(P, P^{'})$ - ochiq matnlar, $(C, C^{'})$ - esa ularga mos shifrmatnlar berilgan bo‘lsin.

Ta’rif. (P, C) *va* $(\mathrm{P}^{'}, C^{'})$ juftlik slayd juftlik deyiladi, agar quyidagi shartlar bajarilsa:

– $F(P) = C$, $F(P^{'}) = C^{'}$

– $C = P^{'}$

– $F(P) = P^{'}$, $F(C) = C^{'}$

Agar P ochiq matn F funksiyadan o‘tkazilgandan keyingi natijasi C shifrmatnga , $P^{'}$ ochiq matn F funksiyadan o‘tkazilgandan keyingi natijasi $C^{'}$, hamda birinchi ochiq matnni shifrlash natijasi, ya’ni C shifrmatn, ikkinchi ochiq matn $P^{'}$ ga, ya’ni $C = P^{'}$ teng bo‘lsa, u holda $F(P) = P^{'}$, $F(C) = C^{'}$ bo‘ladi.

Slaydli hujum kriptoanaliz usuli quyidagi tarzda amalga oshiriladi.

$2^{n/2}$ juft (P_i, C_i) ochiq-yopiq matnlar juftligini olanadi va ularning orasidan slaydli juftliklar qidiriladi. Topilgan ochiq-yopiq matnlar orasidan “Tug‘ilgan kunlar” paradoksiga ko‘ra hech bo‘lmaganda bir juft shunday $(i, i^{'})$ indekslar topiladiki, qandaydir qism kalit uchun $F(P_i) = P^{'}{}_i$ va $F(C_i) = C^{'}{}_i$ tengliklar bir vaqtda bajariladi. Slaydli juftlik topilgandan so‘ng, qism kalitning ma’lum bir bitlarini topish mumkin.

Maxfiy kalitning qolgan bitlarini topish uchun keyingi slaydli juftlikni aniqlash va u yordamida tahlil o‘tkazish kerak bo‘ladi. Shunday qilib, maxfiy kalitning bitlarini to‘la aniqlash uchun bir nechta slaydli juftliklarni aniqlash yetarli bo‘ladi. Bu esa kriptotahlilchi oldida turgan murakkab masala hisoblanadi.

Boshlang‘ich berilganlar 4.17-4.20 jadvallarda keltirilgan, ular tahlil qilinayotgan shifrlash algoritmida qo‘llaniladigan kengaytirishli o‘rin almashtirish jadvali, oddiy o‘rin almashtirish va almashtirish jadvalini tashkil etadi. Shuningdek, samarali hujum amalga oshirish uchun slaydli juftlikni aniqlashga yordam beruvchi maska (niqob) jadvali ham berilgan.

4.17-jadval

Kengaytirishli o‘rin almashtirish jadvali

3	1	4	3	2	1	4	2

4.18-jadval

O‘rin almashtirish jadvali

4	2	3	1

4.18-jadval

S1 -blok

	00	01	10	11
00	0	2	1	1
01	1	3	0	2
10	0	3	2	3
11	2	1	3	0

4.19-jadval

S2 -blok

	00	01	10	11
00	0	1	3	2
01	3	2	0	1
10	1	0	1	3
11	3	2	0	2

4.20-jadval

Maska

1	0	1	0

S-DES o‘quv algoritmi Feystel tarmog‘i bo‘yicha qurilgan blokli shifrlash algoritmi bo‘lganligi uchun unga slaydli hujum kriptoanaliz usulini qo‘llash mumkin. Ishni soddalashtirish maqsadida bir xil fiksirlangan 8 bitli K kalitdan foydalaniladi (ya’ni 10 bitli boshlang‘ich kalitdan 8 bitli qism kalitni ajratib olish protsedurasini tushurib qoldiramiz). Boshlang‘ich va yakuniy almashtirishlar tashlab o‘tiladi, chunki ular algoritmning kriptobardoshligiga ta’sir etmaydi. Shuningdek, almashtirishning 2 raundidan emas 20 ta raunddan foydalaniladi, chunki kriptoanalizning bunday ko‘rinishi algoritmda foydalaniladigan raundlar soniga bog‘liq emas.

Mazkur kriptoanaliz usulini o‘tkazish uchun quyidagidalar kerak bo‘ladi:

– $(X, X^{'})$ -ochiq matnlar juftligi;

– $(Y, Y^{'})$ -shifrmatnlar juftligi;

Yuqorida tanlangan maskani kiritib slaydli juftlik ta’rifiga mos keluvchi matnlar juftligi tanlab olinadi. Maska mumkin bo‘lgan slaydli juftliklar oralig‘ini siqib ishni yengillashtirish uchun kiritiladi. Bu shunday matnlar juftliklari bo‘ladiki, birinchi ochiq matnning o‘ngdagi 4 biti ikkinchi ochiq matning chapdagi 4 bitiga teng bo‘ladi, ular esa maskaga teng. Birinchi shifrmatnning chapdagi 4 biti ikkinchi shifrmatning o‘ngdagi 4 bitiga teng.

Quyidagi 4.21-jadvalda 5 juft slaydli juftlik keltirilgan:

4.21-jadval

Slayd juftliklar

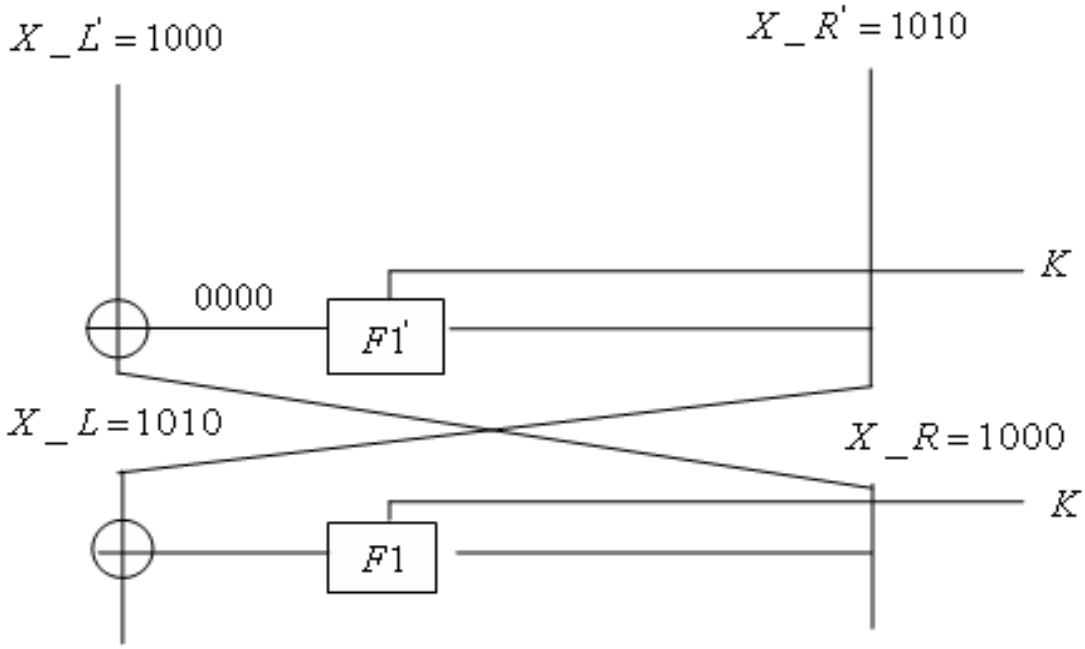
№	**X’**	**Y’**	**X**	**Y**
1	10001010	10111000	10101000	10111011
2	10011010	10011010	10101001	11011001
3	10111010	10111010	10101000	10111011
4	11111010	10011111	10101001	11011001
5	11111010	10011111	10101111	10001001

Topilgan juftliklar tahlilida shifrlash algoritmida foydalanilgan almashtirish jadvali bilan ishlashga to‘g‘ri kelganligi sababli ishni yengillashtirish uchun 4.22-jadvalda ko‘rsatilganidek, almashtirish bloklarining kirish va chiqishi taqqoslanadi:

4.22-jadval

S blok kirishi	**S_1 blok chiqishi**	**S_2 blok chiqishi**
0000	00	00
0001	01	11
0010	10	01
0011	11	10
0100	01	11
0101	00	00
0110	01	01
0111	10	01
1000	00	01
1001	10	11
1010	11	00
1011	10	00
1100	10	01
1101	11	00
1110	11	11
1111	00	10

Matnning birinchi juftini ko‘rib chiqamiz. Buning uchun, 4.12-rasmda ko‘rsatilgan juftlikning birinchi ikki raundini ko‘rib chiqamiz.



4.12-rasm. Birinchi raund birinchi slaydli juftlik tahlili

Birinchi X_R' ochiq matning o‘ng qismi qiymatlari va ikkinchi ochiq matning

chap X_L qism qiymatlari ma’lum bo‘lgani F_1' funksiya kirishi haqida ma’lumot beradi. X_R va X_L' qiymatlar ham ma’lum bo‘lgani uchun F_1 funksiya chiqish qiymatini aniqlash mumkin, u 0000_2 teng bo‘ladi.

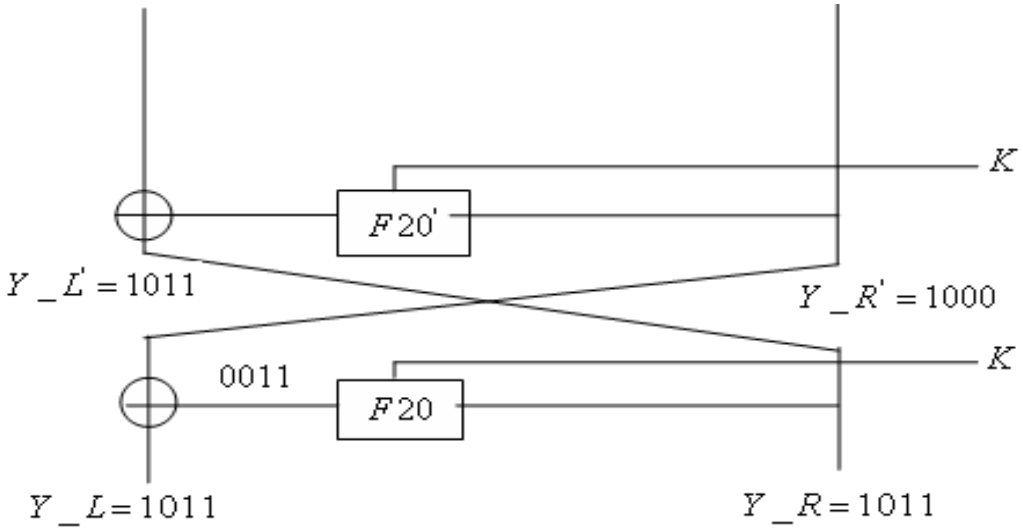
Berilganlar F_1' funksiyadan chiqishdan oldin 4.22-jadvalga muvofiq o‘rin almashsa, bir qadam ortga qaytib, S blok chiqishida 0000_2 qiymat paydo bo‘lishini topamiz, ya’ni 00_2 S_1 blok chiqishi, 00_2 esa S_2 blok chiqishi.

F_1' funksiyaga kiruvchi xabar 4.17-jadvalga muvofiq kengaytirishli o‘rin almashtirishga uchraydi. Demak, 1010_2 kirish 11010100_2 qiymatga o‘zgaradi. Bu esa $K=(k_1,k_2)$ kalitga qo‘shiladi. Shifrlash jarayonida matn ikkita bo‘lakka ajratilib har bir bo‘lagi kalit qismi bilan qo‘shilib keyin esa mos S blok kirishiga kelib tushadi. Biz 8 bitli maxfiy kalitni ikkita k_1 *ва* k_2 4 bitli qism kalitlar yig‘indisi sifatida keltiramiz, ya’ni S_1 blokning $1101\oplus k_1$ kirishi chiqishda 00_2 qiymat beradi. S_2 blokning $0100\oplus k_2$ kirishi esa chiqishda 00_2 qiymat beradi.

Yuqoridagi 4.22-jadvaldan foydalanib, aniqlash mumkinki, 00_2 qiymat S_1 blokning chiqishida hosil bo‘ladi, qachonki kirishga quyidagi $0000_2,0101_2,1000_2$ yoki 1111_2 qiymatlardan biri kirgan bo‘lsa. Shunday qilib, har bir kirishi mumkin bo‘lgan qiymatga 1101_2 ni qo‘shib, k_1 kalitning mumkin bo‘lgan qiymatlarini topamiz. Bular $1101_2,1000_2,0101_2$ yoki 0010_2 qiymatlar bo‘ladi.

Xuddi shu tarzda 00_2 qiymat S_2 blok chiqishida paydo bo‘ladi, qachonki kirishga quyidagi $0000_2,0101_2,1010_2$ yoki 1101_2 qiymatlar kelib tushsa. Demak, har bir kirishi mumkin bo‘lgan qiymatiga 0100_2 ni qo‘shib, k_2 ning mumkin bo‘lgan qiymatlarini olamiz. Bular $0100_2,0001_2,1110_2$ yoki 1001_2 qiymatlar bo‘ladi.

Endi shu slaydli juftlik uchun shifrlashning so‘nggi ikki raundini ko‘rib chiqamiz.



4.13-rasm. So‘nggi raund birinchi slaydli juftlik tahlili

Birinchi shifrmatn Y_L' chap qismi va ikkinchi shifrmatnning Y_R o‘ng qismi

qiymatlarining ma’lumligi $F_{20}^{'}$ funksiyaning kirish qiymati haqida ma’lumot beradi. $Y\_R^{'}$ va Y_L qiymatlar ham ma’lum bo‘lgani uchun, F_{20} chiqish qiymatini aniqlash mumkin, u 0011_2 ga teng bo‘ladi.

Berilganlar $F_{20}^{'}$ funksiyadan chiqishdan oldin 4.22-jadvalga muvofiq o‘rin almashsa, bir qadam ortga qaytib, S blok chiqishida 0011_2 qiymat paydo bo‘lishini topamiz, ya’ni 00_2 S_1 blok chiqishi, 11_2 esa S_2 blok chiqishi.

F_{20} funksiyaga kiruvchi xabar 4.17-jadvalga muvofiq kengaytirishli o‘rin almashtirishga uchraydi. Demak, 1011_2 kirish 11110110_2 qiymatga o‘zgaradi. Bu esa $K=(k_1,k_2)$ kalitga qo‘shiladi. Shifrlash jarayonida matn ikkita bo‘lakka ajratib, xar bir bo‘lagi kalit qismi bilan qo‘shilib, keyin esa mos S blok kirishiga kelib tushadi. Biz 8 bitli maxfiy kalitni ikkita k_1, *ва* k_2 4 bitli qism kalitlar yig‘indisi sifatida keltiramiz, ya’ni S_1 blokning $1111\oplus k_1$ kirish chiqishda 10_2 qiymat beradi. S_2 blokning $0110\oplus k_2$ kirishi esa chiqishda 10_2 qiymat beradi.

Yuqorida berilgan 4.22-jadvaldan foydalanib, 10_2 qiymat S_1 blokning chiqishida hosil bo‘ladi, qachonki kirishga quyidagi $0010_2,0111_2,1001_2$ yoki 1100_2 qiymatlardan biri kirgan bo‘lsa. Shunday qilib, har bir kirishi mumkin bo‘lgan qiymatga 1111_2 ni qo‘shib, k_1 kalitning mumkin bo‘lgan qiymatlarini topamiz. Bular $1101_2,1000_2,0110_2$ yoki 0011_2 qiymatlar bo‘ladi.

Xuddi shu tarzda aniqlash mumkinki 10_2 qiymat S_2 blok chiqishida paydo bo‘ladi, qachonki kirishga quyidagi $0011_2,0110_2,1011_2$ yoki 1111_2 qiymatlar kelib tushsa. Demak, har bir kirishi mumkin bo‘lgan qiymatiga 0110_2 ni qo‘shib, k_2 ning mumkin bo‘lgan qiymatlarini olamiz. Bular $0101_2,0000_2,1101_2$ yoki 1001_2 qiymatlar bo‘ladi.

Shifrlashning barcha raundlarida bir xil kalit ishlatilgani uchun birinchi raundning k_1 qiymati so‘nggi raundning k_1 qiymatiga mos kelishi va birinchi raundning k_1 kalitiga mos kelishi kerak. Keyin k_1,k_2 ning barcha mumkin bo‘lgan qiymatlarini taqqoslab shuni ko‘rishimiz mumkinki, faqat ikkita $k_1=1101_2$ va $k_1=1000_2$ qiymati mavjud, ularni birinchi raundda ham so‘nggi raunda ham qo‘llash mumkin va bitta $k_2=1001_2$ qiymati mavjud. Buni ham birinchi va so‘nggi raundda qo‘llash mumkin. Shunday qilib, qidirilayotgan kalitning ikkita mumkin bo‘lgan qiymati topildi, $K=11011001_2$ va $K=10001001_2$.

Yuqorida K maxfiy kalitning qiymati berilganligi bois olingan ikkita variant bilan taqqoslash natijasida olingan ikkinchisi haqiqiy K maxfiy kalit ekanligi ma’lum bo‘ldi.

2.3. Simmetrik blokli shifrlash algoritmlariga nisbatan apparat xatoliklarni generatsiyalashga asoslangan kriptotahlil usuli

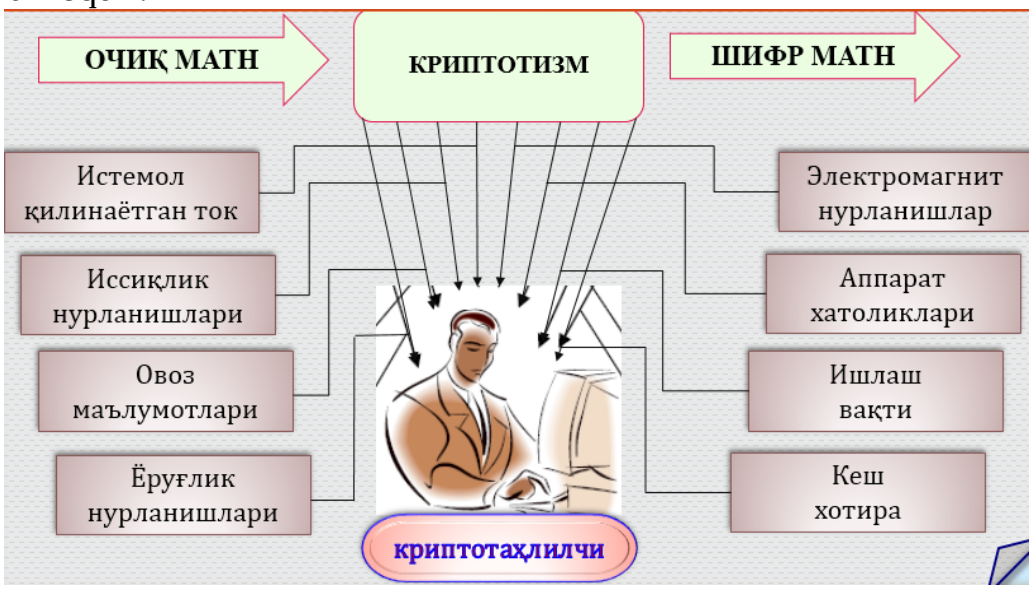
Qo‘shimcha kanallar bo‘yicha kriptotahlil

So‘nggi vaqtlarda kriptotahlilning muhim yo‘nalishlaridan biri, axborotni

kriptografik himoyalash apparat-dasturiy qurilmalarini qo‘llanilishida yuzaga keladigan qo‘shimcha kanallardan va ishchi muhitning alohida xususiyatlaridan foydalanishga qaratilgan hujumga asoslanmoqda. Tashqi yoki qo‘shimcha kanal bo‘yicha hujum – bu tashqi yoki qo‘shimcha kanallardan olingan ma’lumotlardan foydalangan holda olib boriladigan kriptografik hujum turidir. Qo‘shimcha kanallar bo‘yicha olingan ma’lumotlar bu shifrlash qurilmasidan olingan bo‘lishi mumkin bo‘lib, shu bilan birga ochiq matn va yopiq matn ham emasdir.

Amaliyotda kriptotizimlarga nisbatan amalga oshirilgan barcha muvaffaqqiyatli hujumlar, asosan kriptoalgoritm mexanizmlarining amalda qo‘llanilishida yuzaga keladigan zaifliklardan foydalangan holda amalga oshirilgan. Bunday hujum, maxfiy kalitga bog‘liq ravishda hisoblash mashinasining ichki holati va hisoblash jarayonining turli vaqtidagi o‘lchanadigan fizik parametrlari (energiya sarfi, hisoblashga ketgan vaqt, elektromagnit tarqalishlar va h.k.) qiymatlari o‘rtasidagi korrelyatsiyaga asoslangan. Tajribada, qo‘shimcha kanallar bo‘yicha hujum, faqat matematik tahlilga asoslangan ananaviy hujumlarga nisbatan samaraliroq hisoblanadi. Qo‘shimcha kanallar bo‘yicha hujum, hisoblash mashinasiga kiritilgan, maxfiy parametrlarni chiqarib olish uchun kriptografik himoyalash apparat-dasturiy qurilmalari qo‘llanilishining o‘ziga xos xususiyatlaridan foydalanadi (implementation attacks).

Bunday yondashuv, kriptografik algoritmlarning apparat-dasturiy qurilmalaridan foydalanish bilan bevosita bog‘liq bo‘lganligi uchun kamroq umumlashgan bo‘lsada, mavjud klassik kriptotahlil usullariga nisbatan qisman samaraliroqdir.



1.2.1 – rasm. Qo‘shimcha kanallar bo‘yicha kriptotahlil.

Qo‘shimcha kanallar bo‘yicha hujum quyidagi uch tur bo‘yicha klassifikatsiyalanadi:

- hisoblash jarayoni ustidan nazorat qilish bo‘yicha: aktiv va passiv;
- kriptomodulga ruxsat olish bo‘yicha: agressiv (invasive), yarimagressiv (semi - invasive) va noagressiv (non- invasive);
- tahlil jarayonida qo‘llanilish usuli bo‘yicha: oddiy – simple side channel attack (SSCA) va har-xil – differential side channel attack (DSCA).

Hozirgi kunda o‘ndan ortiq qo‘shimcha kanallar aniqlangan. Hujumlar, foydalanilayotgan qo‘shimcha kanallarning turiga ko‘ra farqlanadi (1.2.1- rasm): jarayonga sarflanayotgan vaqt bo‘yicha hujum (Timing Attacks), energiya sarfi bo‘yicha hujum (Power Analysis Attacks), apparat xatoliklari bo‘yicha hujum (Fault Attacks), elektromagnit nurlanishlar bo‘yicha hujum (ElectroMagnetic Analysis), aloqa kanalidagi xatolik bo‘yicha hujum (Error Message Attacks).

Bundan tashqari, kesh-xotira bo‘yicha (Cache-based Attacks), akustik (Acoustic Attacks), yorug‘lik nurlanishi bo‘yicha hujum (Visible Light Attacks) kabi turlari ham mavjud.

Vaqt bo‘yicha hujum

Vaqt bo‘yicha hujum bu – foydalanuvchi kriptografik operatsiyalarni bajarish jarayonida, vaqtni aniq o‘lchash orqali maxfiy ma’lumotga ega bo‘lishdir. Bu qo‘shimcha kanal bo‘yicha hujumning kriptografiyada paydo bo‘lgan dastlabki turlaridan biri hisoblanadi. Kriptotizimlarda ma’lumotlarni qayta ishlash vaqti ko‘p hollarda kirish qiymati (masalan, ochiq va yopiq matn)ga qarab biroz o‘zgarishi mumkin. Vaqt bo‘yicha hujum, shifrlash modulining kerakli shifrlash operatsiyasining bajarish uchun ketgan vaqtni o‘lchab borishga asoslangan bo‘lib, maxfiy kalitlar bo‘yicha ma’lumotlarning ochilishiga olib kelishi mumkin. Masalan: maxfiy kalit bilan ishlash operatsiyasini bajarish uchun ketgan vaqtni aniq o‘lchash orqali, kriptotahlilchi Diffi-Xelmman algoritmining eksponenta aniq qiymatini topishi mumkin.

Ta’kidlash joizki, vaqt bo‘yicha hujum, RSA algoritmining maxfiy kalitini, kriptografik operatsiyalarni amalga oshirishga ketgan vaqtni ma’lum bir intervalda o‘lchash orqali tiklab olish mumkinligi 1995 yilda bir qancha shov-shuvlarga sabab bo‘lgan. Bu turdagi hujumlar mikroprotsessorli kartochkalar va boshqa idintifikatsiyalash vositalari, shuningdek tarmoqdagi elektron tijorat serverlariga muvoffaqiyatli qo‘llanilgan.

Quvvat bo‘yicha tahlil

Quvvat bo‘yicha tahlil kriptografik vositalarning apparat vositalari uchun foydaliroqdir va tarkibida maxfiy kalitlarni saqlovchi smart-karta va boshqa tizimlarni ochishda muvoffaqiyatli qo‘llaniladi.

Quvvat istemolini o‘lchash uchun, tarmoq zanjiriga yoki yerga ulanishga ketma-ket ravishda kichik qarshilikli (masalan 50 Om) rezistorlarni ulash kerak bo‘ladi. Quvvatning kamayishini, qarshilikka bo‘lsak, tok kuchini beradi. Zamonaviy laboratoriyalar bugungi kunda, quvvatning o‘ta yuqori chastotalarida (1 GGts) ham yuqori aniqlikda (1 % xatolik bilan) o‘lchash qurilmalariga ega.

Ta’kidlash joizki, qo‘shimcha kanallardan foydalanishda quvvatning o‘zgarishi – tahlil uchun yaxshi vositalardan biri hosoblanashi bilan birga juda kam xarajatli hisoblanadi.

Apparat xatoliklari bo‘yicha tahlil

Kriptografik modulning ishlash jarayonida vujudga keladigan apparat ta’minotidagi xatoliklar yoki xatoli chiqish bloklari qo‘shimcha kanallar uchun muhim bo‘lishi va ba’zan shifrlarning mavjud kriptotahlil usullariga nisbatan bardoshsizligini sezilarli oshirishi mumkin.

Apparat xatoliklariga asoslangan kriptotahlil – kriptotahlilchi shifrlash

qurilmasiga tashqi fizik ta’sir o‘tkaza olishi va ma’lum bir blok ma’lumotni shifrlash jarayonida bir xildagi xatoliklarni generatsiya qilish imkoniyatiga egaligiga asoslanadi. Kriptografik algoritmlarga xatoliklar bo‘yicha hujum 1996 yildan boshlab o‘rganib kelinayotgan bo‘lib, shu paytga qadar deyarli barcha shifrlash algoritmlariga mazkur turdagi hujum qullanilgan.

Apparat xatoliklarining samaradorligi kriptotahlilchining tizimda maxsus xatolikni amalga oshira olish yoki tabiiy xatoliklardan foydalana olish imkoniyatiga bog‘liq bo‘ladi.

Bu turdagi hujumga bardoshlilik masalasi ayniqsa intelektual elektron kartochkalarida qo‘llaniladigan shifratorlar uchun muhimdir.

Xatoliklar quyidagi jihatlari bo‘yicha klassifikatsiyalanadi:

- kriptotahlilchi kriptografik modulning ishlash jarayonida vujudga keladigan xatolikning vaqtini va joyini tanlashdagi aniqlik;
- ta’sir etayotgan xatolikning uzunligi: masalan faqat, bir bit;
- xatolikning davomiyligi: xatolik qisqami yoki davomiy;
- xatolik turi: bir bitning o‘zgarishi; bitning, faqat bir tomonlama (masalan 1 dan 0 ga); bitni ixtiyoriy qiymatga o‘zgarishi va h.k..

Umuman olganda, kriptografik modulga yoki qurilmaga nisbatan xatolikni samarali amalga oshirish ikki qadamdan iborat: xatolikni hosil qilish va bu xatolikdan foydalanish.

Mazkur hujum usuli asosan nazariy jixatdan o‘rganilgan bo‘lib barcha shifrlash tizimlariga nisbatan qo‘llanilgan.

Jumladan, GOST 28147-89, DES va RC6 shifrlash algoritmlariga nisbatan apparat xatoliklarning generatsiyasiyaga asoslangan hujum amalga oshirilgan.

Elektromagnit nurlanishlar bo‘yicha hujum

Kompyuterda hisoblash operatsiyalarini amalga oshirish jarayoni elektromagnit nurlanishlar bilan bevosita bog‘liq. Mazkur nurlanishlarni o‘lchash va tahlil qilish orqali, kriptotahlilchi hisoblash jarayonlari va foydalanilayotgan ma’lumotlar to‘g‘risida yetarlicha axborot olishi mumkin. Elektromagnit nurlanishlar bo‘yicha tahlil ham ikki turga bo‘linishi mumkin: ya’ni oddiy – simple (SEMA) va har-xil – differential (DEMA).

Nazariy savollari:

1. Chiziqli kriptoanaliz usulining mohiyatini tushuntirib bering
2. TDES algoritmi qanday maqsadlarda ishlatiladi?
3. Simmetrik blokli shifrlash algoritmlariga differensial kriptoanaliz usuli qanday qo‘llaniladi?
4. Chiziqli-differensial kriptoanaliz usuli qanday amalga oshiriladi?
5. “Slaydli hujum” kriptoanaliz usulini tushuntirib bering
6. Algebraik kriptoanaliz usuli nimaga asoslanadi?
7. Simmetrik blokli shifrlash algoritmlari uchun integral kriptoanaliz usuli qanday amalga oshiriladi?

Adabiyotlar va internet resurslar:

1. Xasanov P.F., Xasanov X.P., Axmedova O.P., Davlatov A.B. Kriptotahlil va

uning maxsus usullari, O‘quv qo‘llanma, Toshkent, 2010
2. Akbarov D.YE. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanishlari. Toshkent. ”O‘zbekiston markasi“, 2009
3. Л.К.Бабенко, Е.А.Ищукова. Современные алгоритмы блочного шифрования и методы из анализа: учеб. пособие для студентов вузов, обучающихся по группе специальностей в обл. информ. безопасности – М.: Гелиос АРВ, 2006. – 376 с.
4. M.Stamp. Applied cryptanalysis: Breaking Ciphers in the Real World. John Wiley & Sons, Inc, 2007, -P. -417.
5. Б.Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – Москва: ТРИУМФ, 2002.
6. Xasanov P., Xasanov X., Axmedova O., Davlatov A. Kriptotahlil va uning maxsus usullari. O‘quv qo‘llanma.– Toshkent, 2010.
7. O.P.Axmedova, Z.T.Xudoykulov, O. Allanov, I.M.Boyquziyev Kriptoanaliz. O‘quv qo‘llanma. T.: “Iqtisod-Moliya”, 2022. 171 b.
8. Kuryazov D.M., Sattorov A.B., Axmedova B.B. Blokli simmetrik shifrlash algoritmlari bardoshligini zamonaviy kriptotahlil usullari bilan baholash. O‘quv qo‘llanma. T.: “Aloqachi”. 2017, 228 bet.
9. http://jnicholl.org/Cryptanalysis/Tools/
10. https://www.cryptool.org/en/cto/
11. https://resources.infosecinstitute.com/topic/cryptanalysis-tools/
12. http://rumkin.com/tools/cipher/
13. https://blackarch.org/crypto.html
14. https://www.guballa.de/vigenere-solver
15. https://www.simonsingh.net/The_Black_Chamber/substitutioncrackingtool.html
16. https://www.guru99.com/how-to-make-your-data-safe-using-cryptography.html
17. https://www.cs.bu.edu/~goldbe/teaching/CS558S17/Lab1.pdf

4-ma’ruza. Asimmetrik kriptotizimlarni kriptotahlil qilish usullari.

Reja:

2.1. Faktorlash muammosining murakkabligiga asoslangan kriptotizimlarning bardoshliligi.
2.2. Diskret logorifmlash muammosining murakkabligiga asoslangan kriptotizimlarning bardoshliligi.

Tayanch iboralar: *asimmetrik algoritmlar, ochiq kalitli tizimlar, faktorlash muammosi, eksponensial murakkablik, sub-eksponensial murakkablik, chekli maydon*

2.1. Faktorlash muammosining murakkabligiga asoslangan kriptotizimlarning bardoshliligi.

Faktorizatsiyalash muammosi sonni tub ko’paytuvchilarga ajratish muammosi hisoblanib, kichik sonlarda bu muammoni hal qilish unchalik katta vaqt va xarajat talab qilmasligi mumkin, lekin yetarlicha katta sonlarda bu ishni amalga oshirish uchun juda ko’p vaqt va xarajat talab qilinadi. Bizga ma’lumki kriptografiyada, ayniqsa ochiq kalitli kriptotizimlarda asosiy amallar tub sonlar ustida amalga oshiriladi. Bunda tub sonlarning o’ziga xos xususiyatlaridan foydalanish kriptotizimning ishonchliligi va bardoshliligini ta’minlab beradi. Misol uchun RSA ochiq kalitli shifrlash algortimni olsak, unda ikkita p va q tub sonlar olinib N = p * q hisoblanadi. So’ngra Eyler funksiyasi yordamida φ(N) = (p -1) * (q – 1) hisoblanib, ixtiyoriy e (1 < e < N) soni tanlab olinadi va kengaytirilgan Yevklid algoritmiga ko’ra, e * d = 1 mod(φ(N)) tenglikni qanoatlantiruvchi d soni topiladi. Shunda (e, N) sonlar juftligi ochiq kalitni, (d, N) sonlar juftligi esa maxfiy kalitni tashkil qiladi. Ma’lumotlar hammaga ma’lum bo’lgan ochiq kalit yordamida shifrlanib, faqatgina qabul qiluvchiga ma’lum bo’lgan maxfiy kalit yordamida rasshifrovka qilinadi. Bu shuni anglatadiki, (d, N) maxfiy kalitni bilgan har qanday odam shifrmatnni rasshifrovka qilib, ochiq matnga ega bo’ladi. Bunda maxfiy kalit hammaga ma’lum bo’lgan ochiq kalit yordamida hisoblab topilishi mumkin. Buning uchun buzg’unchi (e, N) ochiq kalitdagi N sonini ikkita sonning ko’paytmasi shaklida ifodalashi kerak, shundan so’ng Eyler funksiyasi yordamida φ(N) ni hisoblab, undan so’ng Kengaytirilgan Yevklid algoritmi yordamida maxfiy kalit (d, N) ga ega bo’ladi. Buning uchun u N sonini tub ko’paytuvchilarga ajratishi lozim. RSA algoritmi aynan shu faktorizatsiya muammosiga asoslanadi. Yuqorida aytib o’tganimizdek, N ning qiymati kichik bo’lgan hollarda buning hech qanday qiyinchiligi yo’q. Lekin yetarlicha katta qiymatlarda bu ishni amalga oshirish juda katta vaqt va xarajat talab qiladi. Demak faktorizatsiyalash muammosi butun tizimning bardoshliligini ta’minlab berar ekan.

Faktorizatsiya muammosi hal qiluvchi algoritmlar ikki guruhga bo’linadi:

- Eksponensial turdagi algoritmlar
- Sub-eksponensial turdagi algoritmlar

Eksponensial turdagi algoritmlar, muammoni hal qilishda katta vaqt va xarajat talab qiladigan yechimlarni topishda yordam beradi. Bu usul, sonni tub ko’paytuvchilarga ajratish uchun har bir imkoniyatli bo'lim bo'yicha hisoblashni o'z ichiga oladi. Ammo, bu guruhdagi usullarning katta vaqt va xarajatga ega bo'lishi sababli, katta sonlarda foydali emas. Misol uchun, 512 bitlik sonni tub ko’paytuvchilarga ajratish kerak bo’ladi, ammo ishni eksponensial turdagi algoritmlar bilan hal qilish uchun katta vaqt va xarajat talab qiladi.

Sub-eksponensial turdagi algoritmlar esa, eksponensial turdagi algoritmlardan ko’ra ko'p vaqt va xarajatga ega bo'lmagan yechimlar topishda yordam beradi. Bu usulda, faktorizatsiyaga yordam beruvchi bir necha yuqori darajali matematik funksiyalar va hisoblash texnologiyalari ishlatiladi. Sub-eksponensial turdagi algoritmlar 100 bitdan katta sonlarni tub ko’paytuvchilarga ajratishda yuqori samaradorlikka ega bo'lgan algoritmlar hisoblanadi.

RSA kriptotizimi protokolining zaif tomonlaridan foydalanishga asoslangan hujumlar

RSA algoritmi yordamida qo‘yilgan imzoga hujum

Boshlang‘ich shartlar: Undan o‘tadigan hujjatlarni imzolovchi elektron xizmat bor deb tasavvur qilamiz. N – bu xizmat imzolashni rad etayotgan ochiq matn. Kriptoanalizchiga xizmatning ochiq kaliti (e, n) ma’lum.

Qo‘yilgan masala: N matnini imzolash.

Kriptoanalizchi N bilan o‘zaro tub bo‘lgan ma’lum bir tasodifiy son x ni tanlaydi va $y = xe\ (mod\ n)$ ni hisoblaydi. So‘ngra $M = yN$ qiymatni oladi va xizmat ga imzolash uchun jo‘natadi. Xizmat esa uni imzolaydi $M^d(modn) = S$ (chunki, u endi N emas), ya’ni $S = M^d(mod\ n) = y^d N^d = (x^e)^d N^d = xN^d$, demak $N^d = Sx^{-1}(modn)$, ya’ni faqatgina S ni x ga bo‘lish kifoya.

Himoya qilish: Imzo qo‘yish vaqtida ma’lumotga biron-bir tasodifiy son (masalan, vaqt momenti) qo‘shish lozim. Shu orqali M sonining buzilishi ro‘y beradi, ya’ni $M_{(qo‘shilgandan\ so‘ng)} + yN$.

Tanlangan shifrmatn bo‘yicha RSA algoritmidan foydalanib qo‘yilgan imzoga hujum

Boshlang‘ich shartlar: C shifrmatni mavjud. Kriptoanalizchiga jo‘natuvchining ochiq kaliti (e, n) ma’lum.

Qo‘yilgan masala: Ochiq matn M ni topish.

Kriptoanalizchi qandaydir r ni tanlaydi: $r < n, (r, n) = 1$ va $x = r^e(mod\ n)$ ni hisoblaydi. So‘ngra u $t = r^{-1}(mod\ n)$ va $y = xC(mod\ n)$ hisoblaydi va y ni jo‘natuvchi imzolashi uchun jo‘natadi.

Jo‘natuvchi hech narsadan shubhalanmay y matnni imzolaydi: $w = y^d(mod\ n)$ va w qaytarib jo‘natib yuboradi.

Kriptoanalizchi $tw(modn) = r^{-1}y^d(modn) = (r = x^d modn$ bo‘lgani uchun) $= x^{-d}x^dC^d(mod\ n) = C^d = M$ M ni topadi.

Kriptoanalizchi C ni birdaniga imzolash uchun yubora olmaydi, chunki jo‘natuvchi imzolashdagi natijalarni tekshirayotgan bo‘lishi va sezib qolishi mumkin.

Ushbu hujum ko‘p gipotetik xususiyatga ega emas, lekin shunga qaramay, quyidagicha bir nechta xulosalar chiqarish imkonini beradi:

a) imzolash va shifrlashni turli xil kalitlarda amalga oshirish lozim;

imzolash paytida tasodifiy vektor qo‘shish lozim yoki xeshlash funksiyasidan foydalanish lozim.

2.2. Diskret logorifmlash muammosining murakkabligiga asoslangan kriptotizimlarning bardoshliligi.

Diskret logorifmlash muammolari, matematika va kriptografiya sohalarida keng qo‘llaniladigan bir muammo turidir. Bu muammo biror modul bo‘yicha diskret yechimni hisoblashni talab qiladi. Diskret logorifmlash muammosi bir qancha maqsadlarda foydalaniladi, ma’lumotlarni himoyalash, shifrlash va deshifrlash.

Diskret logorifmlashning asosiy maqsadi, ma’lum bir gruppada berilgan sonning qanday darajasi berilgan boshqa songa tengligini aniqlashga qaratilgan. Ya’ni:

$$a^x \equiv b\ mod\ p$$

tenglikda x noma'lumni topishga qaratilgan. Bu yerda $p-G$ guruh tartibi, a – guruh generatori, b – guruh elementi.

Diskret logorifmlash muammosini yechishda, ya'ni x noma'lumni topish uchun bir nechta algoritmlar mavjuddir, ba'zi bir modullar bo'yicha hisoblash amaliy jihatdan imkonsiz deb hisoblanadi, ba'zida esa nisbatan tez yechim topishni ta'minlaydi. Shu sababli, kriptografiyada, bir moduldan tashqari yechim topish mumkin bo'lgan algoritmlardan foydalaniladi, bu esa shaxslarning ma'lumotlarini himoyalashga yordam beradi.

Diskret logorifmlash, bugungi kunda ma'lumotlar himoyalanishida katta ahamiyatga ega bo'lib, xususan, kredit kartalari va bank hisob varaqlari kabi shaxsiy ma'lumotlar va shaxsiy identifikatsiyada amalga oshirishda qo'llaniladi. Shuningdek, kriptovalyuta yaratish va uning operatsiyalari ham diskret logorifmlash murakkabligiga asoslangan. Shuningdek, xabarlar zanjirli tizimi (blockchain) ham diskret logorifmlash murakkabligiga asoslangan.

Diskret logorifmlash muammosini yechish uchun bir qancha algoritmlar ma'lum. Biz algoritmlarni ikkita toifaga ajratamiz, ***umumiy algoritmlar*** va ***guruhga xos*** algoritmlar. Birinchi toifani biz umumiy algoritmlar deb ataymiz, chunki ular odatda har qanday siklik guruhga nisbatan qo'llaniladi. Umumiy algoritm umumlashtirilgan diskret logorifmlash muammosini (GDLP) hal qiladi. Algoritmlarning ikkinchi toifasi guruhga xos algoritmlardir. Bular guruh elementlaridagi strukturadan foydalanadigan va faqat ma'lum guruhlar oilalarida qo'llaniladigan maxsus algoritmlardir.

Biz ko'rib chiqadigan umumiy algoritmlarga Shank algoritmi kiradi, bu algoritm Baby-Step Giant-Step algoritmi, Pollardning Rho va Pollardning Kangaroo algoritmlari deb ham ataladi. Bu algoritmlar har qanday siklik guruhga, shu jumladan elliptik egri guruhlarga va Z_p^* ning kichik guruhlariga nisbatan qo'llaniladi, bu yerda yaxshiroq usullar qo'llanilmaydi. Biz muhokama qiladigan guruhga xos algoritmlar indekslarni hisoblash algoritmlaridir. Ular Z_p^* guruhlarida qo'llaniladi. Shuning uchun indekslarni hisoblash algoritmlari standart diskret logorifmlash muammosini (DLP) hal qiladi.

Diskret logorifmlash muammosini yechuvchi algoritmlarni ***Big O notation*** yordamida, nazariy jihatdan ish vaqti murakkabligini o'lchaymiz.

Algoritmni ishga tushirish uchun zarur bo'lgan aniq vaqt, vaqt murakkabligi haqida to'liq tasavvurga ega bo'lish uchun yetarli ma'lumot emas. Ushbu muammoni hal qilish uchun siz Big O dan foydalanishingiz mumkin. Big O ko'pincha turli ilovalarni solishtirish va qaysi biri eng samarali ekanligini aniqlash uchun ishlatiladi, keraksiz tafsilotlarni o'tkazib yuboradi va algoritmning ishlash vaqtida nima muhimligiga e'tibor beradi.

Turli xil algoritmlarni ishga tushirish uchun zarur bo'lgan soniyalar vaqtiga bir nechta bog'liq bo'lmagan omillar, jumladan protsessor tezligi yoki mavjud xotira ta'sir qilishi mumkin. Boshqa tomondan, Big O apparat diagnostikasi nuqtai nazardan ish vaqtining murakkabligini ifodalash uchun platformani taqdim etadi. Big O bilan siz algoritmingizning ishlash vaqti kirish hajmiga nisbatan qanchalik tez o'sishi nuqtai nazaridan murakkabligini ifodalaysiz.

Agar n algoritmga kirish hajmi deb faraz qilsak, Big O n va algoritm yechim topish uchun bajaradigan qadamlar soni o‘rtasidagi munosabatni ifodalaydi. Big O bosh harfi “O” dan keyin qavslar ichidagi bu munosabatdan foydalanadi. Masalan, O(n) ularning kiritish hajmiga mutanosib ravishda bir necha bosqichlarni bajaradigan algoritmlarni ifodalaydi.

Big O	**Complexity (Murakkablik)**	**Tavsif**
$O(1)$	*constant (doimiy)*	Ish vaqti kirish hajmidan qat’iy nazar doimiydir. Xesh jadvalidagi elementni topish *doimiy vaqt* ichida bajarilishi mumkin bo‘lgan operatsiyaga misoldir.
$O(n)$	*linear (chiziqli)*	Ish vaqti kirish hajmiga qarab *chiziqli* ravishda o‘sadi. Ro‘yxatning har bir bandidagi shartni tekshiradigan funksiya $O(n)$ algoritmiga misol bo‘la oladi.
$O(n^2)$	*quadratic (kvadratik)*	Ish vaqti kirish hajmining *kvadratik* funktsiyasidir. Har bir element ikki marta tekshirilishi kerak bo‘lgan ro‘yxatdagi takroriy qiymatlarni topishning sodda amalga oshirilishi kvadratik algoritmga misoldir.
$O(2^n)$	*exponential (ko‘rsatkichli)*	Ish vaqti kirish hajmi bilan *eksponent* ravishda o‘sadi. Ushbu algoritmlar juda samarasiz deb hisoblanadi.
$O(logn)$	*logarithmic (logorifmik)*	Ish vaqti *chiziqli* ravishda o‘sadi, kirish hajmi esa *eksponent* ravishda o‘sadi. Misol uchun, ming elementni qayta ishlash uchun bir soniya kerak bo‘lsa, o‘n mingni qayta ishlash uchun ikki soniya, yuz mingni qayta ishlash uchun uch soniya va hokazo. Ikkilik qidiruv logorifmik ish vaqti algoritmiga misoldir.

Nazariy savollari:

1. Diskret logorifmlash muammosi nima?
2. Diskret logorifmlash muammosining kriptografiyadagi ahamiyati qanday?
3. Chekli gruppada diskret logarifmlash qanday hisoblanadi?
4. Dikson usuli nechta bosqichda amalga oshiriladi? Unda qaysi algebraik amallardan foydalaniladi?
5. Kvadratik g‘alvir usulining Dikson usuliga o‘xshash tomonlari nimada?
6. Xizmat li sxemada ishlatilgan RSA algoritmi yordamida qo‘yilgan imzoga hujum qanday uyushtiriladi va hujumdan qanday himoyalanish mumkin?
7. Tanlangan shifrmatn bo‘yicha RSA algoritmidan foydalanib qo‘yilgan imzoga hujum qanday uyushtiriladi?

Adabiyotlar va internet resurslar:

1. Xasanov P.F., Xasanov X.P., Axmedova O.P., Davlatov A.B. Kriptotahlil va

uning maxsus usullari, O‘quv qo‘llanma, Toshkent, 2010
2. Akbarov D.YE. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanishlari. Toshkent. ”O‘zbekiston markasi“, 2009
3. Л.К.Бабенко, Е.А.Ищукова. Современные алгоритмы блочного шифрования и методы из анализа: учеб. пособие для студентов вузов, обучающихся по группе специальностей в обл. информ. безопасности – М.: Гелиос АРВ, 2006. – 376 с.
4. M.Stamp. Applied cryptanalysis: Breaking Ciphers in the Real World. John Wiley & Sons, Inc, 2007, -P. -417.
5. Б.Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – Москва: ТРИУМФ, 2002.
6. Xasanov P., Xasanov X., Axmedova O., Davlatov A. Kriptotahlil va uning maxsus usullari. O‘quv qo‘llanma.– Toshkent, 2010.
7. O.P.Axmedova, Z.T.Xudoykulov, O. Allanov, I.M.Boyquziyev Kriptoanaliz. O‘quv qo‘llanma. T.: “Iqtisod-Moliya”, 2022. 171 b.
8. Kuryazov D.M., Sattorov A.B., Axmedova B.B. Blokli simmetrik shifrlash algoritmlari bardoshligini zamonaviy kriptotahlil usullari bilan baholash. O‘quv qo‘llanma. T.: “Aloqachi”. 2017, 228 bet.
9. http://jnicholl.org/Cryptanalysis/Tools/
10. https://www.cryptool.org/en/cto/
11. https://resources.infosecinstitute.com/topic/cryptanalysis-tools/
12. http://rumkin.com/tools/cipher/
13. https://blackarch.org/crypto.html
14. https://www.guballa.de/vigenere-solver
15. https://www.simonsingh.net/The_Black_Chamber/substitutioncrackingtool.html
16. https://www.guru99.com/how-to-make-your-data-safe-using-cryptography.html
17. https://www.cs.bu.edu/~goldbe/teaching/CS558S17/Lab1.pdf

5-ma’ruza. Xesh funksiyalarning kriptotahlili, Psevdotasodifiy va tasodifiy sonlar generatorlarining tahlilli.

Reja:

2.1. Tug‘ilgan kun muammosi.
2.2. MD4 va MD5 algoritmlarining kriptotahlili.
2.3. NIST va DIEHARD statistik testlar to‘plami.

Tayanch iboralar: *Tug‘ilgan kun muammosi, kolliziya, MD4, MD5, PTSG, NIST, Diehard*

2.1. Tug‘ilgan kun muammosi.

Agar kriptoalgoritmning maxfiy kalitlar to‘plami kompozitsiya amaliga

nisbatan berk bo‘lsa, ya’ni har qanday ikki kalit z_i va z_j uchun shunday kalit z_k topilsinki, har qanday matnni ketma-ket z_i va z_j kalitlarida shifrlash natijasi shu matnni z_k bilan shifrlangan matnga aynan teng bo‘lsin, ya’ni

$$F(z_j, F(z_i, x)) = F(z_k, x).$$

Unda bu xossadan foydalanib, shifrlash kalitini topish mumkin, ya’ni z_k ni topish uchun ekvivalent juftlik $<z_i, z_j>$ ni topish kifoya. Bu usul "tug‘ilgan kunlar paradoksi"ga asoslanadi. Ma’lumki, tug‘ilgan kunlar tekis taqsimlangan deb hisoblansa, 24 kishilik guruhda *r=0,5* ehtimollik bilan ikki kishining tug‘ilgan kuni bir xil chiqadi.

Umumiy holda bu paradoks quyidagicha ifodalanadi: agar $a \in n$ predmetlar n ta predmet orasidan qaytarilish bilan tanlansa, ikki predmetning bir xil bo‘lish ehtimoli

$$p = 1 - e^{-a^2/2}$$

Faraz qilinsinki, ochiq matn x va uning shifrogrammasi u ma’lum. x uchun tasodifiy tarzda kalitlar to‘plami z_l va shifrogrammalar $w = F(z_l, x)$ to‘plamini saqlovchi ma’lumotlar bazasi (MB) tuziladi va shifrogrammalarni w bo‘yicha tartibga solinadi. MB hajmini $0((p\#\{z\})$ ga teng qilib olinadi.

So‘ngra tasodifan z_{l1} kalitni olib, u shifrmatn ochiladi va natija $v = F(z_{l1}, u)$ ni MB bilan taqqoslanadi. Agar v biror w bilan teng chiqsa, kalit z_{ll} izlangan kalit z ga ekvivalent bo‘ladi.

Vaqt bo‘yicha bu usul murakkabligi

$$O(\varphi\#\{z\}log\#\{z\}).$$

Ko‘paytuvchi $log\#\{z\}$ saralash murakkabligini hisobga oladi.

Zarur xotira $O((r\#\{z\}log\#\{z\})$ bit yoki $O((r\ \#\{z\})$ blokdan iborat. Blok uzunligi va kalit uzunligi cheklangan doimiyga farq qiladi deb faraz qilinadi.

Bu usul kalitlar to‘plami yarim gruppa bo‘lgan qism to‘plamni o‘z ichiga olgan bo‘lsa ham qo‘llanilishi mumkin. Bu usulning boshqa qo‘llanilishini to‘plam yarim gruppa bo‘lmagan hol uchun xesh-funksiyalar misolida namoyish etish mumkin.

Masalan, ERIni soxtalashtirish uchun bitta xesh-obrazga ega ikki matn topish lozim. Undan so‘ng imzolangan xabarni boshqa o‘sha xesh-obrazga ega bo‘lgan xabar bilan almashtirib qo‘yish mumkin. Bunday ikki xabarni topishni "o‘zaro uchrashish" usulida amalga oshirilsa, izlash murakkabligi

$0((p\ \#\{z\})$ bo‘ladi.

Bunda $\#\{z\}$ mumkin bo‘lgan xesh-obrazlar soni. Amerikalik matematik D. SHenks tomonidan taklif etiltan bu algoritm ehtimollik algoritmidir.

Birthday attack- tug‘ilgan kun paradoksi asosida shifrlarni sindirish yoki xesh funksiyalarining to‘qnashuvlarini topish usuli. Usulning mohiyati to‘qnashuvni aniqlash uchun zarur bo‘lgan xesh funksiyasiga berilgan argumentlar sonini sezilarli darajada kamaytirishdan iborat, chunki xesh funksiyasi n-bit qiymat hosil qilsa, u holda kamida bitta xesh qiymat to‘qnashuvi aniqlanishi mumkin bo‘lgan xesh funksiyasining tasodifiy argumentlari soni (ya’ni, har xil argumentlarda olingan

kamida bitta juft xeshsh kodlari mavjud) 2^n ga teng emas, balki atigi $2^n/2$ ga teng.

Misol uchun 23 kishilik guruhdagi ikki kishi bir xil kunda tug‘ilganmi? Kabisa yillarini hisobga olmaganda, bir yil 365 kunni tashkil qiladi, shuning uchun tug‘ilgan kunlar soni 365 tani tashkil etadi, bu 23 tadan ko‘p.

Agar ma’lum bir kun tanlangan bo‘lsa, ushbu kunda kamida bitta odam tug‘ilishi yehtimoli 1- $(364/365)^{23}$ taxminan 6,1%. Ammo, 1-365!/((365-n)!365^n) formulasi bo‘yicha kamida bitta odamning tug‘ilgan kunini boshqa odamlar bilan bir xil bo‘lish ehtimoli taxminan 50% ni tashkil qiladi. n=70 uchun bunday tasodifning ehtimoli 99,9% ni tashkil qiladi.

Umumiy holda tug‘ilgan kun haqidagi parodoks usuli yordamida kolliziya topish quyidagi ifoda orqali topiladi.

$$k = \sqrt{n \cdot \ln\left(\frac{1}{1-P_z}\right)} \qquad (6.1)$$

bu yerda P_z-ixtiyoriy ikkita qiymatning bir xil bo‘lish ehtimolligi, masalan P_z=0.5 bo‘lganda:

$$k = \sqrt{n * \ln(\frac{1}{1-0.5})} = \sqrt{n * ln2} = 0.83\sqrt{n} \qquad (6.2)$$

Blok uzunligi 64 bit va undan kichik bo‘lgan ixtiyoriy bardoshli xesh-funksiyaga kolliziya topish mumkinligini bildiradi.

Bugungi kunda super komyuterlar yordamida parallel hisoblashlardan foydalanib 232 ta amalni tegishli vaqt oralig‘ida bajarish mumkin.

Shu sababli yaratilayotgan barcha xesh-funksiyalar kirish blok uzunligi kamida 128 bit va undan katta qilib tanlanadi. Agar N=128 bit bo‘lsa:

$$Matnlar\ soni \approx \sqrt{2 * 2^N * \ln p^{-1}} = \sqrt{2 * 2^{128} * \ln 2^1} \approx 2^{64}$$

ta ochiq matnni tahlil qilish yetarli. Bunday holatda kolliziya topish uchun $3*10^{15}$ yilga teng vaqt ketadi. Agar N=256 bit bo‘lsa:

$$\boldsymbol{Matnlar\ soni} \approx \sqrt{2 * 2^N * \ln p^{-1}} = \sqrt{2 * 2^{256} * \ln 2^1} \approx 2^{128}$$

ta ochiq matnni tahlil qilish yetarli. Kolliziya topish uchun $3*10^{54}$ yil kerak bo‘ladi. Bu o‘z navbatida bugungi kundagi hisoblash texnikasi imkoniyat darajasidan chiqib ketadi.

2.2. MD4 va MD5 algoritmlarining kriptotahlili.

MD4 bu zamonaviy kompyuterlarda mavjud bo'lgan asosiy arifmetik va mantiqiy amallar yordamida ishlab chiqilgan xesh funksiya hisoblanadi. Bunday turdagi xesh-funksiyalar ko'pincha ajratilgan xesh-funksiyalar deb ataladi va ular blokli shifrlarga asoslangan xesh-funksiyalardan ancha farq qiladi.

MD4 oilasida bir nechta maxsus xesh-funksiyalar muvaffaqiyatli ishlab chiqilgan, jumladan MD5, HAVAL, RIPEMD, RIPEMD-160, SHA-1, SHA-256 va boshqalar. Ushbu xesh funksiyalar, garchi murakkabroq bo'lsa-da, barchasi MD4 bilan bir xil dizayn falsafasiga amal qiladi va MD4 bilan o'xshash tuzilmalarga ega. Xususan, RIPEMD MD4 ning ikkita parallel nusxasidan iborat. MD4 algoritmi uchun bir qancha muhim kriptotahlil natijalari mavjud. 1996 yilda H. Dobbertin MD4 ga kolliziya hujumini ishlab chiqdi va bu 2^{-22} ehtimollik bilan kolliziyani

topadi. Shuningdek, u kolliziyani qanday topishni ko'rsatdi.

MD4 algoritmining kriptoanalizini o'rganishdan oldin uning ishlash prinsipini o'rganish maqsadga muvofiq hisoblanadi.

MD4 algoritmi

Xabarlar xeshlash algoritmi MD4 har qanday ixtiyoriy bit uzunlikdagi ma'lumotni 128 bitli xesh qiymatiga siqib chiqaradi. Har qanday xabarni xeshlashdan avval algoritm uni 512 bitga karrali uzunlikdagi xabarga bo'lib oladi. Har bir 512-bitli xabar bloki uchun MD4 siqish funktsiyasidan foydalanib, uni 128-bitli xesh qiymatiga siqib chiqaradi. MD4 siqish funksiyasi uchta turga ega. Har bir turda quyidagi tarzda aniqlangan chiziqli bo'lmagan mantiqiy funktsiyadan foydalaniladi:

$$F(X,Y,Z) = (X \cap Y) \cup (\neg X \cap Z)$$

$$G(X,Y,Z) = (X \cap Y) \cup (X \cap Z) \cup (Y \cap Z)$$

$$H(X,Y,Z) = X \oplus Y \oplus Z$$

Bu erda X, Y, Z 32 bitli so'zlar. Uchta funksiyaning hammasi bitli amallar. $\neg X - X$ ning bit bo'yicha to'ldiruvchisi, $\wedge, \oplus$ va $\vee$ mos ravishda bit bo'yicha AND, XOR va OR amallaridir.

Siqish funksiyasining har bir bosqichi 16 marta takrorlanadi va har bir bosqichda to'rtta o'zgaruvchi a, b, c, d yangilanadi.

$$\phi_0(a,b,c,d,m_k,s) = ((a + F(b,c,d + m_k) mod 2^{32} <<< s$$

$$\phi_1(a,b,c,d,m_k,s) = ((a + G(b,c,d) + m_k + 0x5a827999) mod 2^{32} <<< s$$

$$\phi_2(a,b,c,d,m_k,s) = ((a + H(b,c,d) + m_k + 0x6ed9eba1) mod 2^{32} <<< s$$

MD4 algoritmi uchun dastlabki qiymat quyidagiga teng:

$(a,b,c,d) = (0x67452301, 0xefcdab89, 0x98badcfe, 0x10325476)$.

MD4 siqish funksiyasi. To'ldirilgan M xabarining 512 bitli M bloki uchun $M = (m0, m1, \ldots, m15)$ siqish funktsiyasi quyidagicha aniqlanadi:

1. (aa, bb, cc, dd) M uchun kirish o'zgaruvchilari bo'lsin. Agar M xeshlangan birinchi xabar bloki bo'lsa, u holda (aa, bb, cc, dd) boshlang'ich qiymat sifatida o'rnatiladi. Aks holda ular oldingi xabar blokini siqishdan olingan natijadir.
2. Uch raundda quyidagi 48 ta qadam bajariladi:

   $For\ j = 0,1,2\ and\ i = 0,1,2,3$

$$a = \phi_j(a,b,c,d,w_{j,4i},,s_{j,4i})$$

$$d = \phi_j(d,a,b,c,w_{j,4i+1},,s_{j,4i+1})$$

$$c = \phi_j\left(c, d, a, b, w_{j,4i+2},, s_{j,4i+2}\right)$$

$$b = \phi_j\left(b, c, d, a, w_{j,4i+3},, s_{j,4i+3}\right)$$

Bu yerda $s_{j,4i+k}$ $(k = 0, 1, 2, 3)$ qadamlarga bog‘liq o‘zgarmaslar, $w_{j,4i+k}$ xabar so‘zi va $\ll s_{j,4i+k}$ siklida $s_{j,4i+k}$ bilan chapga siljiydi.

3. Joriy xabar bloki uchun yakuniy o'zgaruvchilarni ishlab chiqarish uchun kirishdagi o'zgaruvchilariga mos ravishda a, b, c va d o'zgaruvchilar qo'shiladi.

$$aa = (a + aa) mod 2^{32}$$
$$bb = (b + bb) mod 2^{32}$$
$$c = (c + cc) mod 2^{32}$$
$$d = (d + dd) mod 2^{32}$$

Agar M oxirgi xabar bloki bo'lsa, $H(M') = aa|bb|cc|dd$ M xabarining xesh qiymatidir. Aks holda yuqoridagi jarayonni keyingi 512 bitli xabar bloki bilan takrorlanadi va (aa, bb, cc, dd) kirish o'zgaruvchilari sifatida olinadi.

MD4 algoritmiga kolliziya hujumi

MD4 algoritmiga kolliziya hujumini 2^{-2} dan 2^{-6} gacha imkoniyatda muvaffaqiyatli amalga oshirish imkoniyati mavjud. Bunda hisoblash murakkabligi 2^8 dan past. Hujum uch qismdan iborat:

1. M va M’ xabarlar uchun kolliziya hosil qiladigan differensial topiladi;

2. Kolliziya differensialini saqlab turishni ta'minlaydigan yetarli shartlar to'plami ishlab chiqiladi;

3. Har qanday tasodifiy M xabari uchun yuqoridagi shartlar bajarilguncha M ga o'zgartirish kiritib boriladi.

MD4 algoritmi uchun kolliziya differensiali

MD4 algoritmi uchun kolliziya differensiali quyidagicha tanlanadi:

$$\Delta H_0 = 0 \left(\xrightarrow{(M,M')}\right) \Delta H = 0$$

Shu kabi

$$\Delta M = M' - M = (\Delta m_0, \Delta m_1, \ldots., \Delta m_{15})$$
$$\Delta m_1 = 2^{31}, \Delta m_2 = 2^{31} - 2^{28}, \Delta m_{12} = -2^{16}$$
$$\Delta m_i = 0, 0 \le i \le 15, i \ne 1,2,12.$$

Kolliziya differensialidagi barcha xususiyatlarni 6.4-jadvalda topish mumkin. Birinchi ustun qadamni bildiradi, ikkinchi ustun M uchun har bir qadamdagi zanjirli o'zgaruvchisi, uchinchisi - har bir qadamda M uchun xabar so'zi, to'rtinchisi – siljish sikli, beshinchi va oltinchi ustunlar - mos ravishda M va M' ma’lumotlari differensiali, yettinchisi esa M' uchun zanjirli o'zgaruvchidir. Ayniqsa, beshinchi va oltinchi ustunlardagi bo'sh elementlar nol farqlarni bildiradi va jadvalda ko'rsatilmagan qadamlar xabar so'zlari va zanjirli o'zgaruvchilar uchun nolga teng

differensialga ega.

Ko'rinib turibdiki, kolliziya differensiallari mos ravishda 2-25 qadam va 36-41 bosqichli ikkita ichki moslikdan iborat.

Barcha xususiyatlarni ushlab turishni ta'minlaydigan yetarli shartlar 6.5-jadvalda keltirilgan mantiqiy funktsiyalarning xususiyatlari bilan osongina tekshirilishi mumkin. Bu shuni anglatadiki, agar M 6.5-jadvaldagi barcha shartlarni qanoatlantirsa, M va M' ma'lumotlarning kolliziya qiymatlari topilgan bo'ladi.

Quyida 6.4-jadvalning 9-bosqichidagi yetarlilik shartlarining natijasi keltirilgan. 9-bosqichdagi differensial xarakteristika:

$$(b_2[-13,-14,15], c_2[19,20,-21], d_2[14], a_2)$$
$$\rightarrow (a_3[17], b_2[-13,-14,15], c_2[19,20,-21,22], d_2[14])$$

1. 1-taklifga binoan, $c_{2,13} = d_{2,13}$ va $c_{2,15} = d_{2,15}$ shartlar b_2 dagi 13 va 15-bitlardagi o'zgarishlar hech qanday o'zgarishga olib kelmasligini ta'minlaydi.

2. 1-taklifga binoan, $b_{2,19} = 0$, $b_{2,20} = 0$, $b_{2,21} = 0$ va $b_{2,22} = 0$ shartlar 19-chi, 20-bandlardagi o'zgarishlarni ta'minlaydi. c_2 ning , 19-, 21- va 22-bitlari a_3 ning o'zgarishiga olib kelmaydi.

6.4- jadval

MD4 algoritmi uchun kolliziya differensialidagi xarakteristikalar

Qadam	**M uchun zanjirli qiymat**	$W_{j,i}$	**Siljish**	Δm_i	***i*-bosqichdagi differensial**	***M'* uchun *i*-chi chiqish**
1	a_1	m_0	3			a_1
2	d_1	m_1	7	2^{31}	2^6	d_1[7]
3	c_1	m_2	11	$-2^{28}+2^{31}$	-2^7+2^{10}	c_1[-8,11]
4	b_1	m_3	19		2^{25}	b_1[26]
5	a_2	m_4	3			a_2
6	d_2	m_5	7		2^{13}	d_2 [14]
7	c_2	m_6	11		$-2^{18}+2^{21}$	c_2[19,20-21,22]
8	b_2	m_7	19		2^{12}	b_2[-13,-14,15]
9	a_3	m_8	3		2^{16}	a_3 [17]
10	d_3	m_9	7		$2^{19}+2^{20}-2^{25}$	d_3[20,-21,-22,23-26]
11	c_3	m_{10}	11		-2^{29}	c_3[-30]
12	b_3	m_{11}	19		2^{31}	b_3[32]
13	a_4	m_{12}	3	-2^{16}	$2^{22}+2^{25}$	a_4[23,26]
14	d_4	m_{13}	7		$-2^{26}+2^{28}$	d_4[-27,-29,30]
15	c_4	m_{14}	11			c_4
16	b_4	m_{15}	19		2^{18}	b_{14}[19]
17	a_5	m_0	3		$2^{25}-2^{28}-2^{31}$	a_5[-26,27,-29,-32]
18	d_5	m_4	5			d_5

Qadam	M uchun zanjirli qiymat	$W_{j,i}$	Siljish	Δm_i	i-bosqichdagi differensial	M' uchun i-chi chiqish
19	c_5	m_8	9			c_5
20	b_5	m_{12}	13	-2^{16}	$-2^{29}+2^{31}$	b_5[-30,32]
21	a_6	m_1	3	2^{31}	$2^{28}-2^{31}$	a_6[-29,30,-32]
22	d_6	m_5	5			d_6
23	c_6	m_9	9			c_6
24	b_6	m_{13}	13			b_6
25	a_7	m_2	3	$-2^{28}+2^{31}$		a_7
…	…					…….
36	b_9	m_{12}	15	-2^{16}	2^{31}	b_9[-32]
37	a_{10}	m_2	3	$-2^{28}+2^{31}$	2^{31}	a_{10}[-32]
38	d_{10}	m_{10}	9			d_{10}
39	c_{10}	m_6	11			c_{10}
40	b_{10}	m_{14}	15			b_{10}
41	a_{11}	m_1	3	2^{31}		a_{11}

3. f funksiyaning xossasidan $b_{2,14} = 1$, $d_{2,14} = 0$ va $c_{2,14}$=0 shartlar f($b_{2,14}, d_{2,14}, c_{2,14}$) = 0 ni hosil qiladi. va f($\neg b_{2,14}$, $c_{2,14}$, $\neg d_{2,14}$) = 1. Demak, $\Delta a_3 = 2^{16}$.

4. $a_{3,17} = 0$ sharti $a'_3 = a_3$ bo'lishini ta'minlaydi.

Shunday qilib, yuqoridagi 10 ta shart 9-bosqichdagi differensial xarakteristikalar uchun yetarli shartlar to'plamidan iborat bo'ladi va MD4 algoritmi uchun kolliziya hujumini ifodalaydi.

6.5-jadval

MD4 algoritmida kolliziya uchun yetarlilik shartlar to'plami

a_1	$a_{1,7} = b_{0,7}$
d_1	$d_{1,7} = 0$, $d_{1,8} = a_{1,8} = 1$, $c_{1,11} = a_{1,11}$
c_1	$c_{1,7} = 1$, $c_{1,8} = 1$, $a_{1,8} = 1$, $c_{1,11} = 0$, $c_{1,26} = d_{1,26}$
b_1	$b_{1,7} = 1$, $b_{1,8} = 0$, $b_{1,11} = 0$, $b_{1,26} = 0$
a_2	$a_{2,8} = 1$, $a_{2,11} = 1$, $a_{2,26} = 0$, $a_{2,14} = b_{1,14}$
d_2	$d_{2,14} = 0$, $d_{2,19} = a_{2,19}$, $d_{2,20,} = a_{2,20,} d_{2,22,} = a_{2,21,} = d_{2,22} = a_{2,22,} d_{2,22} = 1$
c_2	$c_{2,13} = d_{2,13}$, $c_{2,13,} = 0$ $c_{2,15} = d_{2,15,} c_{2,19} = 0$, $c_{2,20} = 0$, $c_{2,21} = 1$, $c_{2,22} = 0$
b_2	$b_{2,13} = 0$, $b_{2,14,} = 1$ $b_{2,15,} = 0$, $b_{2,17,} c_{2,17,}$ $b_{2,19,} = 0$, $b_{2,20} = 0$, $b_{2,21,} = 0$, $b_{2,22,} = 0$,
a_3	$a_{3,13} = 1$, $a_{3,14} = 1$ $a_{3,15} = 1$, $a_{3,17} = 0$, $a_{3,19} = 0$, $a_{3,20} = 0$, $b_{3,20} = 0$, $a_{3,21} = 0$, $a_{3,23}$, = $b_{2,23} a_{3,22} = 1$, $a_{3,26} = b_{2,26}$
d_3	$d_{3,13} = 1$, $d_{3,14} = 1$, $d_{3,15} = 1$, $d_{3,17} = 0$, $d_{3,20} = 0$, $d_{3,21} = 1$, $d_{3,22} = 1$, $d_{3,23} = 0$,

	$d_{3,26} = 1, d_{3,26} = 1, d_{3,30} = a_{3,30}$
c_3	$c_{3,17} = 1,\ c_{3,20} = 0, c_{3,21} = 0,\ c_{3,22} = 0,\ c_{3,23} = 0, c_{3,26} = 0, c_{3,30} = 1, c_{3,32},\ c_{3,32} = d_{3,32}$
b_3	$b_{3,20} = 0,\ b_{3,21} = 1, b_{3,22} = 1,\ b_{3,23,} = c_{3,23,}\ b_{3,26} = 1, b_{3,30} = 0,\ b_{3,32} = 0$
a_4	$a_{4,23} = 0,\ a_{4,26} = 0,\ a_{4,27} = b_{3,27,} a_{4,29} = b_{3,29,}\ a_{4,30} = 1, a_{4,32} = 0,$
d_4	$d_{4,23} = 0,\ d_{4,26} = 0,\ d_{4,27} = 1, d_{4,29} = 1, d_{4,30} = 0,\ d_{4,32} = 1,$
c_4	$C_{4,19} = d_{4,19}, c_{4,23} = 1, c_{4,26} = 1, c_{4,27} = 0,\ c_{4,29} = 0, c_{4,30} = 0,$
b_4	$b_{4,19} = 0,\ b_{4,26} = c_{4,26} = 1, b_{4,27} = 1,\ b_{4,29} = 1, b_{4,30} = 0,$
a_5	$a_{5,19} = c_{4,19}, a_{5,26} = 1, a_{5,27} = 1,\ a_{5,29} = 1, a_{5,32} = 1,$
d_5	$d_{5,19} = a_{5,19}, d_{5,26} = b_{4,26,} d_{5,27} = b_{4,27}, d_{5,29} = b_{4,29}, d_{5,32} = b_{4,32},$
c_5	$c_{5,26} = d_{5,26}, c_{5,27} = d_{5,27,} c_{5,29} = d_{5,29}, c_{5,30} = d_{5,30}, c_{5,32} = d_{5,32},$
b_5	$b_{5,29} = c_{5,29}, b_{5,30} = 1, b_{5,32} = 0,$
a_6	$a_{6,29} = 1,\ a_{6,32} = 1,$
d_6	$d_{6,29} = b_{5,29},$
c_6	$c_{6,29} = d_{6,29},\ c_{6,30} = d_{6,30} + 1, c_{6,32} = d_{6,22} + 1,$
b_9	$b_{9,32} = 1$
a_{10}	$a_{10,32} = 1$

2.3. NIST va DIEHARD statistik testlar to‘plami.

Axborot xavfsizligida talab qilingan tasodifiy sonlarni hosil qilish muammosini bartaraf etishda quyidagi usullardan foydalaniladi:

Xavfsiz bo‘lmagan tasodifiy sonlar generatori. Bu turdagi generatorlar kriptografik psevdo-tasodifiy sonlar generatori hisoblanmaydi. Mazkur turdagi generatorlardan foydalanilganda hujumchi hosil qilinuvchi qiymatlarni oldindan bilishi mumkin bo‘ladi.

Bu turdagi generatorlarga misol sifatida aksariyat dasturlash tillarida mavjud $rand()$ yoki $random()$ funksiyalarini (chiziqlik kongurent generatorlarga asoslangan) keltirish mumkin. Bundan tashqari “Mersenne Twister” generatori ham ushbu toifaga tegishli bo‘lib, qator tizimlarda va dasturiy vositalarga (masalan, Matlab, Excel, PHP, Python va hak.) keng qo‘llaniladi. Bu turdagi generatorlar yuqori darajadagi entropiyaga ega kalitlarni generasiya qila olmasligi bilan zaif sanaladi. Ushbu generator 1997 yilda Makoto Matsumoto va Takuji Nishimuralar tomonidan yaratilgan.

Quyida “Mersenne Twister” algoritmining umumiy ifodasi keltirilgan:

$$x_{k+n} \coloneqq x_{k+m} \oplus \left(\left(x_k^u || x_{k+1}^l \right) A \right)$$

“Mersenne Twister” generatorining 32 bitli tizim uchun mo‘ljallangan shaklida quyidagi parametrlardan foydalanilgan:

$(w,\ n,\ m,\ r) = (32, 624, 397, 31)$;

$a = 9908\text{B}0\text{DF}_{16}$;

$(u,\ d) = (11, \text{FFFFFFFF}_{16})$;

$(s, b) = (7, 9\text{D}2\text{C}5680_{16})$;

$(t, c) = (15, \text{EFC}60000_{16})$;

$l = 18$.

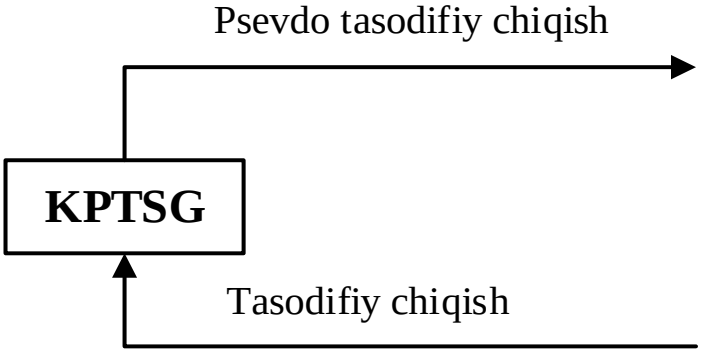
Bu yerda: w- so‘z uzunligi (bitda), $n-$ takrorlanish darajasi, $m-$ foydalaniluvchi o‘rta so‘z, $r-$ bir so‘zning ikkiga bo‘linish nuqtasi, $a-$ twist matritsasi uchun koeffisent, $b, c-$ almashtirish bit maskalari, $s, t-$ almashtirishdashi siljitish bitlari, $u, d, l-$ qo‘shimcha siljitish va maska parametrlari. Umumiy holda ushbu generatorning psevdokodi quyidagicha:

```
// generator holatini saqlash uchun n uzunlikdagi massivni yaratish
int[0..n-1] MT
int index := n+1
const int lower_mask = (1 << r) - 1
const int upper_mask = lowest w bits of (not lower_mask)

// Dastlabki seed qiymatdan generatorni ishlatish
function seed_mt(int seed) {
  index := n
  MT[0] := seed
  for i from 1 to (n - 1) {
    MT[i] := lowest w bits of (f * (MT[i-1] xor (MT[i-1] >> (w-2))) + i)
  }
}

// MT[index] dan qiymatlarni ajratish
// har n tada twist() ni chaqirish
function extract_number() {
  if index >= n {
    if index > n {
     error "Generator was never seeded"
     }
    twist()
  }

  int y := MT[index]
  y := y xor ((y >> u) and d)
  y := y xor ((y << s) and b)
  y := y xor ((y << t) and c)
  y := y xor (y >> l)

  index := index + 1
  return lowest w bits of (y)
}
// x_i lar ketma-ketligidan keyingi n qiymatni generasiya qilish
```

```
function twist() {
  for i from 0 to (n-1) {
    int x := (MT[i] and upper_mask)
         + (MT[(i+1) mod n] and lower_mask)
    int xA := x >> 1
    if (x mod 2) != 0 {
      xA := xA xor a
    }
    MT[i] := MT[(i + m) mod n] xor xA
  }
  index := 0 }
```

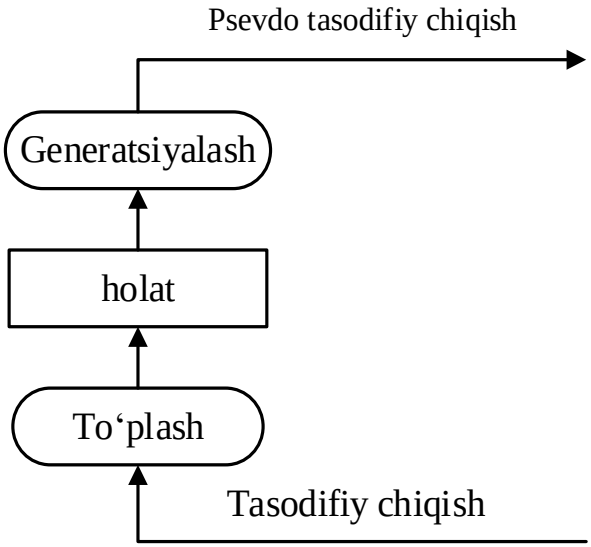
Ushbu generatorda almashtirish funksiyasi sifatida bir tomonlama funksiyadan foydalanilmaganiligi sababli, xavfsiz emas deb qaraladi. Ushbu generatorning keyingi versiyalarida tezkorlikni oshirishga harakat qilingan (TinyMT).

Kriptografik psevdotasodifiy sonlar generatori (KPTSG). Mazkur usulga asosan xavfsiz yagona boshlang‘ich qiymat (seed) ni kiritish orqali kriptografik algoritm talab etilgan uzunlikdagi tasodifiy qiymatlarni generasiya qilib beradi. Ushbu holat aksariyat hollarda tasodifiy qiymatlarni generasiya qilishdagi asosiy yechim sifatida qaraladi. Umumiy holda *KPTSG* larni 5.2-rasmdagi kabi tasvirlash mumkin.



5.3-rasm. KPTSGlarni umumiy ko‘rinishi

Tasodifiy hodisalar manbasidan olingan qiymatlan dastlab to‘plash jarayoni orqali ma’lum vaqt to‘planib boriladi. Ushbu to‘plangan ma’lumotlar orqali generator holati yangilanadi va shundan so‘ng generasiyalash jarayonida psevdotasodifiy chiqishlar hosil qilinadi (5.3-rasm).



5.4-rasm. KPTSGning takshiliy jarayonlari

KPTSGning holat jarayoni muhim ahamiyatga ega bo‘lib, qator qism bosqichlardan iborat. Dastlab kiritilgan tasodifiy qiymatlar *pool* deb ataluvchi yig‘uvchida to‘planib boradi va u davomiy amalga oshiriladi. Yig‘uvchi *pool* to‘plangan qiymatlar asosida generator ichki holati yangilanadi (*reseed*). Shundan so‘ng har bir generasiya qilingan psevdotasodifiy blokdan so‘ng, *seed* jarayoni orqali generator ichki holati qaytadan yangilanadi. Bunda generatorning chiqish qiymatidan foydalaniladi. Umumiy holda *seed* va *reseed* jarayonlarining asosiy farqi ularning generator ichki holatini yangilashda foydalanadigan qiymatlaridadir. Boshqa so‘z bilan aytganda, *reseed* jarayonida ichki holat *pool* dagi qiymatlar asosida yangilansa, *seed* jarayoni generasiyalash jarayonidan foydalangan holda uni amalga oshiradi.

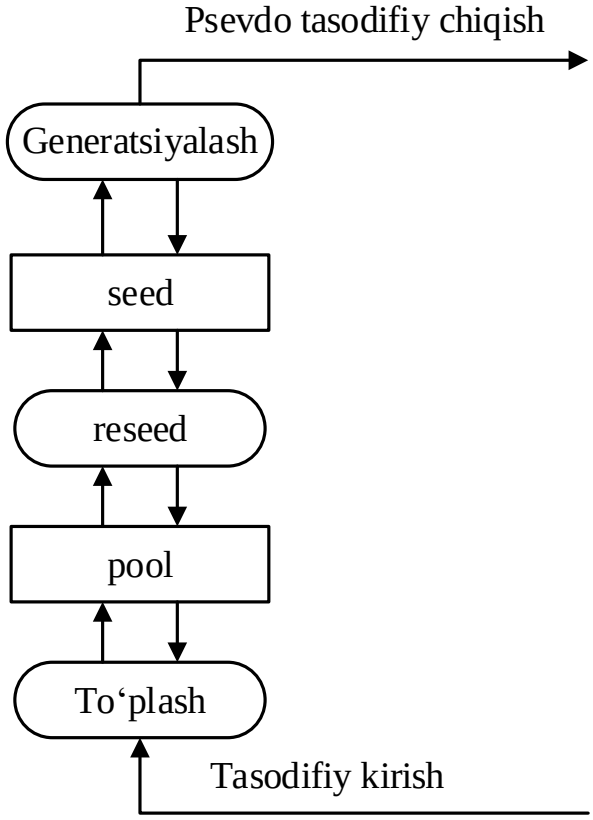
ANSI X9.17 KPTSG. Ushbu generator asosan DES algoritmi uchun kalit va boshlang‘ich vektor (IV)ni hosil qilish uchun ishlab chiqilgan. Bunda u 3DES algoritmidan foydalangan bo‘lsada, amalda boshqa blokli shifrlardan ham foydalanish mumkin.

1. Dastlab tasodifiy hodisalar manbasidan olingan tasodifiy kalit *K* olinadi. U maxfiy saqlanadi va barcha kirishlar davomida o‘zgarmaydi hamda maxfiy holatni ta’minlaydi.
2. Har safar zarur bo‘lgan chiqishni hosil qilish uchun quyidagilar bajariladi:
   a. $T_i = E_R(joriy\ vaqt\ metkasi)$;
   b. $chiqish[i] = E_K(T_i + seed[i])$;
   c. $seed[i+1] = E_K(T_i + chiqish[i])$.

DSA KPTSG. Digital Signature Standard (DSA) standartida elektron raqamli imzo algoritmi bilan birgalikda algoritmning zarur bo‘lgan parametrlarini hosil qilish uchun foydalaniladigan sodda PTSG ham keltirilgan. Ushbu algoritm SHA1 (yoki DES algoritmi) xesh funksiyasiga asoslanganda $N = 160$ yoki uning boshqa qiymatlaridan ($160 \le N \le 512$) ham foydalanilishi mumkin. $N = 160$ hol uchun generatorning ishlash ketma-ketligi quyidagicha:

1. KPTSG uzluksiz o‘zgarib turuvchi holat X_i dan iborat.

2. KPTSG tanovga ko‘ra kirish qiymati W_i ni qabul qiladi. Agar bu qiymat amalga oshirilmasa, u holda u nolga teng deb olinadi.
3. KPTSG har bir chiqish bloki uchun quyidagilarni amalga oshiradi:
   a. $output[i] = hash\big((W_i + X_i) mod 2^{160}\big)$;
   b. $X_{i+1} = (X_i + output[i] + 1) mod 2^{160}$.



5.5-rasm. Umumiy KPTSG, davomiy ichki holatni yangilab borish

4. KPTSG uzliksiz o‘zgarib turuvchi holat X_i dan iborat.
5. KPTSG tanovga ko‘ra kirish qiymati W_i ni qabul qiladi. Agar bu qiymat amalga oshirilmasa, u holda u nolga teng deb olinadi.
6. KPTSG har bir chiqish bloki uchun quyidagilarni amalga oshiradi:
   a. $output[i] = hash\big((W_i + X_i) mod 2^{160}\big)$;
   b. $X_{i+1} = (X_i + output[i] + 1) mod 2^{160}$.

RSA REF KPTSG. RSAREF 2.0 hujjatida keltirilgan *KPTSG* ikki amaldan: MD5 asosida xeshlash va $mod 2^{128}$ bo‘yicha qo‘shishdan iborat. Ushbu *PTSG*ning amalga oshirish ketma-ketligi quyidagicha:

1. 128 bitli sanoq C_i berilgan bo‘lsin.
2. Agar dastlabki kirish qiymati X_i bo‘lsa, $C_{i+1} = (C_i + MD5(X_i)) mod 2^{128}$ hisoblanadi.
3. Psevdotasodifiy ketma-ketlik quyidagicha hisoblanadi:
   a. $output[i] = MD5(C_i) mod 2^{128}$;
   b. $C_{i+1} = (C_i + 1) mod 2^{128}$.

Entropiya to‘plovchilar. Ushbu tizimlar odatda “haqiqiy” tasodifiy sonlar generatori deb ham yuritiladi va ular turli manbalardan tasodifiy qiymatlar (entropiya) ni to‘playdi hamda bevosita taqdim etadi. Ular aksariyat hollarda xavfsiz

deb qaralsada, qiymatlarni generasiya qilish tezligi past.

CryptGenRandom. Ushbu kriptografik PTSGi Microsoft CryptoAPI ichida mavjud bo‘lib, Windows OTdagi barcha ilovalar undan foydalanishi mumkin. Ushbu generator gibrid sanalib, entropiya to‘plovchi va PTSGlaridan iborat.

Ushbu generatorda kriptografik algoritmlar sifatida RC4 oqimli shifrlash algoritmi va SHA1 xesh-funksiyasi foydalanilgan. Ushbu generator algoritmi yoki ochiq kodi chop etilmagan bo‘lib, dizassamberlash natijasida olingan psevdokodi quyidicha:

```
CryptGenRandom (Buffer , Len)
// output Len bytes to buffer
while (Len >0) {
    R := R ⊕ get_next_20_rc4_bytes ()
    State := State ⊕ R
    T := SHA -1’(State)
    Buffer := Buffer | T
        // | denotes concatenation
    R[0..4] := T[0..4]
        // copy 5 least significant bytes
    State := State + R + 1
    Len := Len – 20
}
```

Unga asosan har bir siklda 20 baytli tasodifiy qiymat hosil bo‘ladi. Generatorning asosiy holati ikkita registr R va $State$ dan iborat. Ushbu ikki registor holati har bir siklda yangilanib boradi va chiqish qiymatni hosil qiladi.

Ushbu generatorning entropiya to‘plovchi qismi operasion tizimning turli manbalaridan 3584 baytgacha ma’lumotni yig‘ishi aytib o‘tilgan. Ushbu to‘plangan ma’lumotlar “katta xesh funksiya” (VeryLargeHash) deb ataluvchi funksiya yordamida 80 baytga aylantiriladi.

/dev/random. Ushbu tasodifiy sonlar generatori Linux OT muhiti uchun eng keng tarqalgan bo‘lib, u Teodor Tso tomonidan ishlab chiqilgan va ushbu generator Linux 1.3.30 dan boshlab OT o‘zak qismiga aylangan. Ushbu tasodifiy sonlar genaratori turli manbalardan keladigan entropiya qiymatlarini yig‘ishga asoslangan. Talab etilgan tasodifiy qiymat to‘plangandan so‘ng, generator chiqish qiymatini taqdim etadi. Shuning uchun ushbu generator talab qilingan qiymat mavjud bo‘lmaganda bloklangan holatda bo‘ladi.

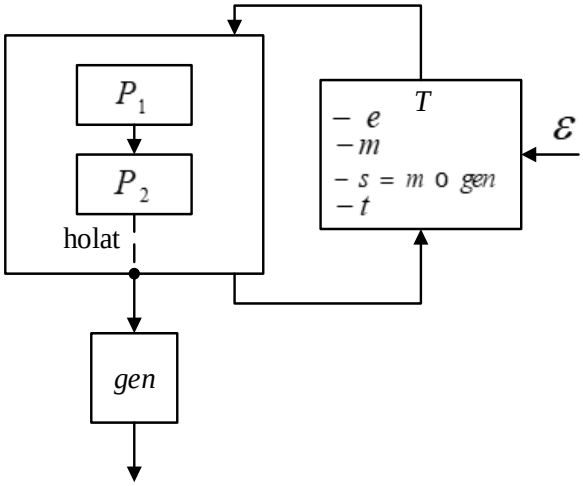
Bundan tashqari ushbu algoritm asosida yaratilgan */dev/urandom* generatori mavjud bo‘lib, u entropiya to‘plovchi va KPTSGlari mujassamlashganidan iborat.

/dev/random generatori ikkita “pul” (pool) dan iborat. Birlamchi pul $\mathcal{P}_1$ tashqi hodisalar manbai $\mathcal{E}$ dan keluvchi entropiyani to‘plash uchun foydalanilsa, ikkinchi pul $\mathcal{P}_2$ tasodifiy qiymatlarni generasiya qilish uchun foydalaniladi. Bunda baytlar $\mathcal{P}_1$ dan $\mathcal{P}_2$ ga ko‘chirib o‘tkaziladi. “Pul”lar bilan aralashtirishni amalga oshirish uchun ikkita funksiya mavjud bo‘lib, ulardan biri m – aralashtirish funksiyasi va gen – generasiyalash funksiyasi sanaladi. Aralashtirish funksiyasi pulga kirishda foydalanilsa, generasiya funksiyasi esa chiqishda tasodifiy ketma-ketliklarni hosil

qilishda foydalanadi. Ikki pulning o‘lchami 64 ga karrali bo‘lgan bitdan iborat bo‘lib, siqish funksiyasi sifatida CRC-32 funksiyasidan foydalanilgan.

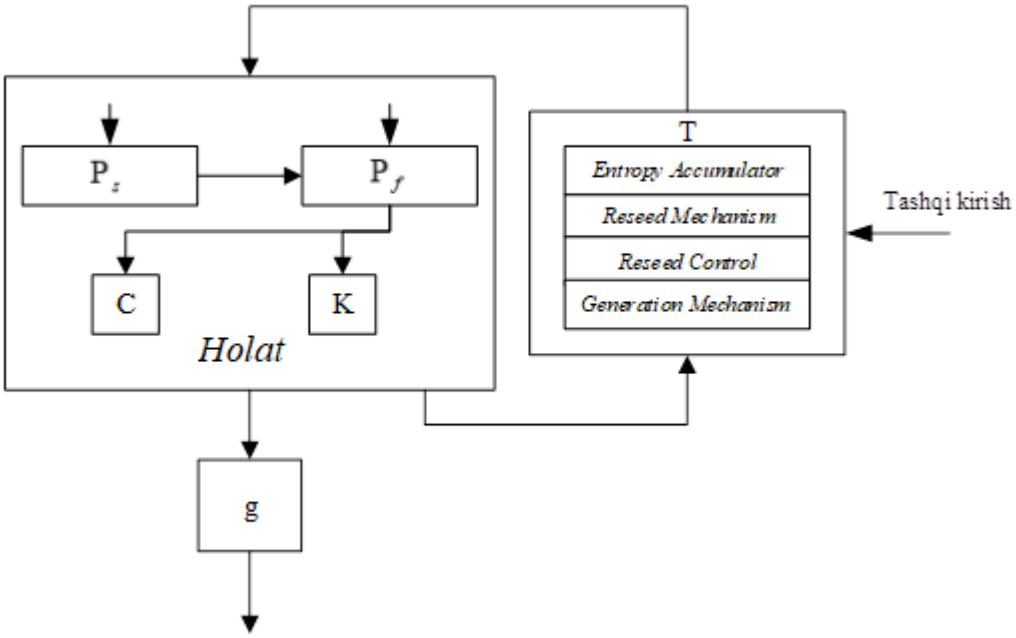
Yarrow. Ushbu generator tasodifiy sonlar generatorini qurish uchun umumiy konsepsiya bo‘lib, Counterpane Systems tashkilotida N.Fergusson, J. Kelsey va B.Shnayerlar tomonidan ishlab chiqilgan.

Ushbu konsepsiyaga asosan kriptografik xesh – funksiya asosida to‘ldiriluvchi ikkita pul: *tezkor (fast)*, P_f va *sekin (slow)*, P_s to‘ldirib boriladi. Ulardan blokli simmetrik shifrlash algoritmining kaliti K hosil qilinadi va u bilan ortib boruvchi sanagich qiymati C shifrlanadi. Ushbu konsepsiyaga ko‘ra tanlangan xesh funksiya kriptografik xesh funksiya talablariga javob berishi va blokli simmetrik shifrlash algoritmi ham bardoshli bo‘lishi talab etiladi. Xususan, Yarrow-160 da 160-bitli SHA1 xesh funksiyasi va 3DES algoritmidan foydalanilgan.



5.6-rasm. /dev/randomning umumiy strukturasi

Yarrow konsepsiyasi 5.6-rasmda keltirilgan 4 ta komponentdan iborat. *Entropy Accumulator* jarayonida tashqi manbalardan kiruvchi ma’lumotlarni ikkita pulga joylashtirish va entropiyani hisoblashdan iborat. *Reseed Mechanism* jarayonida holat talabdagi kabi bo‘lsa pullardan yangi kalit hosil qilinadi. *Reseed Control* mexanizmi esa *Reseed Mechanism* uchun yetarli entropiya to‘planganini aniqlash uchun foydalaniladi. *Generation Mechanism* jarayonida hosil bo‘lgan kalit va sanaq qiymatiga ko‘ra tasodifiy baytlar ketma-ketligi hosil qilinadi.



5.7-rasm. Yarrowning umumiy tuzilishi

Ushbu generatorning bardoshligi foydalanilgan xesh funksiyadan olingan xesh qiymat uzunli m va hosil qilingan kalit uzunligi k larning eng kichigining qiymatiga teng bo‘ladi. Ya’ni, kalit 3DES uchun $k = 192$ va SHA1 xesh funksiya uchun $m = 160$ ligidan, generatorning bardoshligini 160 bitga teng deb qarash mumkin.

Axborot xavfsizligida tasodifiy sonlar generatoridan hosil bo‘lgan ketma-ketliklarni tasodifiylik darajasini tekshirish uchun mos aniqlash usuli mavjud bo‘lishi zarur. Hozirgi kunda tadqiqotchilar tomonidan qurilmaga yoki dasturiy ta’minotga asoslangan yangi tasodifiy sonlar generatorlari ishlab chiqilmoqda. Biroq, ulardan hosil bo‘lgan tasodifiy qiymatlarga baho bermasdan turib, ularni amalga foydalanish tavsiya etilmaydi.

Tasodifiy sonlar generatoridan hosil bo‘lgan qiymatlarni statistik testlash usullari asosida testlash amalga keng foydalanilib, odatda quyidagi turdagi statistik testlar to‘plamidan keng qo‘llaniladi (5.1-jadval).

5.1-jadval

Statistik testlar to‘plami va ularning xususiyatlari

№	**Manba/ muallif**	**Testlar to‘plami nomi**	**To‘plam-dagi testlar soni**
1.	Donald Knuth/ Stanford University	The Art Of Computer Programming Vol. 2 Seminumerical Algorithms	11 ta
2.	George Marsaglia/Florida State University	DIEHARD	15 ta
3.	Helen Gustafson, et. al./ Queensland University of Technology	Crypt-XS	6 ta

№	Manba/ muallif	Testlar to‘plami nomi	To‘plam-dagi testlar soni
4.	Alfred Menezes, et. al./CRC Press, Inc.	Handbook of Applied Cryptography	
5.	Pierre L’Ecuyer, Richard Simard/ Université de Montréal	TestU01’s test batteries	SmallCrush (10) Crush (96 ta) BigCrush (106 ta)
6.	Andrew Rukhin, et. al./NIST ITL	NIST Statistical Test Suite	15 ta

Donald Knut tomonidan yozilgan “The Art of Computer Programming, Seminumerical Algorithms, Volume 2” nomli kitobda, muallif qator emperik testlarni keltirib o‘tgan. Jumladan, *chastota* (frequency), *ketma-ketlik* (serial), *oraliq* (gap), *poker* (poker), *kupon to‘plovchi* (coupon collector's), *o‘rin almashtirish* (permutation), *yugirish* (run), *t ning maksimumi* (maximum-of-t), *kolliziya* (collision), *tug‘ulgan kun oralig‘i* (birthday spacings) va *ketma-ketlik korrelasiyasi* (serial correlation) testlar.

DIAHARD testlar to‘plami Djorj Marsaliya tomonidan ishlab chiqilgan bo‘lib, 15 ta statistik testlardan: *tug‘ulgan kun oralig‘i* (birthday spacings), *bog‘liqlikni almashtirish* (overlapping permutations), *matrisa rangini o‘lchash* (ranks of 31x31, 32x32, 6x8 matrices), *“20-bitli so‘zda maymun” testi* (monkey tests on 20-bit Words, monkey tests OPSO), *OQSO, DNA, ketma-ketlikdagi birlar sonini aniqlash* (count the 1's in a stream of bytes), *maxsus baytdagi birlar sonini aniqlash* (count the 1's in specific bytes), “avtostoyanka” (parking lot), *minimal distansiya* (minimum distance), *tasodifiy sferalar* (random spheres), *siqish* (squeeze), *bog‘liqliklar yig‘indisi* (overlapping sums), *yugurish* (runs) va *kraps* (craps) iborat.

Crypt-XS statistik testlar to‘plami Avstraliyadagi Kvinslend Texnologiyalar universitetining Axborot xavfsizligi tadqiqotlar markazidagi tadqiqotchilar tomonidan ishlab chiqilgan va u *chastota* (frequency), *binar hosila* (binary derivative), *nuqtalarni almashtirish* (change point), *yugirishlar* (runs), *ketma-ketlik murakkabligi* (sequence complexity) va *chiziqli murakkablik* (linear complexity) testlaridan iborat bo‘lgan.

NIST statistik testlar to‘plami (NIST Statistical Test Suite) NIST institutining Kompyuter xavfsizligi va Statistik injineriya bo‘limlari tomonidan ishlab chiqilgan. Ushbu to‘plam o‘zida 15 ta statistik testlarni mujassamlashtirgan:

1. Chastota (Frequency) testi;
2. Bloklar uchun chastota (Frequency Test within a Block) testi;
3. Yugurishlar (Runs) testi;
4. Blok ichidagi eng uzun yugurish (Longest Run of Ones in a Block) testi;
5. Birlik matrisa rangini hisoblash (Binary Matrix Rank) testi;
6. Diskret Furye almashtirishlari (Discrete Fourier Transform) testi;

7. Davriy bo‘lmagan qismlar (Non-overlapping Template Matching) testi;
8. Davriy bo‘lgan qismlar (Overlapping Template Matching) testi;
9. Maurerning «Universal statistik» (Maurer’s «Universal Statistical») testi;
10. Chiziqli murakkablik (Linear Complexity) testi;
11. Davomiylik (Serial) testi;
12. Taxminiy entropiya (Approximate Entropy) testi;
13. Ortib boruvchi yig‘indi (Cumulative Sums) testi;
14. Tasodifiy tashriflar (Random Excursions) testi;
15. Tasodifiy tashriflar varianti (Random Excursions Variant) testi.

Quyida NIST statistik testlar to‘plami bilan yaqindan tanishib chiqiladi. Mazkur testlar to‘plami yordamida yagona tasodifiy qiymatni tasodifiylikka tekshirish ketma-ketligi 5.2-jadvalda aks ettirilgan. Ushbu ketma-ketlik umumiy testlash senariysini aks ettirgan bo‘lib, NIST statistik testlar to‘plamidan foydalanib testlashda muhim ahamiyatga ega.

5.2-jadval

Yagona binar ketma-ketlikni baholash muolajasi

Qadam va qadam jarayon	**Izoh**
Sizning nollik gipoteza holatingiz	Binar ketma-ketlikni tasodifiy deb faraz qiling
Statistik testlar ketma-ketligini amalga oshirish	Testlash bitlar kesimida amalga oshiriladi
P – qiymatni hisoblash	$P \in [0,1]$ ga tegishli
P – qiymatni α ga solishtirish	$\alpha \in (0.001,0.01]$ kabi kelgilang. Agar $P \geq \alpha$ bo‘lsa, testdan o‘tgan, aks holda o‘ta olmagan

Mazkur testlash to‘plamida kiritilgan har bir test usuli aynan bir maqsadga qaratilgan bo‘lib, aynan bir holat bo‘yicha baho beradi. Quyidagi 5.3-jadvalda har bir testning maqsadi va baho beruvchi asosiy zaiflik tomoni aks ettirilgan.

5.3-jadval

NIST statistik testlar to‘plamining xususiyatlari

№	**Statistik test**	**Zaiflikni aniqlash**
1.	Frequency	Bir yoki nolni juda ko‘pligini
2.	Cumulative Sums	Ketma-ketlik boshlanishida bir yoki nolni juda ko‘pligini
3.	Longest Runs Of Ones	Birlarni uzoq vaqtli davomiyligi taqsimotining og‘ishini
4.	Runs	Bitlar ketma-ketligida tezkor (sekin) birdan nolga va aksincha o‘tishlarni ko‘rsatuvchi yugirishlarning umumiy katta (kichik) sonini
5.	Rank	Mos tasodifiy ketma-ketlikdan qism takroriyligi natijasidagi rang taqsimotini og‘ishini
6.	Spectral	Bitlar ketma-ketligidagi takrorlanish xususiyatini
7.	Non-overlapping	Kesishmagan shablonlarni qanchalik ko‘p paydo

№	Statistik test	Zaiflikni aniqlash
	Template Matchings	bo‘lishini
8.	Overlapping Template Matchings	Birlarning *m* bitli yugirishlarni paydo bo‘lishini
9.	Universal Statistical	Siqilishni (biror qoniniyatga asoslanishini)
10.	Random Excursions	Tasodifiy yurishda yagona holatga o‘tishlar sonini taqsimotining og‘ishini
11.	Random Excursion Variant	Yagona holatga turli holatlardan o‘tishlarning umumiy soni taqsimotining og‘ishini
12.	Approximate Entropy	*m* bit uzunlikdagi so‘zlar taqsimotining bir xil emasligini.
13.	Serial	*m* bit uzunlikdagi so‘zlar taqsimotining bir xil emasligini. Approximate Entropyga o‘xshash
14.	Linear Complexity	Cheklangan uzunlikdagi (qism) qator uchun chiziqli murakkablikning taqsimotidan og‘ishini

Har bir testni amalga oshirish uchun unga talab etilgan uzunlikdagi tasodifiy qiymat kiritilishi talab etiladi. NIST tomonidan keltirilgan har bir test uchun kiritiladigan tasodifiy qiymatlarga minimal uzunlik talabi qo‘yilgan (5.4-jadval).

5.4-jadval

NIST statistik testlariga kirish qiymatlariga uzunlik talabi

№	Statistik test	Minimal kirish qiymat uzunligi (bit)
1.	Chastota (Frequency) testi	100
2.	Bloklar uchun chastota (Frequency Test within a Block) testi	100
3.	Yugurishlar (Runs) testi	100
4.	Blok ichidagi eng uzun yugurish (Longest Run of Ones in a Block) testi	128
5.	Birlik matrisa rangini hisoblash (Binary Matrix Rank) testi	38912
6.	Diskret Furye almashtirishlari (Discrete Fourier Transform) testi	1000
7.	Davriy bo‘lmagan qismlar (Non-overlapping Template Matching) testi	10^6
8.	Davriy bo‘lgan qismlar (Overlapping Template Matching) testi	10^6
9.	Maurerning «Universal statistik» (Maurer’s «Universal Statistical») testi	387840
10.	Chiziqli murakkablik (Linear Complexity) testi	10^6
11.	Davomiylik (Serial) testi	128
12.	Taxminiy entropiya (Approximate Entropy) testi	100
13.	Ortib boruvchi yig‘indi (Cumulative Sums)	100

№	Statistik test	Minimal kirish qiymat uzunligi (bit)
	testi	
14.	Tasodifiy tashriflar (Random Excursions) testi	10^6
15.	Tasodifiy tashriflar varianti (Random Excursions Variant) testi	10^6

Tasodifiy ketma-ketliklar entropiyasini o‘lchash usullari. Generasiya qilingan psevdotasodifiy ketma-ketliklarni statistik testlar orqali tekshirish bilan har doim ham ularga aniq baho berib bo‘lmaydi. Kalitlarni tasodifiy darajasini tekshirishda odatda ularning entropiya qiymatini o‘lchash muhim ahamiyat kasb etadi.

NIST SP 800-90B nashridagi entropiyani o‘lchash usuli. Ushbu nashrda *min-Entropy – minimal entropiya* usuli keltirilgan bo‘lib, uning ketma-ketligi quyidagicha:

1. Tasodifiy sonlar generatoridan hosil qilingan ketma-ketliklar ma’lum bloklarga ajratilib, to‘plam shaklida ifodalanadi. Bunda agar blok uchunligi n bit bo‘lsa, to‘plamdagi bloklar soni N kamida 2^n ga teng bo‘lishi zarur.
2. To‘plam ichida eng ko‘p takrorlangan qiymat C_{max} ga o‘zlashtiriladi.
3. Ushbu qiymat uchun ehtimollik $p_{max} = {C_{max}}/{N}$ ga teng bo‘ladi.
4. Chegara qiymat $C_{chegara} = C_{max} + 2.3\sqrt{N * p_{max}(1 - p_{max})}$ tenglik orqali hisoblanadi.
5. Chegara qiymat uchun entropiya $H = -\log_2({C_{chegara}}/{N})$ tenglik orqali hisoblanadi.
6. Yakuniy $\text{minimal} - \text{entropiya} = \min(n, H)$ ga ya’ni, ikki qiymatning eng kichigiga teng bo‘ladi.

/dev/random generatorida entropiyani o‘lchash. Ushbu algoritmda muallif tomonidan isbotga ega bo‘lmagan quyidagi entropiyani hisoblash tengligidan foydalanilgan:

$$\Delta_n^1 = time_n - time_{n-1},$$
$$\Delta_n^2 = \Delta_n^1 - \Delta_{n-1}^1,$$
$$\Delta_n^3 = \Delta_n^2 - \Delta_{n-1}^2,$$
$$\Delta_n = \min(|\Delta_n^1|, |\Delta_n^2|, |\Delta_n^3|),$$
$$entropy_n = log_2(\left[\frac{\Delta_n}{2}\right] (mod\ 2^{12})).$$

$time_n$ o‘zgaruvchisi biror manbadagi tashqi hodisani vaqt belgisini ifodalaydi. Har bir manba o‘zining $\{time_n\}_{n\geq 0}$ ketma-ketliklariga ega. $mod\ 2^{12}$ dan foydalanish esa entropiya qiymatini ko‘pi bilan 12 bitga teng bo‘lishini bildiradi.

Yarrow generatorida entropiyani o‘lchash. Mualliflar tomonidan mazkur algoritm uchun entropiyani to‘plash uchun o‘zgacha usuldan foydalanilgan. Har bir hodisalar manbasi uchun alohida entropiyani o‘lchash sanog‘i qo‘yilgan bo‘lib, har bir genetorning ichki holati yangilangandan so‘ng, ular nolga olib kelingan.

Ushbu generatorning keyingi avlodi sanalmish *Fortuna* generatorida esa hodisalar manbasidan kelgan qiymatlarni 32 ta pulga taqsimlangan holda saqlash va

ulardan generator ichki holatini yangilashda o‘zgacha usuldan foydalanish orqali entropiyani hisoblashdan qochilgan.

Bundan tashqari entropiyani hisoblashda ko‘plab usullardan foydalanilgan bo‘lib, ular ichida EGD (Entropy Gathering Daemon) entropiya to‘plovchisida foydalanilgan yondashuv muhim ahamiyat kasb etadi. Ushbu yondashuvga ko‘ra manbadan olingan har bir bayt uchun bir bit entropiyaga ega deb faraz qilingan.

Umumiy holda mavjud entropiyani o‘lchash usullarini turli statistik usullarga va farazlarga asoslanilganini yoki uni hisoblashdan qochilganiga ko‘rish mumkin.

Nazariy savollari:

1. Tug‘ilgan kun muammosi nimaga asoslanadi?
2. Tug‘ilgan kun haqidagi paorodoks usuli qanday amalga oshiriladi?
3. SHA-1 xesh funksiya algoritmiga differensial kriptotahlil usulini qo‘llash bosqichlarini tushuntirib bering.
4. MD4 algoritmi va uning kriptoanalizi natijalari haqida ma’lumot bering
5. MD4 algoritmiga kolliziya hujumini tushintirib bering.
6. Psevdotasodifiy sonlar generatorini baholash usullari
7. Kriptografik psevdotasodifiy sonlar generatori
8. Tasodifiylikka tekshirish testlarining qanday turlari mavjud?
9. Tasodifiy ketma-ketliklar entropiyasini o‘lchash usullari
10. To‘liq tanlash hujumi nimaga asoslanadi
11. Statistik tahlil hujumini tushuntiring

Adabiyotlar va internet resurslar:

1. Xasanov P.F., Xasanov X.P., Axmedova O.P., Davlatov A.B. Kriptotahlil va uning maxsus usullari, O‘quv qo‘llanma, Toshkent, 2010
2. Akbarov D.YE. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanishlari. Toshkent. ”O‘zbekiston markasi“, 2009
3. Л.К.Бабенко, Е.А.Ищукова. Современные алгоритмы блочного шифрования и методы из анализа: учеб. пособие для студентов вузов, обучающихся по группе специальностей в обл. информ. безопасности – М.: Гелиос АРВ, 2006. – 376 с.
4. M.Stamp. Applied cryptanalysis: Breaking Ciphers in the Real World. John Wiley & Sons, Inc, 2007, -P. -417.
5. Б.Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – Москва: ТРИУМФ, 2002.
6. Xasanov P., Xasanov X., Axmedova O., Davlatov A. Kriptotahlil va uning maxsus usullari. O‘quv qo‘llanma.– Toshkent, 2010.
7. O.P.Axmedova, Z.T.Xudoykulov, O. Allanov, I.M.Boyquziyev Kriptoanaliz. O‘quv qo‘llanma. T.: “Iqtisod-Moliya”, 2022. 171 b.
8. Kuryazov D.M., Sattorov A.B., Axmedova B.B. Blokli simmetrik shifrlash

algoritmlari bardoshligini zamonaviy kriptotahlil usullari bilan baholash. O‘quv qo‘llanma. T.: “Aloqachi”. 2017, 228 bet.
9. http://jnicholl.org/Cryptanalysis/Tools/
10. https://www.cryptool.org/en/cto/
11. https://resources.infosecinstitute.com/topic/cryptanalysis-tools/
12. http://rumkin.com/tools/cipher/
13. https://blackarch.org/crypto.html
14. https://www.guballa.de/vigenere-solver
15. https://www.simonsingh.net/The_Black_Chamber/substitutioncrackingtool.html
16. https://www.guru99.com/how-to-make-your-data-safe-using-cryptography.html
17. https://www.cs.bu.edu/~goldbe/teaching/CS558S17/Lab1.pdf

6-ma’ruza. Oqimli shifrlash algoritmlarining kriptotahlili. Kriptotahlilda qo‘shimcha kanallar va yangi texnologiyalardan foydalanish.

Reja:

2.1. Chiziqli, differensial, algebraik va boshqa kriptotahlil usullarining oqimli shifrlash algoritmlariga nisbatan qo‘llanilishi.
2.2. Qo‘shimcha kanallardan foydalanishga asoslangan kriptotahlil usullari.
2.3. Kriptotahlilda yangi texnologiyalardan foydalanish.

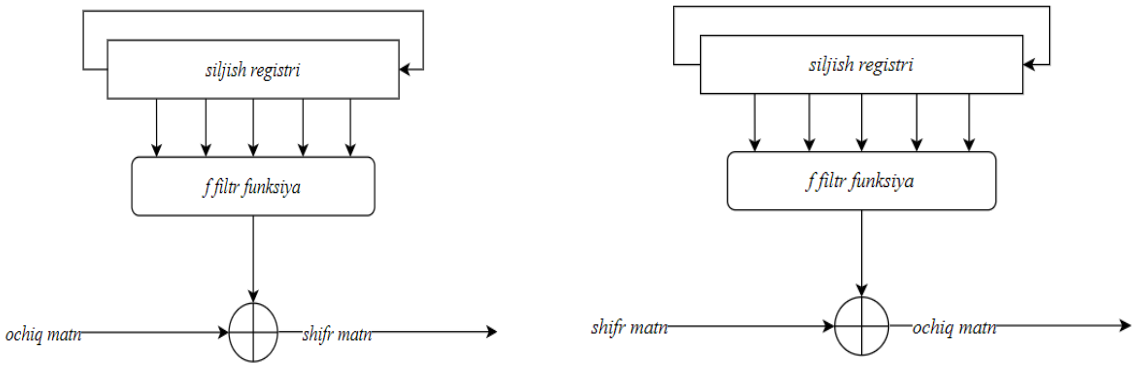
Tayanch iboralar: *Chiziqli kriptotahlil, algebraik kriptotahlil, qo‘shimcha kanallar, yangi texnologiyalar*

2.1. Chiziqli, differensial, algebraik va boshqa kriptotahlil usullarining oqimli shifrlash algoritmlariga nisbatan qo‘llanilishi.

Oqim shifrlash bir martalik bloknot (OTP) shifrlash texnikasiga o‘xshash shifrlashni amalga oshiradi. U maxfiy, tasodifiy ko‘rinadigan ma'lumotlarning katta qismini ishlab chiqaradi va shifrlangan matnni yaratish uchun ularni ochiq matn bilan birlashtiradi. Ochiq matnni shifrlangan matndan ajratib bo‘lmaydi. Tasodifiy ma'lumotlar maxfiy kalitdan olingan va odatda kalit oqimi deb ataladigan bitlar oqimini ifodalaydi. Oqimli shifrlash algoritmlarida maxfiy kalit tomonidan ishga tushiriladigan va har bir shifrlash bosqichidan so‘ng keyingi holatga tarqaladigan ichki shifr holati deb nomlanadigan doimiy xotira mavjud. Bardoshli oqimli shifrlash algoritmlarining chiqishi Pseudo Random Number Generator (PRNG) tomonidan ishlab chiqarilgan bitlar oqimi bilan taqqoslanadi.

Oqimli shifrlash algoritmlarini ishlab chiqishda foydalaniladigan eng mashhur usullardan biri chiziqli bo‘lmagan ikkilik ketma-ketliklarni ishlab chiquvchi generatorlardan foydalanishdir. Ushbu generatorlar ikkilik kalitlar oqimini ishlab chiqaradi, bu juda katta maxfiy kalitni talab qilmasdan muntazam bir martalik shifrlash imkonini beradi. Chiziqli bo‘lmagan oqim shifriga asoslangan odatiy kriptotizimning umumiy ko‘rinishi 1-rasmda tasvirlangan. Ushbu turdagi shifrlarni kichik apparat ko‘rinishida amalga oshirish imkoniyati sababli juda

mashhur hisoblanadi.



1-rasm. Oddiy chiziqsiz oqimli shifrlash tizimi sxemasi

1-rasmda ko‘rsatilgan kriptografik algoritm shifrning ichki holatini ifodalovchi aylanuvchi siljish registrini o‘z ichiga oladi. Kalitning har bir bitini hisoblashdan so‘ng, ichki funksiya ko‘proq entropiyani saqlab qolish maqsadida chiziqli funktsiya orqali ichki holatni yangilaydi. Chiqish komponenti keyingi kalit oqimi bitini hisoblash uchun chiziqli bo‘lmagan $f(\cdot)$ filtr funksiyasini qo‘llaydi. Kalit oqim bitlari XOR ($\oplus$) operatsiyasi bilan, jo‘natuvchi tomonidan ochiq matn bitlarini shifrlash uchun ishlatiladi (1a-rasm). Olingan shifrlangan matn xavfsiz bo‘lmagan kanal orqali uzatiladi. Qabul qiluvchi (1b-rasm) aynan bir xil hisob-kitoblarni amalga oshiradi va kalit oqimi bitlari bilan birgalikda shifrlangan matn bitlaridan ochiq matnni hosil qilish uchun XOR operatsiyasini qo‘llaydi. Shifrlangan matnga allaqachon kiritilgan kalit oqimi bitlari bekor qilinadi va qabul qiluvchida ko‘rinadi asl ochiq matn bitlari hosil bo‘ladi.

Adabiyotlarda kriptotahlil deb ataladigan oqimli shifrlash algoritmlariga nisbatan kriptografik hujumlarda qo‘llaniladigan ko‘plab ilg‘or va murakkab kriptografik hujum metodologiyalari va usullari taklif qilingan. Mazkur maqolada oqimli shifrlash algoritmiga nisbatan kriptotahlil usullarining qo‘llanilish texnikalari yoritilgan.

Korrelyatsion hujum

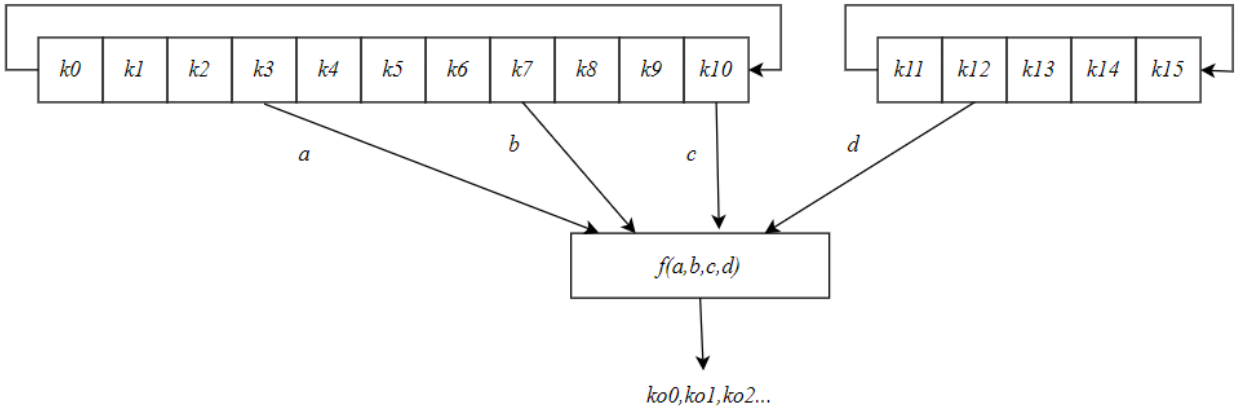
Korrelyatsiya hujumining samarali qo‘llanishiga imkon beruvchi shifrning zaifligi - bu kirish sifatida ishlatiladigan ba'zi ichki holat bitlari tomonidan yuqori ta'sir ko‘rsatadigan statik jihatdan bog‘langan kalit bitlarining generatsiya qilinishidir. Shuning uchun, ushbu kirish bitlari uchun har qanday taxmin, ehtimol, chiqish bitlariga bevosita ta'sir qiladi. Statistik tahlil usullaridan foydalangan holda, tahlilchi ushbu ichki holat bitlari haqida ma'lumot olishi mumkin.

Korrelyatsion hujumning afzalligi shundaki, tahlilchi yashirin asosiy nomzodlar to‘plamini sezilarli darajada qisqartirishi mumkin. Algoritm tarkibida tartibsizlik qanchalik keng tarqalgan bo‘lsa, kirish va chiqish munosabatlarini tahlil qilishda shunchalik ko‘p ma'lumot sizib chiqadi. Ayniqsa, oqim shifrlari ko‘pincha korrelyatsion hujumlarga moyil. Adabiyotlarda oqimli shifrlash algoritmlariga nisbatan tezkor va optimallashtirilgan korrelyatsion hujumlarni qo‘llash bo‘yicha ko‘plab takliflar mavjud.

Oqimli shifrlarda korrelyatsion hujum usuli ko‘pincha bir nechta ketma-ket shifrlash chiqishlarida qo‘llaniladi. Oqimli shifrda asosiy holatiga erishilgandan

so‘ng, avval tanlangan bir nechta bit keyingi iteratsiya uchun kirish bilan bir-biriga mos kelishi mumkin. Bundan tashqari, farqlar har bir ishlab chiqarilgan ketma-ketlik bo‘yicha tekshirilishi mumkin, bu esa tahlilchiga oldingi va keyingi holatlarni o‘zaro bog‘lash imkonini beradi. Ko‘p variantlarni shifrlash natijalarining kombinatsiyasi to‘liq ichki holat haqida ko‘proq ma'lumot olishga olib keladi. Eng ko‘p nomzodlar to‘plami haqiqiy maxfiy kalitdan olingan ichki holatni o‘z ichiga olishi mumkin.

Korrelyatsion hujum mohiyatini tushuntirish uchun tanlab olingan zaif oqimli shifrlash algoritmi 2-rasmda keltirilgan. Tasvirlangan algoritm chiziqli bo‘lmagan $f(\cdot)$ filtr funksiyasiga tayanadigan chiqish komponentiga ega oddiy siljish registriga asoslangan oqimli shifrlash algoritmidir.



2-rasm. k maxfiy kaliti bilan ishga tushirilgan korrelyatsion hujumga zaif oqimli shifrlash algoritmi

2-rasmda ko‘rsatilgan shifr ikkita alohida siljish registrlaridan iborat va 16 ta maxfiy kalit bitlari bilan ishga tushirilgan kattaroq ichki holatga ega. Bundan tashqari, u toq va juft bitlarni ajratishga asoslangan “bo‘lib tashla va egalik qil” hujumini samarali qo‘llashga imkon bermaydi. Algoritm chiziqli bo‘lmagan filtr funktsiyasidan foydalanadi, ushbu funksiya kirishga nisbatan statistik jihatdan qarama-qarshi bo‘lgan chiqishlarni hosil qiladi.

Chiziqsiz $f: F_4 \to F_2$ filtr funksiyasining ifodalanishi:

$$f(a,b,c,d) = ((a \wedge b \wedge c) \vee (\bar{a} \wedge \bar{b} \wedge \bar{c})) \oplus d$$

Filtr funktsiyasi to‘rtta $(a, b, c$ va $d)$ bitlarini kirish sifatida oladi va belgilangan chiziqli bo‘lmagan tenglamani natijasini hisoblash orqali bitta chiqish bitini ishlab chiqaradi. 1-jadvalda $f(\cdot)$ ning kiritish-chiqish munosabatini ifodalovchi mantiqiy jadval (rostlik jadvali) tasvirlangan.

1-jadval. $f(\cdot)$ ning rostlik jadvali

$abcd$	$f(a,b,c,d)$
0000	1
0001	0
0010	0
0011	1
0100	0
0101	1
0110	0
0111	1

1000	0
1001	1
1010	0
1011	1
1100	0
1101	1
1110	1
1111	0

Funksiyaning og‘ishi uning 1-jadvalda keltirilgan kirish-chiqish munosabatiga qarab osongina aniqlanadi. $f(\cdot)$ balanslashgan chiqish hosil qilsada, ya'ni ishlab chiqarilgan chiqish bitlarining yarmi nolga teng va ularning yarmi bitta bo‘lsa-da, d kirish biti a, b va c kirish bitlariga qaraganda chiqishga sezilarli darajada ta'sir qiladi. 1-jadvaldagi to‘rtta belgilangan qatorlar abc kirish bitlari bir-biriga teng bo‘lgan holatlarni ko‘rsatadi.

$abcd$ ning 16 ta holatidan 12 tasida ko chiqish biti kirish biti d bilan aynan bir xil. Shu sababli, tasodifiy taqsimlangan kirish bitlari bilan o‘rtacha $\frac{3}{4}$ holatda $ko = d$, faqat $\frac{3}{4}$ holatda $ko \neq d$ degan xulosaga kelish o‘rinlidir. Demak, ikkinchi siljish registri ishlab chiqarilgan kalit oqimi bitlarining qiymatiga ko‘proq ta'sir qiladi.

Faraz qilaylik, tahlilchi ko_0 kalit oqimining birinchi bitini tiklaydi. U ko_0 ni $f(\cdot)$ funksiyasi orqali $f(k_3, k_7, k_{10}, k_{12})$ argumentlari bilan hisoblanganligini biladi. Shuning uchun u $\frac{3}{4}$ ehtimol bilan d kirish uchun to‘g‘ri qiymatni aniqlay oladi, bu ko_0 uchun o‘n uchinchi maxfiy kalit biti k_{12}. Garchi bu mumkin bo‘lgan nomzod kalitlar to‘plamini sezilarli darajada kamaytirsa ham, korrelyatsiya hujumining samarasi ketma-ket bir necha marta qo‘llanilganda yaxshiroq namoyon bo‘ladi.

$k_0, k_1, k_2, \ldots, k_{15}$ maxfiy kalit bitlari siljish registrlariga o‘rnatilganda k_3, k_7, k_{10}, k_{12} bitlar ko_0 chiqish bitini hisoblashda foydalanilsa, beshta iteratsiyadan keyin ikkinchi registr to‘liq aylanib bo‘ladi va k_8, k_1, k_4, k_{12} bitlar ko_5 chiqishni hisoblashda foydalaniladi. Ikkala holatda ham ko_0 va ko_5 chiqishlarni hisoblashda $f(\cdot)$ ga to‘rtinchi kirish biti k_{12} maxfiy kalit bitidir.

Agar $ko_0 \neq k_{12}$ bo‘lishi $\frac{1}{4}$ ehtimollik bilan bajarilsa $ko_5 \neq k_{12}$ ham $\frac{1}{4}$ ehtimollik bilan bajariladi. Agar $ko_0 = ko_5$ bo‘lsa, $ko_0 = ko_5 \neq k_{12}$ tenglikning bajarilish ehtimolligi $\frac{1}{4} \times \frac{1}{4} = \frac{1}{16}$ ga tengligini va sezilarli darajada pasayishini taxmin qilishi mumkin. Buning sababi shundaki, ikkala holatda ham (mustaqil) kirish bitlari a, b va c bir-biriga teng bo‘lishi ehtimoldan yiroq emas. Kirish va chiqish bitlarining kombinatsiyasiga qaratilgan korrelyatsion hujum ancha katta afzalliklarni beradi. To‘g‘ri ba’zida kalit bitini taxmin qilish ehtimoli shifrdagi mustaqil tekshiriladigan statistik moyillikka mos keladigan barcha ehtimoliy variantlar ko‘paytmasidan olinishi ham mumkin.

ko_0 va ko_5 chiqishlarga o‘rnatilgan korrelyatsion hujum qayta tiklangan kalitlar oqimi to‘plamidagi yana boshqa bitlar uchun ham amal qiladi. Bir-biridan

beshta pozitsiyada joylashgan kalit oqimi bitlarining har bir jufti uchun ($ko_i = ko_i + 5$ bu erda $i \in \{0, \ldots, 10\}$), ularning maxfiy kalitning mos keladigan biti bilan aynan bir xil bo‘lish ehtimoli $\frac{15}{16}$ ga teng. Ushbu shifrning xususiyatlari yanada yaxshiroq (lekin murakkabroq) korrelyatsion hujumga ham imkon beradi.

[23] ishda korrelyatsiya hujumiga qarshi himoyasiz keng tarqalgan shifrlash algoritmi keltirilgan va kriptografik algoritmning bir qismi bo‘lgan chiqish bitlarini tanlash funksiyasidagi statistik bog‘liqlik yordamida maxfiy kalitni qanday tiklash ko‘rsatilgan. Bu erda keltirilgan misoldan biroz farq qilsa-da, hujum ichki holat bitlari haqidagi ma'lumotlarni o‘rganish uchun korrelyatsion zaiflikdan ham foydalanadi.

Faraz qilish va aniqlash hujumi

Adabiyotlarda keltirilgan ko‘plab tavsiyalarga qaramay [24-26], ayrim xususiy oqim shifrlari kalit oqimi bitlarini hisoblash uchun to‘liq ichki holatdan foydalanmaydi. Bunday yaratilgan arxitektura asosida yaratilgan algoritmlar tahlilchiga faraz qilish va aniqlash hujumini amalga oshirish imkonini beradi. Ushbu hujum filtr funksiyasiga kirish sifatida faqat bir nechta ichki holat bitlari berilishidan foydalanadi. Faqat shu bitlar hisoblangan kalit oqimi bitlarining qiymatini aniqlaydi.

Bunday hujumni amalga oshirish uchun tahlilchi faqat ishlatilgan bitlarni taxmin qiladi, chiqishni hisoblaydi va uni haqiqiy algoritmdan olingan tegishli chiqish bitlariga nisbatan baholaydi. Baholash darhol taxmin qilingan nomzodlarning ko‘pchiligi uchun qarama-qarshilikka olib keladi. Baholashdan so‘ng, ichki holat mos ravishda yangilanadi va faqat qo‘shimcha talab qilinadigan bitlar taxmin qilinadi.

[27-33] ishlarda turli kriptografik algoritmlarga nisbatan faqarz qilish va aniqlash hujumlarini amalga oshirish usullarini ko‘rsatadigan bir nechta samarali, ammo biroz murakkab misollar mavjud. Murakkab va optimallashtirilgan usullarning tafsilotlarini tushunish murakkab bo‘lganligi sababli ushbu tahlil usulining oqimli shifrlash algoritmiga nisbatan qo‘llanishini 2-rasmda keltirilgan sodda variantdagi elementar oqimli shifrlash algoritmi sxemasi va boshqa filtr funksiyasi misolida tushuntiriladi.

Chiziqsiz $f: F_4 \to F_2$ filtr funksiyasining ifodalanishi:

$$f(a, b, c, d) = (\bar{a} \wedge b) \oplus \bar{c} \oplus d$$

Filtr funktsiyasi to‘rtta (a, b, c va d) bitlarini kirish sifatida oladi va belgilangan chiziqli bo‘lmagan tenglamani natijasini hisoblash orqali bitta chiqish bitini ishlab chiqaradi. 2-jadvalda $f(\cdot)$ ning kiritish-chiqish munosabatini ifodalovchi rostlik jadvali tasvirlangan. E'tibor berish joizki, c va d har doim hisoblangan kalit oqimi bitiga ta'sir qiladi, a va b ning ta'siri esa bir-biriga bog‘liq.

2-jadval. $f(\cdot)$ ning rostlik jadvali

$abcd$	$f(a, b, c, d)$
0000	1
0001	0
0010	0
0011	1

0100	0
0101	1
0110	1
0111	0
1000	1
1001	0
1010	0
1011	1
1100	1
1101	0
1110	0
1111	1

Tahlilchi shifrlash holatidagi faraz qilish va aniqlash hujumi uchun imkon beradigan zaifliklarni qidiradi. U chiziqli bo‘lmagan funksiyani hisoblash uchun zarur bo‘lgan tegishli shifr tuzilishini va belgilangan kirish bitlarini tekshirishdan boshlaydi.

Chiqishdagi bir bitni hisoblash uchun shifr bir vaqtning o‘zida faqat to‘rtta kirish bitini talab qiladi. 16 bitli maxfiy kalit ichki holatni ishga tushirganligi sababli ichki holat 16 bitli entropiyaga ega. Shunga qaramay, agar chiquvchi bitni hisoblash uchun har safar ichki holatning faqat to‘rtta biti ishlatilsa, ayniqsa, taxmin qilingan qiymatlar keyingi chiqish bitini hisoblash uchun foydalanilmasa, murakkablikni oshirish va bir vaqtning o‘zida barcha bitlarni taxmin qilish mantiqiy emas. Faraz qilish va aniqlash hujumining kuchi har safar faqat haqiqatda ishlatiladigan bitlarni taxmin qilish va ularning chiqishi kalit oqimiga zid kelmasligiga ishonch hosil qilishdan iborat.

Tahlilchi 2-jadvalda ko‘rsatilgan $abcd$ ning 16 xil kirish bitlari bo‘yicha to‘liq qidiruvni osonlik bilan amalga oshirishi mumkin va har bir $f(a,b,c,d)$ uchun natijani hisoblab chiqadi hamda chiqishni qayta tiklangan kalit oqimi bitlaridan biriga nisbatan solishtirib ko‘radi. Bu ushbu bitlarga mos nomzodlarni ajratish imkonini beradi.

$f(\cdot)$ funksiyasi balanslashgan, shuning uchun u $abcd$ ning barcha 16 xil qiymatlari uchun sakkiz martadan nolga va birga teng qiymat qaytaradi. Shuning uchun, kalit oqimi biti nolga teng bo‘lsa, $abcd$ ning qiymatlarida chiqishni birga olib keladigan sakkizta nomzodi inkor qilinadi.

$f(\cdot)$ ni hisoblash va ikkala registrda bitta aylanishni amalga oshirgandan so‘ng, keyingi kalit oqimi biti boshqa to‘rt xil maxfiy kalit bitlari bilan hisoblanadi. Tahlilchi yana yuqoridagi texnikadan foydalanadi va ikkinchi kalit oqimi biti uchun noto‘g‘ri $abcd$ nomzodlarini inkor qiladi. Har bir ketma-ket chiqish biti uchun kirishni boshqalardan mustaqil ravishda baholash mumkin bo‘lganda, hisoblash murakkabligi sezilarli darajada pasayadi.

Tahlilchi ketma-ket 16 ta $ko_0, ko_1, ko_2, \dots, ko_{15}$ kalit oqimi bitlarini tikladi deb faraz qilib, 3-rasmda ko‘rsatilgan shifrga qanday qilib faraz qilish va aniqlash hujumini qo‘llashi mumkinligini ko‘rib chiqamiz. Chiqish bitlari oqimi bitini

hisoblashda foydalaniladigan maxfiy kalit bitlarini aniqlashtirish uchun $f(\cdot)$ filtr funksiyasining dastlabki 5 ta qadami 3-jadvalda keltirilgan.

3-jadval. Kalit oqimining dastlabki beshta bitini aniqlash formulalari

$ko_0 = f(k_3, k_7, k_{10}, k_{12})$
$ko_1 = f(k_4, k_8, k_0, k_{13})$
$ko_2 = f(k_5, k_9, k_1, k_{14})$
$ko_3 = f(k_6, k_{10}, k_2, k_{15})$
$ko_4 = f(k_7, k_0, k_3, k_{11})$

To‘rtta maxfiy kalit bitlari k_3, k_7, k_{10}, k_{12} birinchi ko_0 kalit oqimi bitini hisoblash uchun ishlatiladi. Tahlilchi 4 ta k_3, k_7, k_{10}, k_{12} maxfiy kalit bitlari uchun barcha $2^4 = 16$ nomzodni taxmin qilishi kerak. Olib tashlangandan so‘ng, nomzodlar to‘plamining faqat yarmi qoladi. Shunday qilib, 4 bitning har bir taxmini raqibga 1 bit entropiyani yo‘q qilishga imkon beradi. 2^4 ta hisoblashdan keyin $\frac{2^4}{2} = 2^3$ mumkin bo‘lgan nomzodlardan iborat kichikroq to‘plam qoladi.

Ikkinchi kalit oqimi ko_1 bitini baholash tahlilchidan maxfiy kalitning yana 4 bitini taxmin qilishni talab qiladi, bu safar k_4, k_8, k_0, k_{13} uchun. Shunda yana nomzodlar to‘plamining faqat yarmi qoladi. Ushbu to‘rtta maxfiy kalit bitlari ko_0 ni hisoblash uchun ishlatiladiganlardan butunlay farq qiladi. Aslida, raqib endi 8 ta mustaqil maxfiy kalit bitini, ya'ni $k_3, k_7, k_{10}, k_{12}, k_4, k_8, k_0, k_{13}$ ni taxmin qildi. Shunga qaramay, ko_1 ni hisoblaydigan bitlarni taxmin qilgandan so‘ng, tahlilchi faqat $2^3 \times 2^4 = 2^7$ nomzodga ega. Barcha 2^7 nomzod uchun kalit oqimi bitini hisoblangandan so‘ng, ularning yarmi yana bir bor yo‘q qilinadi. Shunda maxfiy kalitning 8 bitini ifodalovchi qiymatlarga ega bo‘lgan atigi 2^6 ta mumkin bo‘lgan nomzodlar to‘plamini qoladi.

Tahlilchi xuddi shu texnikani uchinchi kalit oqimi biti ko_2 uchun k_5, k_9, k_1, k_{14} bitlarni tanlash yo‘li bilan qo‘llaydi. U 12 ta maxfiy kalit bitini taxmin qiladi va 2^{10} ta hisob-kitobdan keyin faqat 2^9 ta mumkin bo‘lgan nomzodlar qoladi. To‘rtinchi kalit oqimi biti ko_3 esa k_6, k_{10}, k_2, k_{15} maxfiy kalit bitlari bilan hisoblanadi. E'tibor berish joizki, maxfiy kalit biti k_{10} allaqachon kalit oqimining birinchi biti ko_0 ni hisoblash uchun taxmin qilingan. Bu esa ikkita (qisman) mustaqil muammolarni taqdim etadi, bu xususiyat "bo‘lib tashla va egalik qil" hujumiga o‘xshash.

ko_3 ni baholash juda o‘ziga xos, bu safar raqib to‘rtta o‘rniga faqat uchta bitni taxmin qilishi kerak. Bitlarni taxmin qilgandan so‘ng va kalit oqimiga qarshi nomzodlar to‘plamini baholashdan oldin, nomzodlar to‘plamining o‘lchami 2^{12} ni tashkil qiladi. Ushbu to‘plamdagi nomzodlarning har biri uchun hisoblash amalga oshirilishi zarurligi sababli, hujumning umumiy murakkabligi 2^{12} gacha oshadi. Shunga qaramay, ko_3 ni baholagandan so‘ng, tahlilchi 15 ta maxfiy kalit bitini taxmin qildi va atigi 2^{11} ta nomzoddan iborat to‘plamga ega bo‘ladi.

Beshinchi kalit oqimi bit ko_4 ni hisoblash uchun hali ham hisobga olinmagan oxirgi maxfiy kalit biti k_{11} talab qilinadi. k_{11} ni taxmin qilish hujumning hisoblash murakkabligini biroz oshiradi. Dastlab nomzodlar to‘plami ikki barobarga, ya’ni 2^{12} ga ko‘payadi va 2^{12} hisob-kitobdan so‘ng darhol yana ikki barobar qisqarib, 2^{11}

nomzodga aylanadi. Nomzodlarni tekshirishdan o‘tkazish uchun jami ikki baravar eng katta hisob 2^{12} va kichikroq nomzodlar to‘plamida bajarilgan ba'zi ahamiyatsiz kichikroq hisoblashlar talab qilinadi. Bu talab qilingan umumiy 2^{16} = 65536 hisob o‘rniga $(2\times2^{12})+2^{10}+2^{7}+2^{4}=9360\approx2^{13}$ hujum murakkabligiga olib keladi.

Differensial kriptotahlil

1977 yilda joriy etilgan ma'lumotlarni shifrlash standarti (DES) ko‘p yillar davomida nazariy jihatdan xavfsiz deb hisoblangan. Bu ishonch 1991 yilgacha davom etdi, Biham va Shamir o‘zlarining [15] ishida DESga o‘xshash shifrga kriptografik hujum qilish mumkinligini ko‘rsatdi. Ular differensial kriptoanaliz sifatida joriy qilgan yangi hujum texnikasidan foydalanishgan.

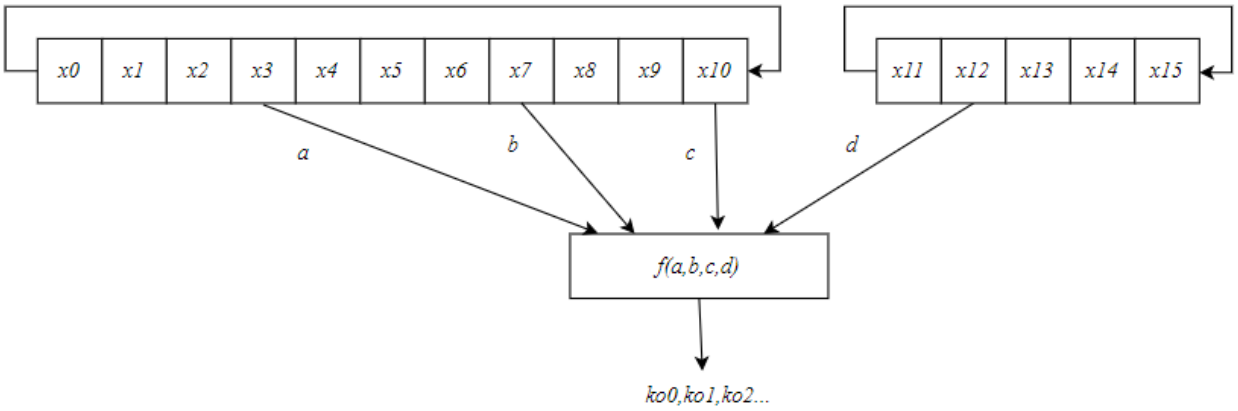
DES ning dastlabki arxitekturasi uchun mas'ul bo‘lgan IBM kompaniyasi [16] ushbu maxsus hujum texnikasi bilan 15 yildan ko‘proq vaqt davomida tanish ekanliklarini da'vo qilishgan, bundan tashqari, ular DESda differensial kriptotahlilni imkon qadar oldini olish uchun o‘z bilimlaridan foydalanganliklarini ta’kidlashgan.

Oradan ikki yil o‘tgach, Biham va Shamir DES kriptografik algoritmiga nisbatan maxsus hujumni amalga oshirish bo‘yicha tadqiqot natijalarini [17] nashr etdilar. Hujum juda katta miqdordagi to‘plangan ma'lumotlarni talab qiladi va shuning uchun natijalar faqat nazariy hisoblangan. Lekin ularning ushbu tadqiqoti ko‘plab tadqiqotchilarni blokli shifrlar [18, 19, 20] va oqimli shifrlar [21, 22, 23] uchun differentsial hujum texnikasini yanada o‘rganish va optimallashtirishga ilhomlantirdi.

Differensial kriptotahlilning qo‘llanilishi ko‘p jihatdan ma'lum darajada farq qiladigan o‘xshash shifrlashlar to‘plamini yig‘ish imkoniyatiga bog‘liq. To‘g‘ridan-to‘g‘ri yondashuv shifrning ichki holatini to‘g‘ridan-to‘g‘ri ta'sir qiladigan va ozgina o‘zgartiradigan usulni topishdir. Bunday texnikani amaliyotda qo‘llash uchun ko‘pincha kriptotizimlarning qo‘shimcha komponentlari qasddan ichki holatda kerakli farqni hosil qilish uchun ishlatiladi. Bunday komponentlarga misol sifatida ichki holatni ishga tushirish tartibi, kalitlarni generatsiya qilish sxemalari va tasodifiy sonlar generatorlari kiradi. Ushbu komponentlarni nazorat qilish orqali tahlilchi ko‘pincha kerakli o‘zgarishlarni oldindan aytib berishi va oldindan hisoblashi mumkin.

Shifrni ishga tushirish protsedurasi tahlilchiga ma'lum bir pozitsiyada bitta ichki holat bitini o‘zgartirishga imkon berishi mumkin. Bunday kichik o‘zgarish to‘g‘ridan-to‘g‘ri boshqa chiqishga olib kelishi mumkin, bu o‘zgartirilgan bit filtr funktsiyasi uchun muhim kirish ekanligini ko‘rsatadi. Agar o‘zgarish mos keladigan kalit oqimi bitiga ta'sir qilmasa, bu bit filtrlash funktsiyasi uchun ahamiyatsiz kirish ekanligini ko‘rsatadi.

2-rasmda tasvirlangan chiziqli bo‘lmagan oqimli shifrlash algoritmi chiziqsiz filtr funksiyasidan foydalanadi.



2-rasm. Chiziqsiz oqimli shifrlash algoritmi

Chiziqsiz $f: F_4 \to F_2$ filtr funksiyasining ifodalanishi:

$$f(a,b,c,d) = (\bar{a} \wedge b) \oplus \bar{c} \oplus d$$

Ko‘pgina kriptotizimlar shifrlashga yangilik kiritish uchun tasodifiy qiyinchiliklardan foydalanadilar. Ushbu misolda muammolar 16-bitli tasodifiy qiymatdan iborat bo‘lib, u *nonce n* deb ataladi. Bundan tashqari, registrlarga k bitlari *nonce n* bilan XOR amali yordamida yuklanadi. Aniqroq aytganda, ishga tushirish $k_i \oplus n \to x_i$ $(i \in \{0, \ldots, 15\})$ifoda yordamida amalga oshiriladi.

Kriptotizimga nisbatan ikkita qo‘shimcha hujum vektori amalga oshiriladi. Tahlilchi n ustidan to‘liq nazoratga ega va u autentifikatsiyaga urinishdan istalgan vaqtda oddiy kalit oqimini chaqirishi va kuzatishi mumkin. Bu unga differensial kriptoanalizni quyidagi tarzda amalga oshirish imkonini beradi. Birinchidan, u $nonce\ n$ yordamida autentifikatsiya qiladi va birinchi hisoblangan kalit oqimi biti ko_0 ni aniqlaydi. Shundan so‘ng, tahlilchi $nonce\ n$ ning to‘rtinchi biti n_3 ni taxmin qiladi va muqobil n' ni aniqlashga harakat qiladi. Keyin, u n_3 bilan qayta autentifikatsiya qiladi va hisoblangan ko_0' bitini avval aniqlangan kalit oqimi biti ko_0 bilan solishtiradi.

Ikkita autentifikatsiyadan so‘ng, raqib x_3 ning haqiqiy qiymatini tiklay olmaydi. Biroq, u ikkita autentifikatsiya seansining ichki holati o‘rtasidagi farq x_3 bitini inkor qilish ekanligini aniqladi. Bundan tashqari, x_3 biti filtr funksiyasiga a kirishini ifodalaydi, bu esa o‘z navbatida ko_0 va ko_0' autentifikatsiyalari uchun birinchi kalit oqimi bitini hisoblash uchun ishlatiladi. E'tibor bering, x_3 bilan ifodalangan b kirish $n_7 = n_7'$ bo‘lganligi sababli $nonce$ tomonidan o‘zgartirilmagan. Xuddi shu narsa $nonce$ning to‘rtinchi biti o‘zgartirilganligi sababli c va d kirishlari uchun ham amal qiladi.

Filtr funksiyasining kirish-chiqish munosabati a kirish qiymati faqat b kiritish rost bo‘lgandagina muhimligini ko‘rsatadi. Birinchi kalit oqimi biti a kirish sifatida berilgan x_3 va b kirish sifatida esa x_3 bilan hisoblanadi. Shunday qilib, x_3 faqat $x_7 = 1$ bo‘lganda ko_0 kalit oqimi bitiga ta'sir qiladi. Agar $ko_0 = ko_0'$ bo‘lsa, tahlilchi $x_7 = 0$ degan xulosaga kelishi mumkin. Xuddi shunday, $ko_0 \neq ko_0'$ bo‘lsa $x_7 = 1$ deb xulosa qilish mumkin.

Xulosa qilib aytganda, mazkur shifrga differensial hujum oddiygina to‘rtinchi bitni taxmin qilib, qayta autentifikatsiya qilishda ishlatish orqali o‘tkazilishi mumkin. Ikkala autentifikatsiyada birinchi hisoblangan kalit oqimi biti o‘rtasidagi

kuzatilgan farqlar x_7 qiymatini ochib beradi. n_7 va x_7 ni bilgan holda, maxfiy kalitning k_7 biti ni oddiygina $k_7 = x_7 \oplus n_7$ hisoblash orqali tiklash mumkin.

Ushbu maxsus misol faqat ikkita autentifikatsiyani amalga oshirish va ahamiyatsiz hisoblash murakkabligi bilan maxfiy kalitning bir bitini qanday tiklashni ko‘rsatadi. Oqimli shifrlash jarayoni muntazam ravishda davom etganligi sababli, maxfiy kalitning ko‘proq bitlarini tiklash uchun xuddi shu usuldan takroran foydalanish mumkin. n_4 bitini bir marta o‘zgartirish va ko_0 dagi farqni kuzatish x_8 ni aniqlash mumkin.

Differensial kriptotahlil maxfiy kalitni qayta tiklashning samarali usullaridan hisoblanadi. Ehtiyotsiz ishlab chiqilgan ba'zi kriptotizimlar shu qadar zaifki, ularga differensial hujumni amaliy qiyinchiliklarsiz qo‘llash ham mumkin. Masalan, [24,25] va [26-28] da taqdim etilgan MIFARE Classic va iClass shifrlash algoritmlari amaliy differensial hujumga amaliy hisoblashlar darajasida zaifdir. Ikkala algoritm ham kirishni hisoblangan chiqish maxfiy kalit haqidagi ma'lumotlarni sizdiradigan ko‘rinishda manipulyatsiya qilishga imkon beradi.

Differensial hujum ko‘pincha ma'lum kirish-chiqish farqlarini talab qiladi. Kriptotizimni ishga tushirish har doim ham raqibga ichki holatda bunday farqlarni qo‘llashga imkon bermasligi mumkin. Shunga qaramay, har doim bog‘liqliklarni aniqlash va oldindan belgilangan shartlarga javob beradiganlarni filtrlash imkoniyati mavjud. Bundan tashqari, tug‘ilgan kun paradoksiga ko‘ra [29], tahlilchi hujumni muvaffaqiyatli amalga oshirish uchun to‘plashi zarur bo‘lgan bog‘liqliklar soni odatda his qilinadigan raqamlardan ancha kichikroq.

Algebraik kriptotahlil

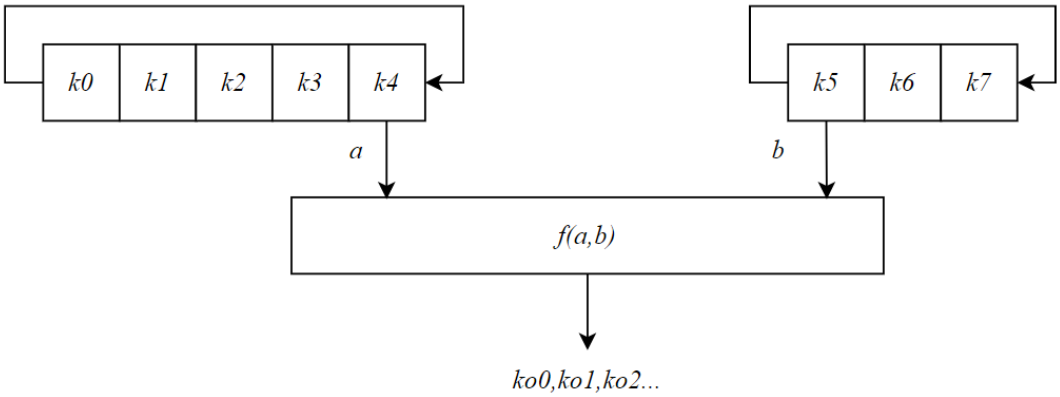
Bir qancha kriptotahlil usullarining metodologiyalari chiziqli bo‘lmagan funksiyaga hujum qilish orqali oqimli shifrlash algoritmlarining hisoblash murakkabligini kamaytirishga qaratilgan. Biroq, ba'zi algoritmlari bir yoki bir nechta chiziqli komponentlardan iborat. Bunday shifrlash algoritmlari algebraik kriptotahlil hujumlariga nisbatan zaifdir. [30-33] ishlarda algebraik hujumlarga oid bir qancha dastlabki tadqiqotlar natijalari keltirilgan. So‘nggi o‘n yillikda hujumlarni umumlashtirish va optimallashtirishning bir nechta usullari taklif qilingan [34-42].

Chiziqli mantiqiy funksiyaning asosiy xususiyati baholashni kechiktirish imkoniyatidir. Kriptotahlil vaqtida rasmiylashtiriladigan hisoblash muammolarini mantiqiy tenglamalar tizimi sifatida tasvirlash mumkin [43]. Natijalarni to‘g‘ridan-to‘g‘ri hisoblash o‘rniga, bu tenglamalarning kombinatsiyasini esa tenglamar sistemasini yechishning Gauss usuli kabi taniqli texnikalar yordamida yechish mumkin [44-45].

Mantiqiy algebraga ko‘ra $f \in F_2$ funksiya o‘z sohasidagi istalgan (x, y) juftlik elementlar uchun $f(x \oplus y) = f(x) \oplus f(y)$ tenglikni qanoatlantirsa chiziqli bo‘ladi. Bundan tashqari, mantiqiy chiziqli funksiya kirish o‘zgaruvchilari har doim yoki hech qachon chiqishga ta'sir qilmasligini belgilaydi. Shunday qilib, chiziqli funksiya tomonidan hisoblangan chiqish bitlarini kuzatish kirish bitlarining mos keladigan o‘zgarishlari orasidagi chiziqli munosabatni ochib beradi. Ta'sir qilingan chiqish bitlarining ketma-ketligi kirish bitlari sonidan oshib ketganda, tenglamalar tizimini murakkab hisob-kitoblarni bajarmasdan hal qilish kifoya. Aksincha, chiziqli

bo‘lmagan funksiya teskari jarayonni qiyinlashtiradi, chunki alohida kirish bitlarining ta'siri ushbu bitlarning haqiqiy qiymatiga bog‘liq. Chiziqli funksiyadan farqli o‘laroq, har bir kirish uchun amal qiladigan chiziqli bo‘lmagan funksiyalar uchun tenglamalarni umumlashtirish ancha qiyin hisoblanadi.

3-rasmda ko‘rsatilgan chiqish bitini chiziqli funksiya yordamida hisoblashga asoslangan shifrlash algoritmiga nisbatan algebraik kriptotahlil o‘tkazish jarayonini ko‘rib chiqamiz. U ikkita juda kichik bit bo‘yicha siljish registrlaridan iborat bo‘lib, ularning ikkalasi ham keyingi kalit oqimi bitini ishlab chiqarish uchun chiziqli filtr funktsiyasi $f(\cdot)$ ga bitta kirish bitini etkazib beradi.



3-rasm. Filtr funksiyasi chiziqli bo‘lgan oqimli shifrlash algoritmi

$f: F_4 \to F_2$ filtr funksiyasining ifodalanishi:

$$f(a,b) = a \oplus b$$

XOR operatori bitlar ustida amalga oshriladigan chiziqli amal bo‘lib, tahlilchiga tenglamalar tizimini tuzishga imkon beradi. Quyidagi $ko_0 ko_1 ko_2 ko_3 ko_4 ko_5 ko_6 ko_7 = 10110101$ kalit oqimi bitlarini ko‘rib chiqamiz. 1-jadval to‘rtta ustundan iborat bo‘lib, ularning har biri baholash bosqichini ifodalaydi. Uch bosqichdan so‘ng, ko‘rib chiqilgan kalit oqimiga mos keladigan sakkizta tenglik hosil bo‘ladi. Ushbu tengliklar maxfiy kalit bitlarini ifodalaydigan tenglamalarda foydalaniladi.

1-jadval. $ko_0 \dots ko_7 = 10110101$ *chiqishga nisbatan algebraik tenglamalarni shakllantirish*

$ko_0 = k_2 \oplus k_5$	$k_5 = k_2 \oplus ko_0$	$k_5 = k_2 \oplus 1$	$k_5 = \overline{k_2}$
$ko_1 = k_3 \oplus k_6$	$k_6 = k_3 \oplus ko_1$	$k_6 = k_3 \oplus 0$	$k_6 = k_3$
$ko_2 = k_4 \oplus k_7$	$k_7 = k_4 \oplus ko_2$	$k_7 = k_4 \oplus 1$	$k_7 = \overline{k_4}$
$ko_3 = k_0 \oplus k_5$	$k_5 = k_0 \oplus ko_3$	$k_5 = k_0 \oplus 1$	$k_5 = \overline{k_0}$
$ko_4 = k_1 \oplus k_6$	$k_6 = k_1 \oplus ko_4$	$k_6 = k_1 \oplus 0$	$k_6 = k_1$
$ko_5 = k_2 \oplus k_7$	$k_7 = k_2 \oplus ko_5$	$k_7 = k_2 \oplus 1$	$k_7 = \overline{k_2}$
$ko_6 = k_3 \oplus k_5$	$k_5 = k_3 \oplus ko_6$	$k_5 = k_3 \oplus 0$	$k_5 = k_3$
$ko_7 = k_4 \oplus k_6$	$k_6 = k_4 \oplus ko_7$	$k_6 = k_4 \oplus 1$	$k_6 = \overline{k_4}$

1-jadvalda ko‘rsatilgan tengliklardan quyida keltirilgan ikkita (1) va (2) tenglamalarni hosil mumkin.

$$k_6 = k_3 = k_1 = k_5 = k_7 \qquad (1)$$

$$\overline{k_6} = k_4 = k_2 = k_0 \qquad (2)$$

Ushbu tenglamalar maxfiy kalit bitlarining ikkita to‘plami mavjudligini ko‘rsatadi. Bitta to‘plamdagi barcha elementlar bir xil qiymatga ega (barchasi nol yoki barchasi bir). Biroq, har ikkala to‘plam bir-biriga qarama-qarshi qiymatni ifodalaydi, bu k_6 birinchi to‘plamning elementi va uning to‘ldiruvchisi $\overline{k_6}$ ikkinchi to‘plamning elementi ekanligi bilan tasdiqlanadi.

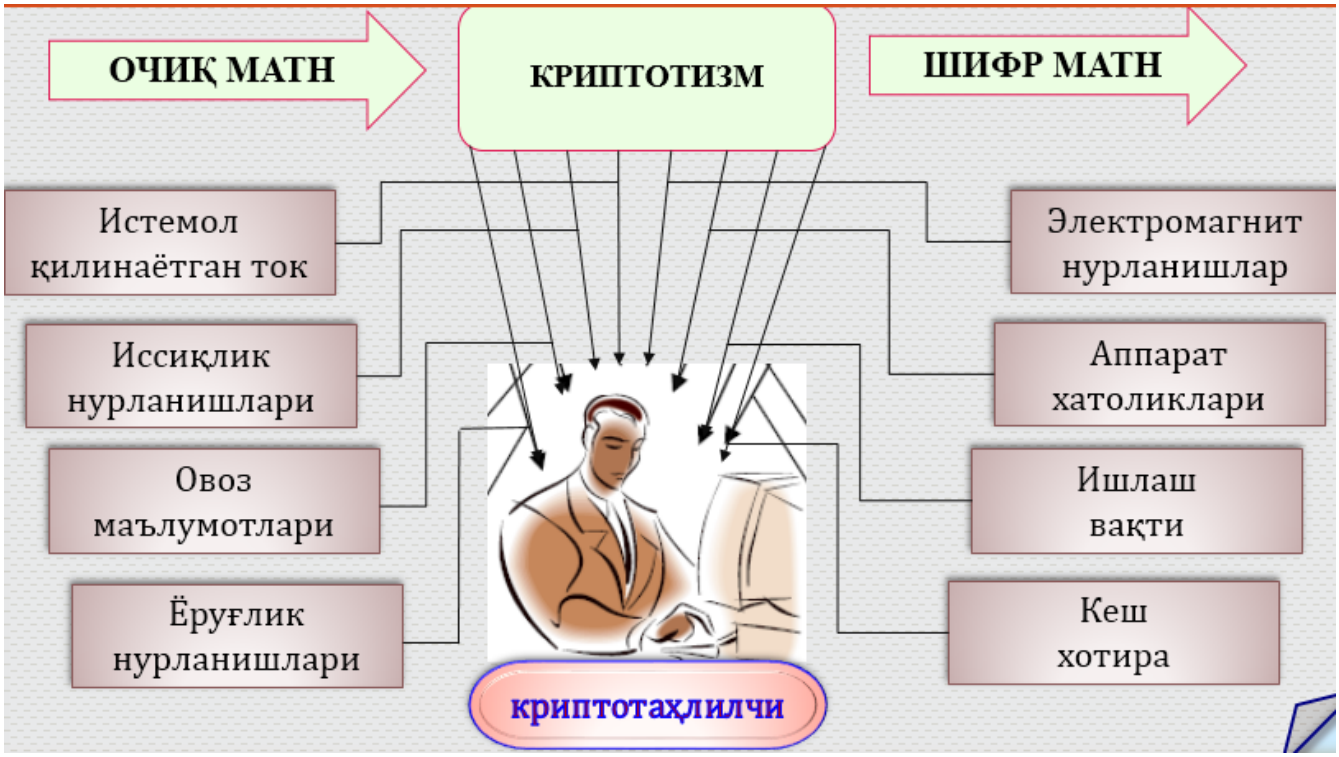
Tenglama (1) va (2) tenglamaga ko‘ra, faqat ikkita $k_0k_1 \ldots k_7 = 10101000$ to‘plam yoki uning bitlari to‘ldiruvchilaridan iborat $k_0k_1 \ldots k_7 = 01010111$ to‘plam yechim bo‘lishi mumkin,. Tenglamalarni baholash uchun hisoblash murakkabligi ahamiyatsiz. Biroq, talab qilinadigan haqiqiy murakkablik, kalit oqimi bitlarini baholash, tengliklarni shakllantirish, keraksizlarini belgilash va yakuniy tenglamalarni shakllantirishni o‘z ichiga oladi. Bunday vazifalarni hisoblashning murakkabligi nuqtai nazaridan umumlashtirish ancha qiyin bo‘lsada bunday harakatlarni samarali optimallashtirish uchun bir nechta variantlar mavjud.

2.2. Qo‘shimcha kanallardan foydalanishga asoslangan kriptotahlil usullari.

So‘nggi vaqtlarda kriptotahlilning muhim yo‘nalishlaridan biri, axborotni kriptografik himoyalash apparat-dasturiy qurilmalarini qo‘llanilishida yuzaga keladigan qo‘shimcha kanallardan va ishchi muhitning alohida xususiyatlaridan foydalanishga qaratilgan hujumga asoslanmoqda. Tashqi yoki qo‘shimcha kanal bo‘yicha hujum – bu tashqi yoki qo‘shimcha kanallardan olingan ma’lumotlardan foydalangan holda olib boriladigan kriptografik hujum turidir. Qo‘shimcha kanallar bo‘yicha olingan ma’lumotlar bu shifrlash qurilmasidan olingan bo‘lishi mumkin bo‘lib, shu bilan birga ochiq matn va yopiq matn ham emasdir.

Amaliyotda kriptotizimlarga nisbatan amalga oshirilgan barcha muvaffaqqiyatli hujumlar, asosan kriptoalgoritm mexanizmlarining amalda qo‘llanilishida yuzaga keladigan zaifliklardan foydalangan holda amalga oshirilgan. Bunday hujum, maxfiy kalitga bog‘liq ravishda hisoblash mashinasining ichki holati va hisoblash jarayonining turli vaqtidagi o‘lchanadigan fizik parametrlari (energiya sarfi, hisoblashga ketgan vaqt, elektromagnit tarqalishlar va h.k.) qiymatlari o‘rtasidagi korrelyatsiyaga asoslangan. Tajribada, qo‘shimcha kanallar bo‘yicha hujum, faqat matematik tahlilga asoslangan ananaviy hujumlarga nisbatan samaraliroq hisoblanadi. Qo‘shimcha kanallar bo‘yicha hujum, hisoblash mashinasiga kiritilgan, maxfiy parametrlarni chiqarib olish uchun kriptografik himoyalash apparat-dasturiy qurilmalari qo‘llanilishining o‘ziga xos xususiyatlaridan foydalanadi (implementation attacks).

Bunday yondashuv, kriptografik algoritmlarning apparat-dasturiy qurilmalaridan foydalanish bilan bevosita bog‘liq bo‘lganligi uchun kamroq umumlashgan bo‘lsada, mavjud klassik kriptotahlil usullariga nisbatan qisman samaraliroqdir.



1.2.1 – rasm. Qo‘shimcha kanallar bo‘yicha kriptotahlil.

Qo‘shimcha kanallar bo‘yicha hujum quyidagi uch tur bo‘yicha klassifikatsiyalanadi:

- hisoblash jarayoni ustidan nazorat qilish bo‘yicha: aktiv va passiv;
- kriptomodulga ruxsat olish bo‘yicha: agressiv (invasive), yarimagressiv (semi - invasive) va noagressiv (non- invasive);
- tahlil jarayonida qo‘llanilish usuli bo‘yicha: oddiy – simple side channel attack (SSCA) va har-xil – differential side channel attack (DSCA).

Hozirgi kunda o‘ndan ortiq qo‘shimcha kanallar aniqlangan. Hujumlar, foydalanilayotgan qo‘shimcha kanallarning turiga ko‘ra farqlanadi (1.2.1- rasm): jarayonga sarflanayotgan vaqt bo‘yicha hujum (Timing Attacks), energiya sarfi bo‘yicha hujum (Power Analysis Attacks), apparat xatoliklari bo‘yicha hujum (Fault Attacks), elektromagnit nurlanishlar bo‘yicha hujum (ElectroMagnetic Analysis), aloqa kanalidagi xatolik bo‘yicha hujum (Error Message Attacks).

Bundan tashqari, kesh-xotira bo‘yicha (Cache-based Attacks), akustik (Acoustic Attacks), yorug‘lik nurlanishi bo‘yicha hujum (Visible Light Attacks) kabi turlari ham mavjud.

Vaqt bo‘yicha hujum

Vaqt bo‘yicha hujum bu – foydalanuvchi kriptografik operatsiyalarni bajarish jarayonida, vaqtni aniq o‘lchash orqali maxfiy ma’lumotga ega bo‘lishdir. Bu qo‘shimcha kanal bo‘yicha hujumning kriptografiyada paydo bo‘lgan dastlabki turlaridan biri hisoblanadi. Kriptotizimlarda ma’lumotlarni qayta ishlash vaqti ko‘p hollarda kirish qiymati (masalan, ochiq va yopiq matn)ga qarab biroz o‘zgarishi mumkin. Vaqt bo‘yicha hujum, shifrlash modulining kerakli shifrlash operatsiyasining bajarish uchun ketgan vaqtni o‘lchab borishga asoslangan bo‘lib,

maxfiy kalitlar bo‘yicha ma’lumotlarning ochilishiga olib kelishi mumkin. Masalan: maxfiy kalit bilan ishlash operatsiyasini bajarish uchun ketgan vaqtni aniq o‘lchash orqali, kriptotahlilchi Diffi-Xelmman algoritmining eksponenta aniq qiymatini topishi mumkin.

Ta’kidlash joizki, vaqt bo‘yicha hujum, RSA algoritmining maxfiy kalitini, kriptografik operatsiyalarni amalga oshirishga ketgan vaqtni ma’lum bir intervalda o‘lchash orqali tiklab olish mumkinligi 1995 yilda bir qancha shov-shuvlarga sabab bo‘lgan. Bu turdagi hujumlar mikroprotsessorli kartochkalar va boshqa idintifikatsiyalash vositalari, shuningdek tarmoqdagi elektron tijorat serverlariga muvoffaqiyatli qo‘llanilgan.

Quvvat bo‘yicha tahlil

Quvvat bo‘yicha tahlil kriptografik vositalarning apparat vositalari uchun foydaliroqdir va tarkibida maxfiy kalitlarni saqlovchi smart-karta va boshqa tizimlarni ochishda muvoffaqiyatli qo‘llaniladi.

Quvvat istemolini o‘lchash uchun, tarmoq zanjiriga yoki yerga ulanishga ketma-ket ravishda kichik qarshilikli (masalan 50 Om) rezistorlarni ulash kerak bo‘ladi. Quvvatning kamayishini, qarshilikka bo‘lsak, tok kuchini beradi. Zamonaviy laboratoriyalar bugungi kunda, quvvatning o‘ta yuqori chastotalarida (1 GGts) ham yuqori aniqlikda (1 % xatolik bilan) o‘lchash qurilmalariga ega.

Ta’kidlash joizki, qo‘shimcha kanallardan foydalanishda quvvatning o‘zgarishi – tahlil uchun yaxshi vositalardan biri hosoblanashi bilan birga juda kam xarajatli hisoblanadi.

Apparat xatoliklari bo‘yicha tahlil

Kriptografik modulning ishlash jarayonida vujudga keladigan apparat ta’minotidagi xatoliklar yoki xatoli chiqish bloklari qo‘shimcha kanallar uchun muhim bo‘lishi va ba’zan shifrlarning mavjud kriptotahlil usullariga nisbatan bardoshsizligini sezilarli oshirishi mumkin.

Apparat xatoliklariga asoslangan kriptotahlil – kriptotahlilchi shifrlash qurilmasiga tashqi fizik ta’sir o‘tkaza olishi va ma’lum bir blok ma’lumotni shifrlash jarayonida bir xildagi xatoliklarni generatsiya qilish imkoniyatiga egaligiga asoslanadi. Kriptografik algoritmlarga xatoliklar bo‘yicha hujum 1996 yildan boshlab o‘rganib kelinayotgan bo‘lib, shu paytga qadar deyarli barcha shifrlash algoritmlariga mazkur turdagi hujum qullanilgan.

Apparat xatoliklarining samaradorligi kriptotahlilchining tizimda maxsus xatolikni amalga oshira olish yoki tabiiy xatoliklardan foydalana olish imkoniyatiga bog‘liq bo‘ladi.

Bu turdagi hujumga bardoshlilik masalasi ayniqsa intelektual elektron kartochkalarida qo‘llaniladigan shifratorlar uchun muhimdir.

Xatoliklar quyidagi jihatlari bo‘yicha klassifikatsiyalanadi:

- kriptotahlilchi kriptografik modulning ishlash jarayonida vujudga keladigan xatolikning vaqtini va joyini tanlashdagi aniqlik;
- ta’sir etayotgan xatolikning uzunligi: masalan faqat, bir bit;
- xatolikning davomiyligi: xatolik qisqami yoki davomiy;
- xatolik turi: bir bitning o‘zgarishi; bitning, faqat bir tomonlama (masalan 1 dan 0 ga); bitni ixtiyoriy qiymatga o‘zgarishi va h.k..

Umuman olganda, kriptografik modulga yoki qurilmaga nisbatan xatolikni samarali amalga oshirish ikki qadamdan iborat: xatolikni hosil qilish va bu xatolikdan foydalanish.

Mazkur hujum usuli asosan nazariy jixatdan o‘rganilgan bo‘lib barcha shifrlash tizimlariga nisbatan qo‘llanilgan.

Jumladan, GOST 28147-89, DES va RC6 shifrlash algoritmlariga nisbatan apparat xatoliklarning generatsiyasiyaga asoslangan hujum amalga oshirilgan.

Elektromagnit nurlanishlar bo‘yicha hujum

Kompyuterda hisoblash operatsiyalarini amalga oshirish jarayoni elektromagnit nurlanishlar bilan bevosita bog‘liq. Mazkur nurlanishlarni o‘lchash va tahlil qilish orqali, kriptotahlilchi hisoblash jarayonlari va foydalanilayotgan ma’lumotlar to‘g‘risida yetarlicha axborot olishi mumkin. Elektromagnit nurlanishlar bo‘yicha tahlil ham ikki turga bo‘linishi mumkin: ya’ni oddiy – simple (SEMA) va har-xil – differential (DEMA).

Apparat xatoliklarni generatsiyalashga asoslangan kriptotahlil usuli.

Apparat xatoliklarni generatsiyalashga asoslangan kriptotahlil usulining mohiyati, algoritm o‘zgartirishlarining ma’lum joylaridagi ayrim bitlarini o‘zgartirishga erishish maqsadida, himoya apparatiga issiqlik, yuqorichastotali, ionizatsiyalash va boshqa tashqi ta’sir usullaridan foydalangan holda ta’sir etishdir. Bunday o‘zgartirish kiritish tahlil usuli ma’lumotni o‘zgartirish kiritilgunga qadar va o‘zgartirilganidan so‘ng ega bo‘lgan ma’lumotlarni solishtirish orqali oxirgi raund kaliti va keyinchalik barcha raund kalitlari to‘g‘risida qiymatlar olishga qaratilgan.

So‘nggi vaqtlarda DES va GOST 28147-89 blokli shifrlash algoritmlariga nisbatan o‘tkazilgan tadqiqotlar, ularning bu turdagi xujumlarga bardoshsiz ekanligini ko‘rsatdi.

Apparat xatoliklarni generatsiyalash tahlil usulining bazaviy elimentlarini ko‘radigan bo‘lsak shifrlarning bu turdagi hujumga nisbatan bardoshliligi, ularning oxirgi raund kalitlari K_R ni to‘liq ko‘rib chiqish (total perebor) murakkabligiga teng kuchli ekanligini ko‘rish mumkin.

Hakikatdan ham, Feystel tarmog‘iga asoslangan blokli shifrlash algoritmlarining oxirgi raund kalitlari quyidagicha aniqlanadi:

1. $X_R=X_R \oplus F(X_L,K_R)$ – xatosiz ko‘rinishi.

2. $X'_R=X_R \oplus F(X'_L,K_R)$ – generatsiya qilingan xatolik bilan ko‘rinishi.

bu yerda ,

X_R – ma’lumotning xatosiz o‘ng bloki

X_L – ma’lumotning xatosiz chap bloki

X'_R – ma’lumotning xatoli o‘ng bloki

X'_L – ma’lumotning xatoli chap bloki

K_R – raund kaliti

$\oplus$ - XOR (modul 2 bo‘yicha qo‘shishi amali)

Ikki tenglamani qo‘shib quyidagi tenglamaga ega bo‘lamiz:
$X_R \oplus X'_R = F(X_L,K_R) \oplus F(X'_L,K_R)$.

Ta’kidlash joizki, bunday tenglamalar sistemasini bir nechta turli xil ochiq va yopiq matnlarga nisbatan qurish mumkin. *F* funksiyaning ko‘rinishiga bog‘liq bo‘lmagan holda bunday tenglamalar sistemasining yagona yechimini topish raund kalitlari K_R ni topishni to‘liq ko‘rib chiqish usuliga teng kuchli.

Raund kalitlari K_R ni to‘liq ko‘rib chiqish usuli bilan topishning eng yuqori qiymati quyidagi ko‘rinishga ega:

$M_{K(r)} = 2^m h M_F$, bu yerda h – sistemadagi tenglamalar soni,

M_F – raund almashtirishlarining hisoblash murakkabligining qiymati, m – kalit uzunligi.

Xuddi shu tartibda keyingi raund kalitlarini topish qiymatining kattaligini ham hisoblash mumkin.

Barcha r raundli kalitlar jadvalini topishning eng yuqori qiymati quyidagiga teng $M=2^m h M_F r$.

Shunday qilib, Feystel sxemasiga asoslangan ixtiyoriy blokli shifrni ochish qiyinchiligi, bitta raund kaliti (2^m) ni topish qiyinchiligiga proporsionaldir.

2.3. Kriptotahlilda yangi texnologiyalardan foydalanish.

Kriptotahlil (kriptografik tahlil) sohasida yangi texnologiyalar va vositalar tez rivojlanmoqda. Quyida kriptotahlilda qo'llanilayotgan so'nggi texnologiyalar va usullar haqida qisqacha ma'lumot beraman:

Kvant hisoblash va kvant tahlil

- **Kvant kompyuterlari**: Kvant hisoblash kriptografik algoritmlar, xususan, **RSA**, **ECC** va **DSA** kabi ochiq kalitli algoritmlarni buzishda katta salohiyatga ega. Masalan, **Shor algoritmi** katta sonlarni samarali faktorizatsiya qilishi mumkin.
- **Post-kvant kriptografiya**: Hozirda kvant hujumlariga chidamli algoritmlar ishlab chiqilmoqda. Masalan:
  - **Lattice-based cryptography**
  - **Code-based cryptography**
  - **Hash-based cryptography**

Mashinasozlik va sun'iy intellekt (AI)

- **Kriptotahlilni avtomatlashtirish**: Sun'iy intellekt algoritmlari, masalan, **neyron tarmoqlar** va **qayta o'rganish modellaridan** foydalanish, shifrlash xatolarini topish va zaifliklarni tahlil qilishda qo'llanilmoqda.
- **Xatarlarni bashorat qilish**: AI yordamida shifrlash tizimlarining zaifliklari va ularning ehtimoliy buzilishlarini oldindan aniqlash.

Differensial va lineer kriptotahlilni rivojlantirish

- **Yangi kriptotahlil metodlari**: Differensial kriptotahlil va lineer kriptotahlil shifrlash algoritmlaridagi statistik zaifliklarni topishda qo'llanilmoqda. Ushbu usullarning yanada samarali variantlari, masalan:
  - **Integral cryptanalysis**
  - **Boomerang attacks** rivojlanmoqda.

Yon kanal hujumlari (Side-Channel Attacks)

- **Zamonaviy yon kanal tahlillari**: Elektron qurilmalardan chiqadigan yon ma'lumotlardan (quvvat iste'moli, elektromagnit nurlanish va vaqt tahlili) foydalanib, shifrlash kalitlarini topish texnologiyalari rivojlandi.
- **Himoya usullari**:
  - Quvvat tahliliga qarshi chidamli usullar (Power analysis resistance)
  - Tasodifiylashtirish texnikalari

Bulutli xizmatlar va distributsiyali hisoblash

- **Distributsiyali hisoblash**: Katta hisoblash quvvatidan foydalanish uchun bir nechta kompyuterlarni birlashtirish orqali shifrlash algoritmlarini tahlil qilishda qo'llaniladi.
- **Bulutda kriptotahlil**: Bulutli platformalar katta miqdordagi ma'lumotlarni tezkor tahlil qilish imkoniyatini beradi. Bu **hash** va **brute-force** hujumlarini amalga oshirishda yordam beradi.

Homomorfik shifrlash va teskari tahlil

- **Homomorfik shifrlash**: Ma'lumotlarni ochmasdan hisoblash imkonini beruvchi usul. Bu texnologiya kriptotahlilni murakkablashtiradi, lekin zaifliklar izlashda tahlilchilarga qiziqish uyg'otmoqda.

Nazariy savollari:

1. T Kvant kompyuterlari RSA, ECC va DSA kabi algoritmlarga qanday ta’sir qilishi mumkin?
2. Shor algoritmi qanday masalalarni samarali yechishi mumkin?
3. Post-kvant kriptografiya nima va uning asosiy maqsadi nima?
4. Post-kvant kriptografiyada ishlatiladigan asosiy usullarni sanab bering.

5. Lattice-based, Code-based va Hash-based kriptografiyalar orasidagi asosiy farq nima?
6. Sun’iy intellekt kriptotahlil sohasida qanday ishlatilmoqda?
7. Kriptotahlilni avtomatlashtirishda neyron tarmoqlar qanday rol o‘ynaydi?
8. AI yordamida xatarlarni qanday bashorat qilish mumkin?
9. Differensial va lineer kriptotahlilning asosiy maqsadi nima?
10. Integral cryptanalysis va Boomerang attacks qanday usullarga asoslanadi?
11. Yangi kriptotahlil metodlarining klassik usullardan farqi nimada?
12. Yon kanal hujumlarining qanday turlari mavjud?
13. Elektron qurilmalarning qaysi xususiyatlari yon kanal tahlillari uchun ma’lumot beradi?
14. Quvvat tahliliga qarshi chidamlilik texnologiyalari qanday ishlaydi?
15. Tasodifiylashtirish texnikalari yon kanal hujumlariga qanday qarshilik ko‘rsatadi?
16. Distributsiyali hisoblash kriptotahlil uchun qanday foyda keltiradi?
17. Bulutli platformalar hash va brute-force hujumlarini qanday osonlashtiradi?
18. Bulutli hisoblash va an’anaviy hisoblash o‘rtasidagi asosiy farqlar nimalardan iborat?
19. Homomorfik shifrlashning asosiy afzalliklari nimada?
20. Ushbu texnologiya kriptotahlilni qanday murakkablashtiradi?
21. Homomorfik shifrlashdagi zaifliklarni qanday aniqlash mumkin?

Adabiyotlar va internet resurslar:

1. Xasanov P.F., Xasanov X.P., Axmedova O.P., Davlatov A.B. Kriptotahlil va uning maxsus usullari, O‘quv qo‘llanma, Toshkent, 2010

2. Akbarov D.YE. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanishlari. Toshkent. ”O‘zbekiston markasi“, 2009

3. Л.К.Бабенко, Е.А.Ищукова. Современные алгоритмы блочного шифрования и методы из анализа: учеб. пособие для студентов вузов, обучающихся по группе специальностей в обл. информ. безопасности – М.: Гелиос АРВ, 2006. – 376 с.

4. M.Stamp. Applied cryptanalysis: Breaking Ciphers in the Real World. John Wiley & Sons, Inc, 2007, -P. -417.

5. Б.Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – Москва: ТРИУМФ, 2002.

6. Xasanov P., Xasanov X., Axmedova O., Davlatov A. Kriptotahlil va uning maxsus usullari. O‘quv qo‘llanma.– Toshkent, 2010.

7. O.P.Axmedova, Z.T.Xudoykulov, O. Allanov, I.M.Boyquziyev Kriptoanaliz. O‘quv qo‘llanma. T.: “Iqtisod-Moliya”, 2022. 171 b.

8. Kuryazov D.M., Sattorov A.B., Axmedova B.B. Blokli simmetrik shifrlash algoritmlari bardoshligini zamonaviy kriptotahlil usullari bilan baholash. O‘quv qo‘llanma. T.: “Aloqachi”. 2017, 228 bet.

9. http://jnicholl.org/Cryptanalysis/Tools/
10. https://www.cryptool.org/en/cto/
11. https://resources.infosecinstitute.com/topic/cryptanalysis-tools/
12. http://rumkin.com/tools/cipher/
13. https://blackarch.org/crypto.html
14. https://www.guballa.de/vigenere-solver
15. https://www.simonsingh.net/The_Black_Chamber/substitutioncrackingtool.html
16. https://www.guru99.com/how-to-make-your-data-safe-using-cryptography.html
17. https://www.cs.bu.edu/~goldbe/teaching/CS558S17/Lab1.pdf

IV-BO‘LIM

AMALIY MASHG‘ULOT MATERIALLARI

IV. AMALIY MASHG‘ULOT MATERIALLARI

1-amaliy ish. Kriptologiyaning ilmiy yo‘nalishlari, kriptografiya va kriptotahlil. Klassik shifrlarning kriptotahlili, kriptotahlilning sodda usullari. Kriptografik algoritmlar bardoshliligi va hisoblash murakkabligi nazariyasi, kriptografik bardoshlilik tushunchasi (2 soat)

Amaliy ishning maqsadi – *Klassik shifrlarning kriptotahlili, kriptotahlilning sodda usullari. Kriptografik algoritmlar bardoshliligi va hisoblash murakkabligi nazariyasi, kriptografik bardoshlilik bo‘yicha ko‘nikmaga ega bo‘lish.*

Nazariy qism

O‘rin almashtirishga asoslangan shifrlash algoritmlari ochiq matnning alohida olingan shifr qiymatlari o‘rinlarini o‘zgartirish natijasida yoki shifr qiymatlarni guruhlab(bloklab) aralashtirish bilan amalga oshiriladi. Shifr belgilarini bloklab aralashtirish kriptografik nuqtai nazardan samarali natijalar beradi. Bloklab shifrlashda ochiq matn N ta simvoldan iborat bloklarga bo‘linib, har bir blokdagi simvollar ma’lum bir qoida(kalit) asosida almashtirilib chiqiladi. O‘rin almashtirish shifrida kalit ikki xil usul bilan qo‘llaniladi.

Kalit $K = k_1 k_2 k_3 \dots k_N$, ochiq matn $M = m_1 m_2 m_3 \dots m_N$ bo‘lsin.

1-usul: ochiq matnni shifrlash uchun uning $i-$simvolini k_i –o‘ringa qo‘yish kerak. Misol: $N = 7$, kalit 5312764 bo‘lsin.

Ochiq matn:“KRIPTOGRAFIYA” 7 tadan qilib bloklarga ajratiladi.

1-blok: KRIPTOG, 2-blok: RAFIYA Kriptogrammalar “IPRGKOT va FIARYA” hosil bo‘ladi.

2-usul: shifrlashda $i-$o‘riniga ochiq matnning k_i-simvoli qo‘yiladi.

$N = 7$; kalit 5312764 bo‘lsin.

Ochiq matn:“KRIPTOGRAFIYA ” 7 tadan qilib bloklarga ajratiladi.

1-blok: KRIPTOG, 2-blok: RAFIYA Kriptogramma “TIKRGOP” va “YAFRAI” hosil bo‘ladi.

Ixtiyoriy o‘rin almashtirishni $G =< V, E >$ graf ko‘rinishida tasvirlash mumkin, bu yerda V - grafning uchlari, E esa grafning tomonlari. O‘rin almashtirish shifrida Gamilton marshrutidan foydalanish juda qulay.

Ta’rif. Agar berilgan graf undagi barcha uchlardan faqat bir martadan o‘tadigan oddiy siklda bo‘lsa, u holda Gamilton sikli deyiladi.

Teorema. (Yetarlilik sharti) $G =< V, E >$ graf berilgan bo‘lsin.

Agar berilgan grafda ixtiyoriy $u \in V$ uchun $\deg(u) \geq \frac{p}{2}$ (bu yerda p – uchlar soni) bo‘lsa, u holda graf Gamilton sikliga ega bo‘ladi.

Umumiy holda K uzunlikdagi bloklar uchun o‘rin almashtirishlar soni $K!$ bo‘ladi. Agar K kichik son bo‘lsa, bu kriptogrammani kalitni to‘liq terib chiqish usuli bilan deshifrlash mumkin, ammo kalitning uzunligi yetarlicha katta bo‘lgan o‘rin almashtirish shifrlari uchun bu katta muammo keltirib chiqaradi. Gamilton marshrutidan foydalanish o‘rin almashtirish kriptogrammalari deshifrlashini yengillashtiradi, chunki barcha kalitlar ichidan Gamilton yo‘li xossasiga ega bo‘lgan kalitlar ishlatiladi. Lekin katta bloklar uchun bu imkoniyat ham sezilarli bo‘lmaydi. Matnda harflarning juft-jufti (diagramma) bilan kelish chastotasini bilish jadvalli o‘rin almashtirish kriptogrammalarini deshifrlash imkoniyatini beradi. Jadvalli o‘rin almashtirish shifri bo‘yicha matnni nxm o‘lchovli jadvalga ustun bo‘yicha joylashtirib, ma’lum bir kalit asosida o‘rni almashtirilib, E kriptogramma hosil qilinadi:

3.1-jadval

Jadvalli o‘rin almashtirish

$e_{1,1}$	$e_{1,2}$	…	$e_{1,t}$	…	$e_{1,f}$	…	$e_{1,m}$
…	…	…	…	…	…	…	…
$e_{i,1}$	$e_{i,2}$	…	$e_{i,t}$	…	$e_{i,f}$	…	$e_{i,m}$
…	…	…	…	…	…	…	…
$e_{j,1}$	$e_{j,2}$	…	$e_{j,t}$	…	$e_{j,f}$	…	$e_{j,m}$
…	…	…	…	…	…	…	…
$e_{n,1}$	$e_{n,2}$	…	$e_{n,t}$	…	$e_{n,f}$	…	$e_{n,m}$

$p(a, c)$ deb ochiq matnda a harfdan keyin c harf kelish ehtimolligi belgilanadi. U holda $i-$ satrdan keyin $j-$ satrning ketma-ket kelish ehtimolligi quyidagicha bo‘ladi:

$$p(i, j) = \prod_{k=1}^{m} p(e_{i,k}, e_{j,k})$$

Bu formula orqali ketma-ket keluvchi barcha satrlar juftligini aniqlash mumkin. Agar ochiq matnda $i-$ satrdan keyin $j-$ satr kelsa, u holda $p(i, j) \geq p(i, k)$ bo‘ladi. Lekin har xil mavzudagi matnlar uchun diagrammalarning uchrash ehtimolligi har xil bo‘ladi. Shuning uchun birorta kriptogrammani deshifrlash uchun avvalambor uning qaysi sohaga tegishli ekanligini bilish katta ahamiyatga ega. Umumiy holda kriptogrammani deshifrlash uchun jadvalning tartibini aniqlab olib,

ehtimolligi katta bo‘lgan satrlarni topishning optimal masalasini yechish kerak.

3.2. O‘rniga qo‘yish shifrlarining kriptoanalizi

Chastotaviy, ya’ni statistik xarakteristikalar usulida simmetrik yoki asimmetrik kriptotizim kriptoanalizchisi shifrmatndagi belgilar, harflar, so‘zlarning takrorlanishlari soni(chastotalari)ni hisoblab, ochiq matn qaysi tilda yozilganini aniqlaydi. So‘ngra esa, shifrmatn shifr belgilari parametrlarini ochiq matn qaysi tilda yozilgan bo‘lsa, shu tilning parametrlari bilan solishtiradi. Chastotaviy tahlil usulida ta’kidlanganidek, ingliz tilida *th, in, is, er, he, en,* bigrammalari ko‘p uchraydi. Quyidagi jadvalda ingliz tili harflarining paydo bo‘lishining nisbiy chastotasi keltirilgan (40 000 ta so‘z ichida).

Yuqorida aytib o‘tilgan prinsiplar hozirgi kunda keng tarqalgan parollarni tanlash bo‘yicha dasturlarda qo‘llaniladi. Parollarni tanlash bo‘yicha dastur avvalo ehtimolligi katta bo‘lgan parollarni tanlaydi, ehtimolligi kichik bo‘lgan parollarni keyinga olib qo‘yadi.

3.1-jadval

Ingliz tili alifbosining chastotalar jadvali

Harf	**Soni**		**Harf**	**Chastotasi**
E	21912		E	12.02
T	16587		T	9.10
A	14810		A	8.12
O	14003		O	7.68
I	13318		I	7.31
N	12666		N	6.95
S	11450		S	6.28
R	10977		R	6.02
H	10795		H	5.92
D	7874		D	4.32
L	7253		L	3.98
U	5246		U	2.88
C	4943		C	2.71
M	4761		M	2.61
F	4200		F	2.30
Y	3853		Y	2.11
W	3819		W	2.09
G	3693		G	2.03
P	3316		P	1.82

Harf	**Soni**		**Harf**	**Chastotasi**
B	2715		B	1.49
V	2019		V	1.11
K	1257		K	0.69
X	315		X	0.17
Q	205		Q	0.11
J	188		J	0.10
Z	128		Z	0.07

1. Shifrmatn quyidagiga teng bo‘lsin:
   GBSXUCGSZQGKGSQPKQKGLSKASPCGBGBKGUKGCEU
   KUZKGGBSQEICACGKGCEUERWKLKUPKQQGCIICUAEU
   VSHQKGCEUPCGBCGQOEVSHUNSUGKUZCGQSNLSHEHI
   EEDCUOGEPKHZGBSNKCUGSUKUASERLSKASCUGBSLK
   ACRCACUZSSZEUSBEXHKRGSHWKLKUSQSKCHQTXKZH
   EUQBKZAENNSUASZFENFCUOCUEKBXGBSWKLKUSQSK
   NFKQQKZEHGEGBSXUCGSZQGKGSQKUZBCQAEIISKOXS
   ZSICVSHSZGEGBSQSAHSGKHMERQGKGSKREHNKIHSLI
   MGEKHSASUGKNSHCAKUNSQQKOSPBCISGBCQHSLIMQ
   GKGSZGBKGCGQSSNSZXQSISQQGEAEUGCUXSGBSSJCQ
   GCUOZCLIENKGCAUSOEGCKGCEUQCGAEUGKCUSZUEG
   BHSKGEHBCUGERPKHEHKHNSZKGGKAD.

   Berilgan shifrmatndagi belgilarning takrorlanish darajasi esa quyidagiga teng:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
17	20	38	2	35	3	57	23	13	1	52	10	3	13	7	7	30	7	61	1	38	3	3	8	0	19

Mos harflarning ehtimolliklari katta bo‘lganlari almashtirilgandan so‘ng, keng uchraydigan ikkiliklar (*TH, EA, OF, TO, IN, IT, IS, BE, AS, AT, SO, WE, HE, BY, OR, ON, DO, IF, ME, MY, UP*), uchliklar (*THE, EST, FOR, AND, HIS, ENT yoki THA*) va ma’nosidan kelib chiqqan holda so‘zlar almashtirilgandan so‘ng quyidagi ochiq matn olinadi:

THE UNITED STATES WAS AT PEACE WITH THAT NATION AND AT THE SOLICITATION OF JAPAN WAS STILL IN CONVERSATION WITH ITS GOVERNMENT AND ITS EMPEROR LOOKING TOWARD THE MAINTENANCE OF PEACE IN THE

PACIFIC IN DEED ONE HOUR AFTER JAPANESE AIR SQUADRONS HAD COMMENCED XOMXING IN OAHU THE JAPANEE AMBASSADOR TO THE UNITED STATES AND HIS COLLEAGUE DELIVERED TO THE SECRETARY OF STATE A FORMAL REPLY TO A RECENT AMERICAN MESSAGE WHILE THIS REPLY STATED THAT IT SEEMED USELESS TO CONTINUE THE EXISTING DIPLOMATIC NEGOTIATIONS IT CONTAINED NO THREAT OR HINT OF WAR OR ARMED ATTACK.

3.3. Bir martalik bloknot shifrining kriptoanalizi

Bir martalik bloknot (One time pad) yoki Vernam shifri nomi bilan tanilgan kriptotizim bardoshli shifrlash algoritmi hisoblanib, tarixda turli vaqtlarda va joylarda foydalanilgan bo‘lsada, ko‘p hollarda amalga oshirishning imkoniyati mavjud emas. Bir martalik deb atalishiga asosiy sabab, undagi kalitning (bloknotning) bir marta foydalanilishi bo‘lib, shunning uchun uni aksariyat hollarda amalga oshirishning imkoni mavjud bo‘lmaydi.

Ushbu shifrlash algoritmini tushuntirish uchun 8 ta belgidan iborat bo‘lgan alfavit olingan bo‘lsin. Olingan alfavit va unga mos bo‘lgan binar qiymatlar quyidagi jadvalda keltirilgan. Shuni esda saqlash kerakki, alifbo va unga mos bo‘lgan bit qiymatlari barcha uchun ochiq va sir saqlanmaydi (ASCII jadvali kabi).

Belgilar	**P**	**I**	**N**	**1**	**3**	**4**	**8**	**9**
	000	001	010	011	100	101	110	111

Faraz qilinsin, biror qonuniy foydalanuvchi A bir martali bloknotdan foydalangan holda “PIN8893144” matnini shifrlab, o‘z sherigi B tomonga yuborishi talab etilsin. Ushbu ochiq matnni binar qiymatdagi ko‘rinishi esa quyidagicha bo‘ladi:

P	**I**	**N**	**8**	**8**	**9**	**3**	**1**	**4**	**4**
000	001	010	110	110	111	100	011	101	101

Bir martalik bloknot usulida shifrlash uchun ochiq matn uzunligiga teng bo‘lgan tasodifiy tanlangan kalit zarur bo‘ladi. Ochiq matnga kalitni XOR amalida qo‘shish orqali shifrmatn hosil qilinadi (*R – ochiq matn*, *K – kalit* va *S – shifrmatn* deb belgilansa): $C = P \oplus K$. XOR amali ($\oplus$) binar amal hisoblanib, quyida keltirilgan:

$$0 \oplus 0 = 0$$

$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

Yuqoridagi jadvaldan, $x \oplus y \oplus y = x$ tenglik o‘rinliligini bilish qiyin emas va shuning uchun bir martali parolda deshifrlash uchun shifrmatnga kalitni XOR amalida qo‘shishning o‘zi yetarli hisoblanadi: $P = C \oplus K$.

Faraz qilinsin A tomon yuqorida keltirilgan ochiq matn uzunligiga teng bo‘lgan quyidagi kalitga ega bo‘lsin:

$$K = \{000\ 000\ 000\ 101\ 111\ 100\ 000\ 101\ 110\ 000\}$$

Ochiq matn	**P**	**I**	**N**	**8**	**8**	**9**	**3**	**1**	**4**	**4**
	000	011	010	110	110	111	100	001	101	101
Kalit	000	000	000	*101*	*111*	*100*	*000*	*101*	*110*	*000*
Shifr matn	000	011	010	*011*	*001*	*011*	*100*	*100*	*011*	*101*
	P	**I**	**N**	**1**	**I**	**1**	**3**	**3**	**1**	**4**

Ushbu kalit asosida *A* tomon yuqorida shifrmatnni hisoblaydi.

A tomonidan yuborilgan shifrmatn *B* tomonda bir xil kalit mavjudligi sababli osongina quyidagicha deshifrlanadi.

Shifr matn	**P**	**I**	**N**	**1**	**I**	**1**	**3**	**3**	**1**	**4**
	000	011	010	*011*	*001*	*011*	*100*	*100*	*011*	*101*
Kalit	000	000	000	*101*	*111*	*100*	*000*	*101*	*110*	*000*
Ochiq matn	000	011	010	110	110	111	100	001	101	101
	P	**I**	**N**	**8**	**8**	**9**	**3**	**1**	**4**	**4**

Ushbu shifrlash algoritmi uchun quyidagi ikki holatni qarab chiqish muhim. Birinchi holatda, faraz qilinsin *A* tomoning dushmani *M* bor va u *A* tomon shifrlagan xabarni o‘qiy olmaydi, lekin o‘zgartira oladi. Ushbu imkoniyatdan foydalanib uzatilayotgan maxfiy xabarning mazmunini o‘zgartirishi mumkin. Buning uchun *M* tomon uzatilayotgan shifrmatnga o‘zining maxfiy kalitini XOR amali bo‘yicha qo‘shadi va qabul qiluvchi *B* ga uzatadi. Ushbu jarayonni quyidagicha ifodalash mumkin:

Shifr matn	**P**	**I**	**N**	**1**	**I**	**1**	**3**	**3**	**1**	**4**
	000	011	010	*011*	*001*	*011*	*100*	*100*	*011*	*101*
***M* tomonning kaliti**	*111*	*000*	*101*	*111*	*100*	*000*	*101*	*100*	*110*	*000*
M	111	011	111	100	101	011	001	000	101	101

tomonidan shifrlangan matn	**9**	**1**	**9**	**3**	**4**	**1**	**I**	**P**	**4**	**4**

Agar *M* dushman ushbu shifrmatnni *B* tomonga qayta uzatsa, u holda *B* tomon shifrmatnni deshifrlash orqali quyidagiga ega bo‘ladi:

M **tomonidan shifrlab yuborilgan matn**	**P**	**I**	**N**	**1**	**I**	**1**	**3**	**3**	**1**	**4**
	000	011	010	*011*	*001*	*011*	*100*	*100*	*011*	*101*
B **tomonning kaliti**	*111*	*000*	*101*	*111*	*100*	*000*	*101*	*100*	*110*	*000*
O‘zgargan ochiq matn	111	011	111	100	101	011	001	000	101	101
	9	**1**	**9**	**3**	**4**	**1**	**I**	**P**	**4**	**4**

B tomon *M* tomonidan yuborilgan o‘zgartirilgan shifrmatnni deshifrlaydi va “PIN8893144”ga teng bo‘lgan haqiqiy xabar o‘rniga “919341IP44”ga teng bo‘lgan soxta xabarga ega bo‘ladi.

Kafolatga ega emasligi sababli, ushbu keltirilgan misollar bir martali bloknot shifrini *bardoshli* ekanini ko‘rsatadi. Bir martali bloknotda agar kalit tasodifiy tanlansa va bir marta foydalanilgan taqdirda hujumchi shifrmatndan ochiq matn haqida biror axborotga ega bo‘la olmaydi (albatta ma’lumotni uzunligidan tashqari). Ya’ni, berilgan shifrmatn uchun mos “kalit” yordamida shifrmatn uzunligidagi ixtiyoriy “ochiq matnlar”ni generatsiya qilish mumkin va bunda barcha ochiq matnlar bir xil o‘xshashlikka ega. Shuning uchun shifrmatndan ochiq matn haqida biror foydali axborotni olishning imkoni yo‘q. Kriptografik nutqai nazardan shifrmatnlar o‘zidan ortiq ma’lumotni bera olmaydi.

Buning uchun albatta, bir martali bloknot to‘g‘ri foydalanilgan, undagi kalit tasodifiy tanlangan, bir marta foydalaniladi va faqat *A* va *B* tomonlarga ma’lum bo‘lishi talab etiladi.

Bir martali bloknot bardoshlilikni ta’minlar ekan, nima uchun har doim undan foydalanilmaydi? Buning asosiy sababi, har bir ochiq matn uchun uning uzunligiga teng bo‘lgan tasodifiy kalitni (bloknotni) generatsiya qilish va qabul qiluvchiga xavfsiz uzatish muammo tug‘diradi. Agar ochiq matn uzunligidagi kalitni (bloknotni) xavfsiz uzatishning imkoniyati mavjud bo‘lsa, u holda kalitning o‘rniga ochiq

matnni uzatish foydali emasmi? Uni shifrlashdan nima ma’no? Bir martali bloknot usulidan tarixda cheklangan uzunlikdagi ma’lumotlarni shifrlash qisman foydalanilgan bo‘lsada, hozirgi kundagi katta hajmli ma’lumotlarni uzatish uchun bir martali bloknotni to‘liq amaliy tomondan qo‘llab bo‘lmaydi.

Bir martali bloknotda kalitlardan faqat bir marta foydalanish zarur hisoblanadi. Buni tushuntirish uchun faraz qilinsin, quyidagi ikki ochiq matn P_1va P_2 bitta kalit K dan foydalanib shifrlangan $C_1 = P_1 \oplus K$ va $C_1 = P_2 \oplus K$ shifrmatnlar mavjud. Kriptografiyada ushbu holatni “xavflilik” deb ataladi va bir martali bloknot xavfli holatda deb tushiniladi, ya’ni foydalanilgan kalit ortiq muammo tug‘dirmaydi:

$$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$$

Mazkur holda shifrmatn haqiqiy ochiq matn haqida ba’zi axborotni oshkor qiladi. Agar bir xil kalitdan foydalanib ko‘p marta shifrlash amalga oshirilsa bu katta xavfga olib kelishi mumkin. Mazkur holatni quyidagi misolda ko‘rib chiqish mumkin. Faraz qilinsin, quyidagi ikkita ochiq matn berilgan (belgilarning binar kodi yuqoridagi jadvaldagi kabi):

$P = LIKE = 100010011000$ va $P = KITE = 011010111000$.

Har ikkala ochiq matn yagona kalit K= 110 011 101 111 bilan shifrlangan va shifrmatnlar quyidagiga teng bo‘lgan:

$\boldsymbol{P_1}$	**L**	**I**	**K**	**E**
	100	010	011	000
$\boldsymbol{K}$	110	011	101	111
$\boldsymbol{C_1}$	010	001	110	111

va

$\boldsymbol{P_2}$	**K**	**I**	**T**	**E**
	011	010	111	000
$\boldsymbol{K}$	110	011	101	111
$\boldsymbol{C_2}$	101	001	010	111

Agar hujumchi kriptoanaliz bilan yaqindan tanish bo‘lsa, ochiq matnlardagi 2 va 4-harflarning bir xilligidan ikkala xabar ham bir xil kalit yordamida shifrlanganligini aniqlay oladi. Sababi, mos o‘rindagi shifrmatn belgilari bir xil. Bundan tashqari, hujumchi taxminiy P_1 ochiq matn oladi va uni to‘g‘riligini P_2 ochiq matn bilan tekshirib ko‘radi. Faraz qilaylik, hujumchi birinchi ochiq matn sifatida $P1 = KILL =$ 011 010 100 100 ni olgan bo‘lsin. Bu holda u unga mos bo‘lgan taxminiy kalitni quyidagicha hisoblaydi:

$\boldsymbol{P_1}$	011	010	100	100
$\boldsymbol{C_1}$	010	001	110	111
Taxminiy kalit $\boldsymbol{K}$	001	011	010	011

Olingan kalit K yordamida esa ikkinchi shifrmatndan ochiq matnni hisoblaydi.

$\boldsymbol{C_2}$	101	001	010	111
Taxminiy kalit $\boldsymbol{K}$	001	011	010	111
Taxminiy ochiq matn $\boldsymbol{P_2}$	100	010	000	100
	L	I	E	L

Hisoblangan kalit K ikkinchi ochiq matn P_2uchun mos bo‘lmagani sababli, hujumchi taxmin qilgan birinchi ochiq matni P_1 ni noto‘g‘riligini biladi. Shu tarzda hujumchi qachonki birinchi ochiq matnni P_1=$LIKE$ tarzida taxmin qilsa, ikkinchi ochiq matnni to‘g‘ri P_2=$KITE$ topa oladi.

Amaliy bajarish uchun vazifalar.

1. O‘rin almashtirish shifrining kriptotahlilini amalga oshirish.
2. O‘rniga qo‘yish shifrining kriptotahlilini amalga oshirish.
3. Bir martalik bloknot shifrining kriptotahlilini amalga oshirish

Adabiyot va Internet saytlar:

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 - 816 с.
2. Венбо Мао. Современная криптография. Теория и практика. – Москва - Санкт-Петербург - Киев: Лори Вильямс, 2005.
3. Нильс Фергюсон, Брюс Шнайер. Практическая криптография –Москва: "Диалектика", 2004.
4. Столлингс В. Криптография и защита сетей. Принципы и практика. Изд.:Лори Вильямс, 2001.

2-amaliy ish. Simmetrik blokli shifrlar kriptotahlilida statistik usullar. Chiziqli, differensial va chiziqli-differensial kriptotahlil usullari (2 soat)

Amaliy ishning maqsadi – *Simmetrik blokli shifrlar kriptotahlilida chiziqli, differensial va chiziqli-differensial kriptotahlil usullarini qo‘llash bilim va ko‘nikmasiga ega bo‘lish.*

Nazariy qism

SP tarmog‘iga asoslangan 9 bit kirib 9 bit chiquvchi 3 raundli o‘quv algoritmiga chiziqli kriptotahlil o‘tkazish

Aytaylik, SP tarmog‘iga asoslangan ixtiyoriy S-blok tanlab olingan bo‘lsin. Tanlab olingan S-blokga nisbatan quyida korrelyatsion matritsani tuzish jarayonini 3 bit kirish va 3 bit chiqishga ega bo‘lgan chiziqsiz akslantirishda ko‘rib o‘tamiz[10].

S-blok

Kirish	0	1	2	3	4	5	6	7
Chiqish	7	1	4	0	6	2	5	3

2.3.1-jadval.Akslantirish jadvali.

Keltirilgan jadvalda birinchi satr kirish bitlari ikkinchi satr esa chiqish bitlarini ifodalaydi. Berilgan S-blokdan foydalanib, akslantirishning chinlik jadvali quyidagicha bo‘ladi.

Kirish	Chiqish
000	111
001	001
010	100
011	000
100	110
101	010
110	101
111	011

2.3.2-jadval. Berilgan S-blokning chinlik jadvali.

Mazkur misolda kiruvchi har bir variant uchun chiziqli kriptotahlil usulini olib borish va kalitning ba’zi bir bitlarini topishni ko‘rib chiqamiz.

Kalit bitlarini topishning bitta effektiv usuli, bu mavjud bo‘lgan barcha (variantlari)kombinatsiyalarini ko‘rib chiqishdan iborat bo‘lib, ushbu usul barcha variantlar sonini kamaytirgan holda berilgan SP tarmog‘iga asoslangan shifrlash algoritmi ma’lum bir akslantirishlarni o‘z ichiga olgan jarayonni ko‘rib chiqish yetarli bo‘ladi. Shuningdek, qaralayotgan algoritmning qaysi sikllarida qanday S-bloklar qatnashganligini (ochiq matnga bog‘liq) e’tiborga olish zarur.

2.3.3-jadvalda kirish bitlari har xil bo‘lgan bir nechta variantlar berilgan bo‘lib, bunda har bir S-bloklarga uch bit kirib uch bit chiqadi.

Birinchi xolatda 2.3.3-jadvaldagi kiruvchi X_9 bit qaysi S-bloklardan o‘tishini

ko‘radigan bo‘lsak, X_9 bit birinchi siklda S_{13}, ikkinchi siklda esa S_{21} va uchinchi siklda S_{31} blokka kiradi.

№	Kirish biti	Maxsus blok	Chiqish biti
1	X_9	$(S_{13}) \rightarrow (S_{21}) \rightarrow (S_{31})$	S_{31} bloklarning chiqishi 010_2, 011_2 va 110_2 ga teng
2	X_7, X_8, X_9	$(S_{13}) \rightarrow (S_{21}, S_{23}) \rightarrow (S_{31})$	S_{31} bloklarning chiqishi 010_2 va 110_2 ga teng
3	X_5	$(S_{12}) \rightarrow (S_{22}) \rightarrow (S_{32})$	S_{32} bloklarning chiqishi 011_2 va 110_2 ga teng
4	X_1, X_4	$(S_{11}, S_{12}) \rightarrow (S_{22}) \rightarrow (S_{33})$	Kiruvchi S_{31} blok,
5	X_2	$(S_{11}) \rightarrow (S_{22}) \rightarrow (S_{32})$	Kiruvchi S_{31} blok,
6	X_8	$(S_{13}) \rightarrow (S_{21}, S_{22}) \rightarrow (S_{31})$	Kiruvchi S_{31} blok,

2.3.3-jadval. Kiruvchi matn variantlari.

Yuqoridagi keltirilgan S-blok akslantirish jadvali orqali, unga mos bo‘lgan kiruvchi va chiquvchi vektorlar yordamida Korrelyatsion matritsalar jadvali quriladi. Korrelyatsion matritsada i-vektori kirish, j-vektori esa chiqish vektori bo‘lib, hisoblash quyidagi formula orqali amalga oshiriladi.

$$(\vec{Y}, \vec{j}) = (\vec{X}, \vec{i}) \qquad (2.3.1)$$

$1 \le i < 9, \quad 1 \le j < 9,$

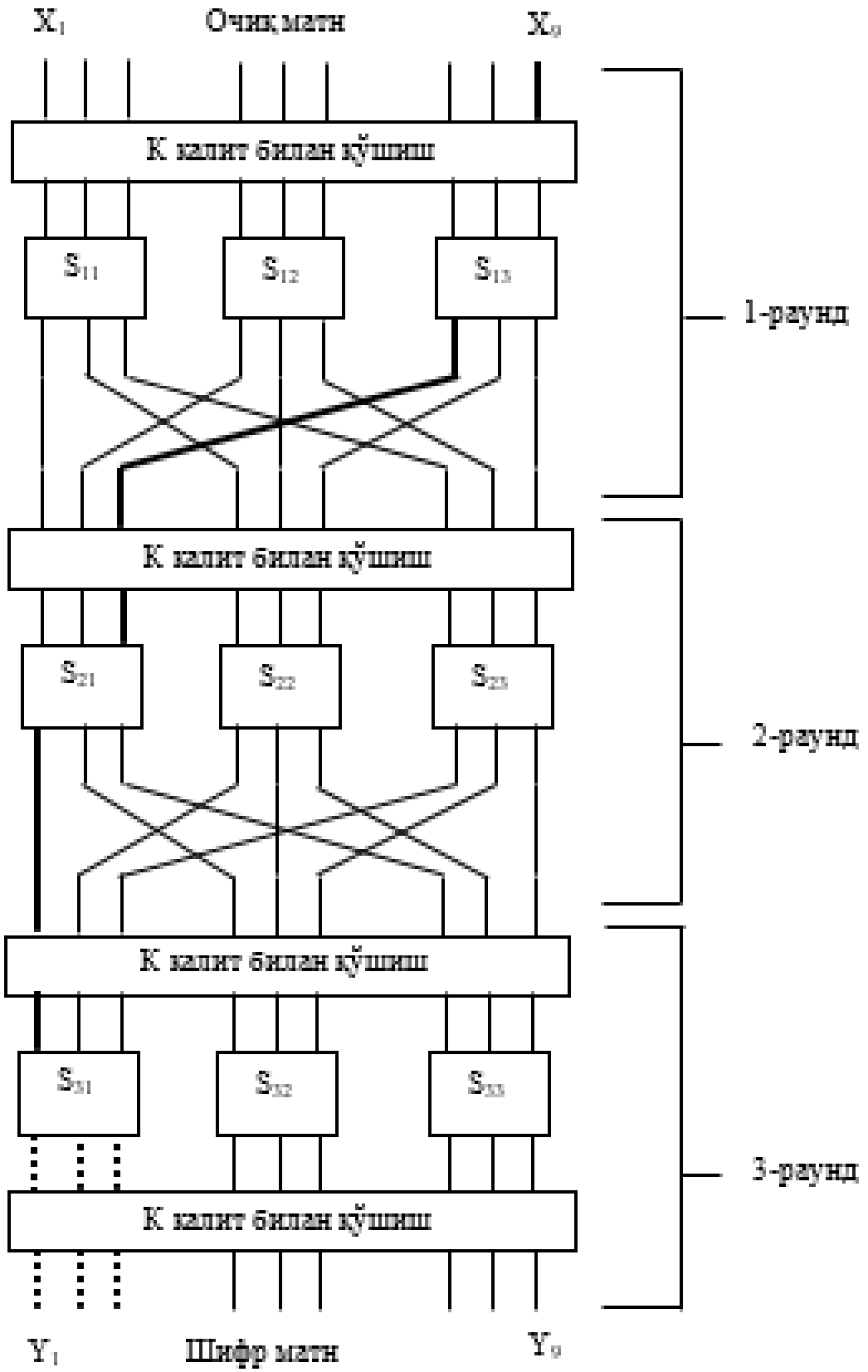
Bu yerda X –kiruvchi ochiq matn, Y esa shifr matn.

Akslantirish jadvalidagi S-blokga kiruvchi va chiquvchi bitlar $(000)_2$ dan $(111)_2$ gacha o‘zgarib turadi. U xolda (2.3.1) formula yordamida Korrelyatsion matritsa qurib olingandan so‘ng, eng katta chetlanishga ega bo‘lgan vektor qaraladi.

Biz ko‘rayotgan 3 bit kirish va 3 bit chiqishga ega bo‘lgan misolda (i, j): (1, 4), (6, 1) va (7, 5) vektorlarning kesishmasida turgan sonlar eng katta chetlanishga ega bo‘ladi. Bu qaralayotgan vektorlarda turgan qiymatlarning ehtimoligi 1/2 dan farqli bo‘lganligi uchun shu vektorlarni qaraymiz.

2.3.4-jadvaldagi birinchi (1, 4) vektorlar juftligini ko‘rib chiqamiz.

$S_{1,1}$ blokiga $(001)_2$ -kiruvchi matnning chiqishida $(100)_2$ bo‘lish ehtimolligi 2.3.4-jadvaldan (1, 4) vektorlar kesishmasidagi qiymat orqali aniqlanadi. Demak, kirish qiymati $(100)_2$ ga teng bo‘lgan bloklarni qarash yetarli. Shuningdek, mazkur jadvalda kirishda eng katta chetlanishga ega bo‘lgan chiqishlar mavjud emas. Bu esa eng katta chetlanishga, kichik chetlanishli ega bo‘lgan vektorlar juftligining ishlatilishini anglatadi.



2.3.1-rasm. O‘rniga qo‘yish va o‘rin almashtirish asosida qurilgan shifrlash tarmog‘i uchun chiziqli kriptotahlil usuli.

Keltirilgan S-blok uchun qurilgan korrelyatsion matritsa jadvali quyidagi

ko‘rinishga ega bo‘ladi[10].

j / I	1	2	3	4	5	6	7
1	4	4	4	0	4	4	4
2	4	2	2	4	4	6	2
3	4	2	6	4	4	6	6
4	4	6	6	4	4	6	2
5	4	2	6	4	4	2	2
6	0	4	4	4	4	4	4
7	4	4	4	4	8	4	4

2.3.4-jadval. Korrelyatsion matritsa jadvali.

2.3.3-jadvaldan foydalanib, $S_{1,3}$,$S_{2,1}$ va $S_{3,1}$ bloklarning yaqinlashishini ko‘rib chiqamiz. **2.**3.1-rasmdagi kiruvchi X_9 bit berilgan bo‘lsin. Bunda U_i orqali kiruvchi bit, V_j esa chiquvchi bitlar deb qaraladi. Qaralayotgan misolda kiruvchi va chiquvchi bloklarning uzunliklari 9 bit. Shunga mos mahfiy kalitning uzunligi ham 9 bit deb olinadi. Bu yerda $U_1 = X \oplus K$ kiruvchi 9 bitli ochiq matnga, 9 bitli mahfiy kalit XOR qilinadi.

2.3.1-rasm birinchi siklining chiziqli yaqinlashidan foydalanib, ehtimolligi nolga teng bo‘lgan:

$$V_{1,7} = U_{1,9} = X_9 \oplus K_9$$

(2.3.2)

ifodaga ega bo‘lamiz. Bu yerda $U_{1,9}$ –kiruvchi bit, $V_{1,7}$ –chiquvchi bit, X_9 –ochiq matn va K_9–raund kalitlarining mos bitlarini ifodalaydi. $S_{1,3}$ blok uchun chiziqli yaqinlashishini ko‘rib o‘tamiz. Ya’ni bunda 2.3.4-jadvaldagi (i, j)=(1, 4) vektorlar juftligi qaraladi. Jadvaldagi (1, 4) vektorning ehtimolik qiymati r_1=0/8 =0 ga teng. Ehtimollikga mos chetlanishi esa Δ=|1-2r|=|1-0|=1 tenglik bilan aniqlanadi.

2.3.1-rasmda ikkinchi raund uchun mos kirish va chiqish bitlari quyidagi ko‘rinishda bo‘ladi:

$$V_{2,1} = U_{2,3} \qquad (2.3.3)$$

buning ehtimolligi r_2=0 ga teng. Bunda $U_{2,3} = V_{1,7} \oplus K_3$ tenglikdan, (2.3.3) tenglik quyidagi ko‘rinishda bo‘ladi.

$$V_{2,1} = V_{1,7} \oplus K_3 \qquad (2.3.4)$$

(2.3.4) va (2.3.2) formulalarni bog‘lasak uning ko‘rinishi quyidagicha bo‘ladi:

$$V_{2,1} \oplus X_9 \oplus K_9 \oplus K_3 = 0 \qquad (2.3.5)$$

(2.3.5) ifodaning ehtimolligi quyidagi:

$$P = 1/2 + 2^{n-1}(P_1 - 1/2)(P_2 - 1/2)(P_3 - 1/2)...(P_n - 1/2) = 1/2 + 2^1(0-1/2)^2(0-1/2) = 1$$

formula orqali hisoblab topiladi. Bundan ko‘rinib turibdiki, chetlanish qiymati birga teng ekan.

Endi 2.3.3-jadvaldagi $S_{3,1}$ blokning chiqishi mumkin bo‘lgan barcha kombinatsiyalarini ko‘rib chiqamiz. Bu yerda $(111)_2$ dan boshqa variantlar ham mavjud deb qaraladi. $S_{3,1}$ blokka kiruvchi bit $(100)_2$ o‘nlik sanoq sistemasida $(4)_{10}$

ni ifodalaydi. Bunda $S_{3,1}$ blokka kirish $(100)_2$ bo‘lganda, chiqishi mumkin bo‘lgan qiymatlar: $(010)_2$, $(011)_2$, $(110)_2$ va $(111)_2$ bitlarga teng bo‘lishi mumkin. Quyida esa chiqishi $(010)_2$, $(011)_2$ va $(110)_2$ bo‘lgan bitlarni ko‘rib o‘tamiz. Birinchi $(010)_2$ xolatda uchinchi sikl uchun aniqlaymiz:

$$V_{3,2} = U_{3,1} \qquad (2.3.6)$$

va uning ehtimolligi 3/4 ga teng.

2.3.1-rasmda uchinchi sikldan chiqish biti $(010)_2$ bo‘lgan xolatni ko‘rib chiqamiz. Bunda kirish biti quyidagi ifoda orqali aniqlanadi $U_{3,1} = V_{2,1} \oplus K_1$, undan

$$V_{3,2} \oplus V_{2,1} \oplus K_1 = 0. \qquad (2.3.7)$$

Endi (2.3.7) formuladagi $V_{2,1}$ ning o‘rniga (2.3.5) formuladagi qiymatni qo‘ysak, uchta S-blok uchun quyidagi formulaga ega bo‘lamiz.

$$V_{3,2} \oplus X_9 \oplus K_9 \oplus K_3 \oplus K_1 = 0. \qquad (2.3.8)$$

(2.3.8) formulada $V_{3,2} = K_2 \oplus Y_2$ tenglikdan quyidagi kelib chiqadi.

$$K_2 \oplus Y_2 \oplus X_9 \oplus K_9 \oplus K_3 \oplus K_1 = 0, \qquad (2.3.9)$$

yoki

$$Y_2 \oplus X_9 = K_2 \oplus K_9 \oplus K_3 \oplus K_1. \qquad (2.3.10)$$

Yig‘uvchi lemmaga asosan, yuqoridagi tenglik:

$$P = 1/2 + 2^{n-1}(P_1 - 1/2)(P_2 - 1/2)(P_3 - 1/2)...(P_n - 1/2) = = 1/2 + 2^2(0 - 1/2)^2(3/4 - 1/2) = 3/4$$

ehtimollik bilan hisoblanadi.

2.3.1-rasmning uchinchi raundida $S_{3.1}$ blokka $(100)_2$ kirganda quyidagi tenglikka ega bo‘lamiz:

$$V_{3,2} \oplus V_{3,3} = U_{3,1} \qquad (2.3.11)$$

va uning ehtimoligi 3/4 ga teng.

2.3.1-rasmda uchinchi sikldan chiqish biti $011_{(2)}$ bo‘lgan xolatni ko‘rib chiqamiz. Bunda kirish biti quyidagi ifoda $U_{3,1} = V_{2,1} \oplus K_1$ orqali aniqlanadi, undan

$$V_{3,2} \oplus V_{3,3} \oplus V_{2,1} \oplus K_1 = 0. \qquad (2.3.12)$$

Endi (2.3.12) formuladagi $V_{2,1}$ ning o‘rniga (2.3.5) formuladagi qiymatni qo‘ysak, uchta S-blok uchun quyidagi formulaga ega bo‘lamiz.

$$V_{3,2} \oplus V_{3,3} \oplus X_9 \oplus K_9 \oplus K_3 \oplus K_1 = 0. \qquad (2.3.13)$$

Bu yerda $V_{3,2} = K_2 \oplus Y_2$ va $V_{3,3} = K_3 \oplus Y_3$ tengligidan, quyidagi kelib chiqadi.

$$K_2 \oplus Y_2 \oplus K_3 \oplus Y_3 \oplus X_9 \oplus K_9 \oplus K_3 \oplus K_1 = 0, \qquad (2.3.14)$$

yoki

$$Y_2 \oplus Y_3 \oplus X_9 = K_2 \oplus K_9 \oplus K_3 \oplus K_3 \oplus K_1 = K_2 \oplus K_9 \oplus K_1. \qquad (2.3.15)$$

Yig‘uvchi lemmaga asosan, yuqoridagi tenglik:

$$P = 1/2 + 2^{n-1}(P_1 - 1/2)(P_2 - 1/2)(P_3 - 1/2)...(P_n - 1/2) = 1/2 + 2^2(0 - 1/2)^2(3/4 - 1/2) = 3/4.$$

ehtimollik bilan hisoblanadi.

2.3.1-rasmning uchinchi raundida $S_{3.1}$ blokka $(100)_2$ kirganda quyidagi tenglikka ega bo‘lamiz:

$$V_{3,1} \oplus V_{3,2} = U_{3,1} \qquad (2.3.16)$$

buning ehtimoligi 1/4 ga teng.

2.3.1-rasmda uchinchi sikldan chiqish biti $110_{(2)}$ bo‘lgan xolatni ko‘rib

chiqamiz. Bunda kirish biti quyidagi ifoda orqali aniqlanadi: $U_{3,1} = V_{2,1} \oplus K_1$ dan

$$V_{3,1} \oplus V_{3,2} \oplus V_{2,1} \oplus K_1 = 0. \qquad (2.3.17)$$

Endi (2.3.17) formuladagi $V_{2,1}$ ning o‘rniga (2.3.5) formuladagi qiymatni qo‘ysak, uchta S-blok uchun quyidagi formulaga ega bo‘lamiz.

$$V_{3,1} \oplus V_{3,2} \oplus X_9 \oplus K_9 \oplus K_3 \oplus K_1 = 0. \qquad (2.3.18)$$

Bunda $V_{3,1} = K_1 \oplus Y_1$ tengligidan, quyidagi kelib chiqadi:

$$K_1 \oplus Y_1 \oplus K_2 \oplus Y_2 \oplus X_9 \oplus K_9 \oplus K_3 \oplus K_1 = 0. \qquad (2.3.19)$$

yoki

$$Y_1 \oplus Y_2 \oplus X_9 = K_2 \oplus K_9 \oplus K_3 \oplus K_1 \oplus K_1 = K_2 \oplus K_9 \oplus K_3. \qquad (2.3.20)$$

Yig‘uvchi lemmaga asosan, yuqoridagi tenglik:

$P = 1/2 + 2^{n-1}(P_1 - 1/2)(P_2 - 1/2)(P_3 - 1/2)...(P_n - 1/2) = 1/2 + 2^2(0 - 1/2)^2(3/4 - 1/2) = 3/4.$

ehtimollik bilan hisoblanadi.

Yuqorida keltirilgan 2.3.3-jadvalga asosan kirish biti X_7, X_8, X_9 bo‘lgan xolatda S_{13}, S_{21}, S_{23} va S_{31} bloklarning yaqinlashishini ko‘rib chiqamiz.

$U_1 = X \oplus K$ tenglik kiruvchi blokning 9 bitini ifodalaydi. Birinchi sikl uchun chiziqli yaqinlashishni hisoblab, 2.3.4-jadvalga muvofiq 1/4 ehtimollikka ega bo‘lamiz.

$$V_{1,7} \oplus V_{1,9} = U_{1,7} \oplus U_{1,8} \oplus U_{1,9} = X_7 \oplus K_7 \oplus X_8 \oplus K_8 \oplus X_9 \oplus K_9 \qquad (2.3.21)$$

Buning ehtimolligi 1 ga teng.

2.3.2-rasmda ikkinchi raund uchun quyidagiga ega bo‘lamiz:

$$V_{2,1} = U_{2,3} \qquad (2.3.22)$$

Buning ehtimolligi esa 0 ga teng. Shuningdek,

$$V_{2,7} = U_{2,9} \qquad (2.3.23)$$

buning ham ehtimolligi 0 ga teng.

Quyidagi $U_{2,3} = V_{1,7} \oplus K_3$ va $U_{2,9} = V_{1,9} \oplus K_9$ tengliklardan kelib chiqib, $V_{2,1} = V_{1,7} \oplus K_3$ formulaning ehtimolligi 0 ga teng. $V_{2,7} = V_{1,9} \oplus K_9$ bu tenglikning ham ehtimolligi 0 ga teng ekanligini yuqorida ko‘rib o‘tdik. Bu tengliklarni (2.3.21) formula bilan birlashtirsak, quyidagi tenglikka ega bo‘lamiz.

$$V_{2,1} \oplus K_3 \oplus V_{2,7} \oplus K_9 \oplus X_7 \oplus K_7 \oplus X_8 \oplus K_8 \oplus X_9 \oplus K_9 = 0 \qquad (2.3.24)$$

Buning ehtimolligi 1 ga teng.Endi 2.3.2-rasmdagi kirish biti $(101)_2$ bo‘lganda unga mos bo‘lgan chiqishlarni ko‘rib chiqamiz.

Birinchi xolatda uchinchi siklda chiqish biti $(010)_2$ bo‘lgan xolat uchun quyidagi:

$$V_{3,2} = U_{3,1} \oplus U_{3,3} \qquad (2.3.25)$$

ifodaga ega bo‘lamiz va u 1/4 ehtimollik bilan hisoblanadi.

2.3.2-rasmda uchinchi sikldan chiqish biti $010_{(2)}$ bo‘lgan xolatni ko‘rib chiqamiz. Bunda kirish biti quyidagi ifodalar: $U_{3,1} = V_{2,1} \oplus K_1$ va $U_{3,3} = V_{2,7} \oplus K_3$ orqali aniqlanadi, undan

$$V_{3,2} \oplus V_{2,1} \oplus K_1 \oplus V_{2,7} \oplus K_3 = 0 \qquad (2.3.26)$$

Endi (2.3.26) formuladagi $V_{2,1}$ ning o‘rniga (2.3.24) formuladagi qiymatni qo‘ysak uchta S-blok uchun quyidagi formulaga ega bo‘lamiz.

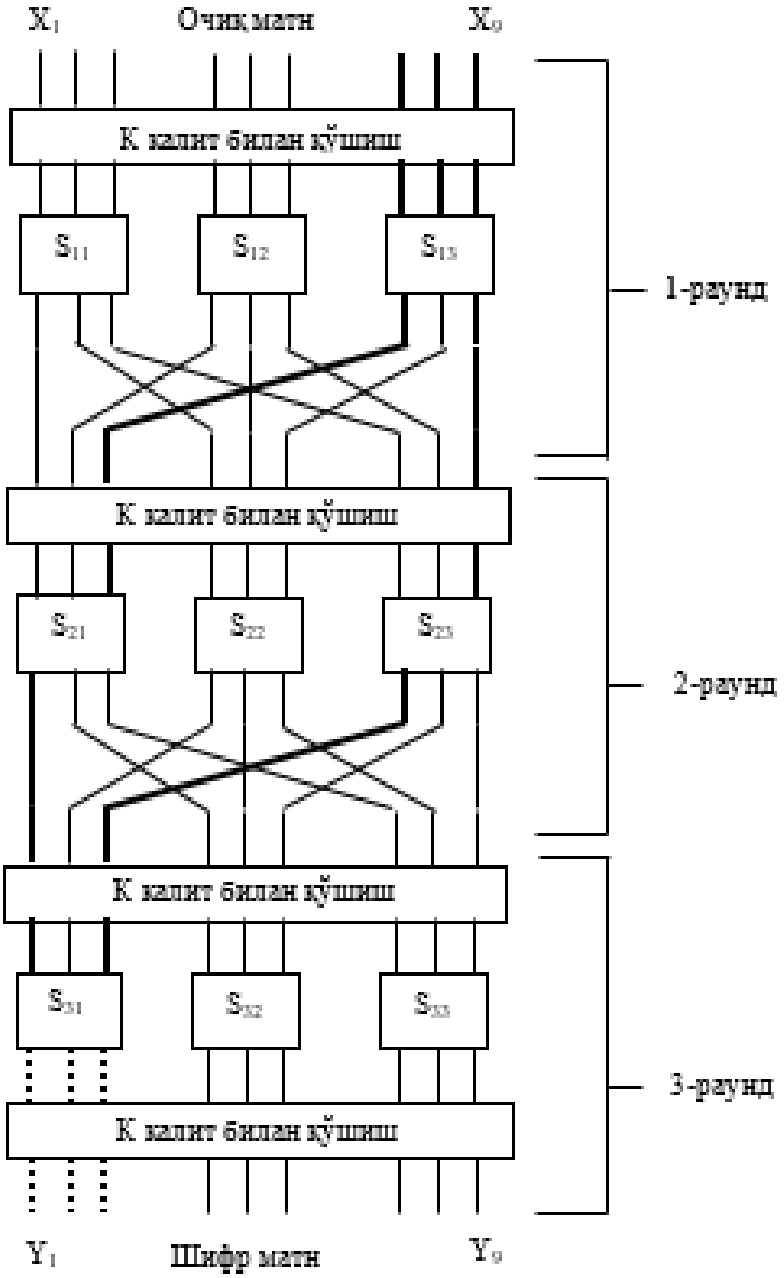
$$V_{3,2} \oplus K_1 \oplus K_3 \oplus K_3 \oplus K_9 \oplus X_7 \oplus K_7 \oplus X_8 \oplus K_8 \oplus X_9 \oplus K_9 = 0. \qquad (2.3.27)$$

(2.3.27) formulada $V_{3,2} = K_2 \oplus Y_2$ tenglikdan quyidagini yozish mumkin:

$$K_2 \oplus Y_2 \oplus K_1 \oplus K_3 \oplus K_3 \oplus K_9 \oplus X_7 \oplus K_7 \oplus X_8 \oplus K_8 \oplus X_9 \oplus K_9 = 0, \qquad (2.3.28)$$

yoki

$$Y_2 \oplus X_7 \oplus X_8 \oplus X_9 = K_1 \oplus K_7 \oplus K_8 \oplus K_2. \qquad (2.3.29)$$



2.3.2-rasm. O‘rniga qo‘yish va o‘rin almashtirish asosida qurilgan shifrlash tarmog‘i uchun chiziqli kriptotahlil usuli.

Yig‘uvchi lemmaga asosan, yuqoridagi tenglik:

$$P = 1/2 + 2^{n-1}(P_1 - 1/2)(P_2 - 1/2)(P_3 - 1/2)...(P_n - 1/2) = 1/2 + 2^3(1-1/2)(1/4-1/2) = 1/4.$$

ehtimollik bilan hisoblanadi.

2.3.2-rasmning uchinchi raundida $S_{3.1}$ blokka $(101)_2$ kirganda quyidagi tenglikka ega bo‘lamiz:

$$V_{3,1} \oplus V_{3,2} = U_{3,1} \oplus U_{3,3} \qquad (2.3.30)$$

ehtimoligi 1/4 ga teng.

2.3.2-rasmda uchinchi sikldan chiqish biti $110_{(2)}$ bo‘lgan xolatni ko‘rib chiqamiz. Bunda kirish biti quyidagi ifoda orqali aniqlanadi: $U_{3,1} = V_{2,1} \oplus K_1$ va $U_{3,2} = V_{2,7} \oplus K_3$, undan

$$V_{3,1} \oplus V_{3,2} \oplus V_{2,1} \oplus K_1 \oplus V_{2,7} \oplus K_3 = 0. \qquad (2.3.31)$$

Endi (2.3.31) formuladagi $V_{2,1}$ ning o‘rniga (2.3.24) formuladagi qiymatni qo‘ysak, uchta S-blok uchun quyidagi formulaga ega bo‘lamiz.

$$V_{3,1} \oplus V_{3,2} \oplus K_1 \oplus K_3 \oplus K_3 \oplus K_9 \oplus X_7 \oplus K_7 \oplus X_8 \oplus K_8 \oplus X_9 \oplus K_9 = 0. \qquad (2.3.32)$$

Bunda $V_{3,1} = K_1 \oplus Y_1$ va $V_{3,2} = K_2 \oplus Y_2$ tengligidan quyidagi kelib chiqadi.

$$K_1 \oplus Y_1 \oplus K_2 \oplus Y_2 \oplus K_1 \oplus K_3 \oplus K_3 \oplus K_9 \oplus X_7 \oplus K_7 \oplus X_8 \oplus K_8 \oplus X_9 \oplus K_9 = 0, \qquad (2.3.33)$$

yoki

$$Y_1 \oplus Y_2 \oplus X_7 \oplus X_8 \oplus X_9 = K_7 \oplus K_8 \oplus K_2. \qquad (2.3.34)$$

Yig‘uvchi lemmaga asosan, yuqoridagi tenglik:

$$P = 1/2 + 2^{n-1}(P_1 - 1/2)(P_2 - 1/2)(P_3 - 1/2)...(P_n - 1/2) == 1/2 + 2^3(1-1/2)(0-1/2)^2$$
$$(1/4 - 1/2) = 1/4$$

ehtimollik bilan hisoblanadi.

Yuqorida keltirilgan 2.3.3-jadvalga asosan kirish biti X_5 bo‘lgan xolatda S_{12}, S_{22} va S_{32} bloklarning yaqinlashishini ko‘rib chiqamiz.

$U_1 = X \oplus K$ tenglik kiruvchi blokning 9 bitini ifodalaydi. Birinchi sikl uchun chiziqli yaqinlashishni hisoblab, 2.3.4-jadvalga muvofiq 1/4 ehtimollikka ega bo‘lamiz.

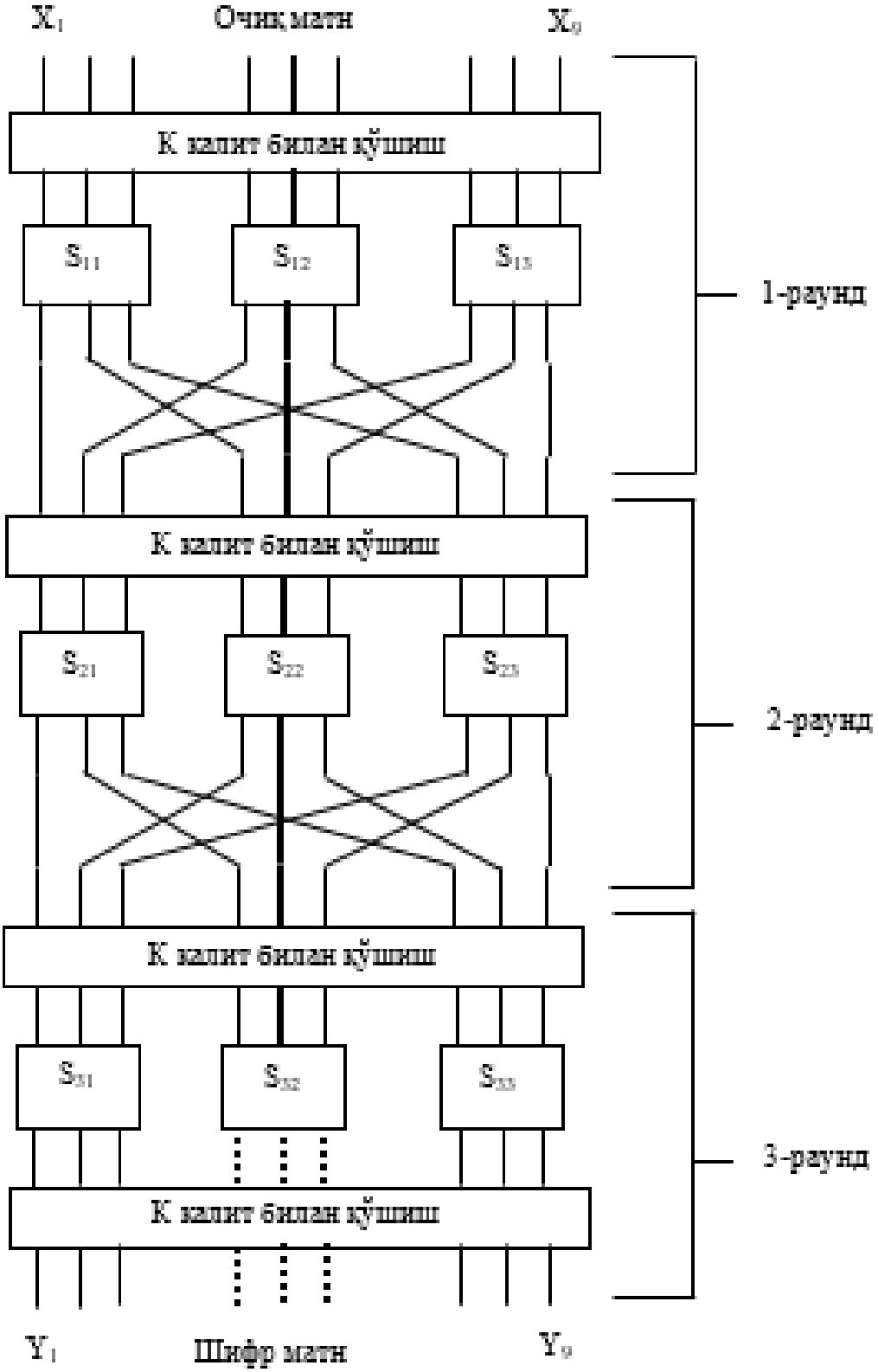
$$V_{1,5} = U_{1,5} = X_5 \oplus K_5 \qquad (2.3.35)$$

Ikkinchi raund uchun quyidagiga ega bo‘lamiz:

$$V_{2,5} = U_{2,5} \qquad (2.3.36)$$

Buning ehtimolligi 1/4 ga teng.

Quyidagi $U_{2,5} = V_{1,5} \oplus K_5$ tenglikdan, $V_{2,5} = V_{1,5} \oplus K_5$ formulaga ega bo‘lamiz. Bu tenglikni (2.3.35) formula bilan birlashtirsak, quyidagi tenglikka ega bo‘lamiz.



2.3.3-rasm. O‘rniga qo‘yish va o‘rin almashtirish asosida qurilgan shifrlash tarmog‘i uchun chiziqli kriptotahlil usuli.

$U_1 = X \oplus K$ tenglik kiruvchi blokning 9 bitini ifodalaydi. Birinchi sikl uchun

chiziqli yaqinlashishni hisoblab, 2.3.4-jadvalga muvofiq 1/4 ehtimollikka ega bo‘lamiz.

$$V_{1,5} = U_{1,5} = X_5 \oplus K_5$$

(2.3.35)

Ikkinchi raund uchun quyidagiga ega bo‘lamiz:

$$V_{2,5} = U_{2,5} \qquad (2.3.36)$$

Buning ehtimolligi 1/4 ga teng.

Quyidagi $U_{2,5} = V_{1,5} \oplus K_5$ tenglikdan, $V_{2,5} = V_{1,5} \oplus K_5$ formulaga ega bo‘lamiz. Bu tenglikni (2.3.35) formula bilan birlashtirsak, quyidagi tenglikka ega bo‘lamiz.

$$V_{2,5} \oplus K_5 \oplus X_5 \oplus K_5 = V_{2,5} \oplus X_5 = 0.$$

(2.3.37)

(2.3.37) formula 1/4 ehtimollik bilan bajariladi.

2.3.3-rasmda uchinchi sikldan chiqish biti $(011)_2$ bo‘lgan xolatni ko‘rib chiqamiz.

Birinchi $(011)_2$ xolatda uchta sikl uchun quyidagini

$$V_{3,5} \oplus V_{3,6} = U_{3,5} \qquad (2.3.38)$$

yozish mumkin va bu formula 1/4 ehtimollik bilan hisoblanadi.

Bunda kirish biti quyidagi ifoda orqali aniqlanadi: $U_{3,5} = V_{2,5} \oplus K_5$

$$V_{3,5} \oplus V_{3,6} \oplus V_{2,5} \oplus K_5 = 0. \qquad (2.3.39)$$

Endi (2.3.39) formuladagi $V_{2,5}$ ning o‘rniga (2.3.37) formuladagi qiymatni qo‘ysak, uchta S-blok uchun quyidagi:

$$V_{3,5} \oplus V_{3,6} \oplus K_5 \oplus X_5 = 0. \qquad (2.3.40)$$

tenglikka ega bo‘lamiz. Bu yerda $V_{3,5} = K_5 \oplus Y_5$ va $V_{3,6} = K_6 \oplus Y_6$ tengliklarni e’tiborga olib, quyidagini hosil qilamiz.

$$K_5 \oplus Y_5 \oplus K_6 \oplus Y_6 \oplus K_5 \oplus X_5 = 0, \qquad (2.3.41)$$

yoki

$$Y_5 \oplus Y_6 \oplus X_5 = K_6. \qquad (2.3.42)$$

Yig‘uvchi lemmaga asosan, yuqoridagi tenglik:

$P = 1/2 + 2^n (P_1 - 1/2)(P_2 - 1/2)(P_3 - 1/2)...(P_n - 1/2) = 1/2 + 2^3 (1/4 - 1/2)^3 = 7/16.$

ehtimollik bilan hisoblanadi.

2.3.3-rasmda uchinchi sikldan chiqish biti $110_{(2)}$ bo‘lgan xolatni ko‘rib chiqamiz. Bunda kirish biti quyidagi ifoda:

$$V_{3,4} \oplus V_{3,5} = U_{3,5}$$

(2.3.43)

va 3/4 ehtimollik bilan aniqlanadi.

Bunda kirish biti quyidagi ifoda orqali aniqlanadi: $U_{3,5} = V_{2,5} \oplus K_5$

$$V_{3,4} \oplus V_{3,5} \oplus V_{2,5} \oplus K_5 = 0. \qquad (2.3.44)$$

Endi (2.3.44) formuladagi $V_{2,5}$ ning o‘rniga (2.3.37) formuladagi qiymatni qo‘ysak, uchta S-blok uchun quyidagi:

$$V_{3,4} \oplus V_{3,5} \oplus X_5 \oplus K_5 = 0. \qquad (2.3.45)$$

tenglikka ega bo‘lamiz. Bu yerda $V_{3,4} = K_4 \oplus Y_4$ va $V_{3,5} = K_5 \oplus Y_5$ tenglikdan quyidagi:

$$K_4 \oplus Y_4 \oplus K_5 \oplus Y_5 \oplus K_5 \oplus X_5 = 0, \qquad (2.3.46)$$

kelib chiqadi Yig‘uvchi lemmaga asosan, yuqoridagi tenglik:

$P = 1/2 + 2^n (P_1 - 1/2)(P_2 - 1/2)(P_3 - 1/2)...(P_n - 1/2) = 1/2 + 2^2 (1/4 - 1/2)^2 (3/4 - 1/2) = 9/16$

ehtimollik bilan hisoblanadi.

Shunga o‘xshash 2.3.3-jadvaldagi kiruvchi boshqa bitlar uchun ham apraksimatsiya tenglamasi yuqorida bayon qilingan kabi quriladi.

№	Kirish ,chiqish va kalit bitlari	P-ehtimollik
1	$Y_2 \oplus X_9 = K_2 \oplus K_9 \oplus K_3 \oplus K_1$	3/4
	$Y_2 \oplus X_3 \oplus X_9 = K_2 \oplus K_9 \oplus K_1$	3/4
	$Y_1 \oplus Y_2 \oplus X_3 \oplus X_9 = K_2 \oplus K_9 \oplus K_1$	3/4
2	$Y_2 \oplus X_7 \oplus X_8 \oplus X_9 = K_1 \oplus K_7 \oplus K_8 \oplus K_2$	1/4
	$Y_1 \oplus Y_2 \oplus X_7 \oplus X_8 \oplus X_9 = K_7 \oplus K_8 \oplus K_2$	1/4
3	$Y_5 \oplus Y_6 \oplus X_5 = K_6$	7/16
	$Y_4 \oplus Y_5 \oplus X_5 = K_4$	9/16
4	$Y_8 \oplus Y_9 \oplus X_1 \oplus X_4 = K_1 \oplus K_5 \oplus K_9$	5/8
5	$Y_5 \oplus X_2 = K_2 \oplus K_4$	9/16
6	$Y_3 \oplus X_8 = K_8 \oplus K_6 \oplus K_2 \oplus K_1$	1/4

2.3.5-jadval. Aproksimatsiya jadvali.

Yuqorida bayon qilingan fikrlardan kelib chiqib, SP-tarmog‘i uchun chiziqli kriptotahlil o‘tkazish jarayoni shifrlash algoritmida foydalanilgan raund kalitlaridan qandaydir bitlarini topish imkoniyatini beradi. Haqiqiy kalit bitlarini tanlab olish chiziqli kriptotahlil usulida tuzilgan tenglamalarning ehtimolligidan kelib chiqib, quyidagi ko‘rinishda aniqlanadi.

SP tarmog‘iga asoslangan simmetrik shifrlash algoritmlariga differensial kriptotahlil usulining qo‘llanishiga misol

Aytaylik SP tarmog‘i asosidagi algoritm qaralayotgan bo‘lsin, uning chiziqsiz akslantirishi hisoblangan S-blok ko‘rinishi 2.3.1-jadvalda va o‘rin almashtirish akslantirishi 2.3.2-jadvalda keltirilgan:

2.3.1-jadval

Kirish	0	1	2	3	4	5	6	7
Chiqish	7	0	6	5	2	1	3	4

2.3.2- jadval

Kirish	1	2	3	4	5	6	7	8	9
Chiqish	1	4	7	2	5	8	3	6	9

Bundan keyingi bajariladigan amallarimizga qulay bo‘lishi uchun, 2.3.1-jadvalning ikkilik sanoq sistemasidagi ko‘rinishi quyidagi 2.3.3-jadvalda ko‘rsatilgan:

2.3.3-jadval

Kirish	000	001	010	011	100	101	110	111

Chiqish	111	000	110	101	010	001	011	100

Tahlil qilinadigan matnlar juftligi quyidagi tartibda olinishi kerak[4]:

1. Tahlil qilinayotgan orttirmalar soni yetarli darajada maxfiy kalitning barcha bitlarini o‘z ichiga olgan bo‘lishi lozim.

2. Agar tahlil qilinayotgan orttirmalar ehtimolliklari kichkina bo‘ladigan bo‘lsa, unda maxfiy kalit bitlarini topish murakkablashadi.

3. Ehtimolligi kichik bo‘lgan hollarda, maxfiy kalit bitlarini to‘liq topish uchun ochiq va yopiq matnlar juftliklarini ko‘proq olishga to‘g‘ri keladi.

Kiruvchi orttirma matnlarning variantlari quyidagi 2.3.4-jadvalda berilgan.

2.3.4-jadval

i	ΔA_i
1	110 000 000
2	000 000 111
3	001 001 000

Qaralayotgan shifrlash algoritmida 9-bitdan iborat kiruvchi matn olinadi va ma’lum bo‘lgan ΔA kiruvchi orttirma uchun $2^9=512$ variant mavjud bo‘ladi.Har bir kiruvchi orttirma uchta raunddan o‘tgandan so‘ng chiquvchi orttirma hisoblangan ΔC ni har xil ehtimolliklar bilan beradi. Shifrlash algoritmida maxfiy kalitni aniqlash uchun o‘rtacha to‘rtta kiruvchi orttirmani tahlil qilish yetarli bo‘ladi.

Avvalo S-blokni tahlil qilish uchun, ya’ni chiquvchi orttirma ΔC va kiruvchi orttirma hisoblangan ΔA ifodalarning o‘zaro bog‘liqligini ko‘rib o‘tamiz.Buning uchun esa differensial kriptotahlilning asosiy tushunchalaridan hisoblangan ayirma matritsa jadvalini tuzib olamiz.

Ayirma matritsaning qiymatlarini 1-bob, 2§-dagi (1.1.3) formulaga ko‘ra hisoblaymiz va uning ko‘rinishi $a=1(001_2)$ xol uchun 2.3.5-jadvalda ifoda etilgan:

2.3.5-jadval

$\mathbf{x}\in 2^3$	S(x)	$x\oplus a$	$S(x\oplus a)$	$b=S(x)\oplus S(x+a)$	b_{10}
000	111	001	000	111	7
001	000	000	111	111	7
010	110	011	101	011	3
011	101	010	110	011	3
100	010	101	001	011	3
101	001	100	010	011	3
110	011	111	100	111	7
111	100	110	011	111	7

Yuqoridagi jadval hisoblash natijalaridan $a=1$ kirishga nisbatan quyidagi taqsimot jadvalga ega bo‘lamiz:

2.3.6-jadval

$\Delta^{(F)}_{a\to b}$		b							
		0	1	2	3	4	5	6	7
a	1	0	0	0	4	0	0	0	4

Xuddi shu amallarni ***a*** ning barcha **0** dan **7** gacha qiymatlari uchun bajarib,

quyidagi umumiy kirish va chiqishga nisbatan taqsimot jadvalini hosil qilamiz:

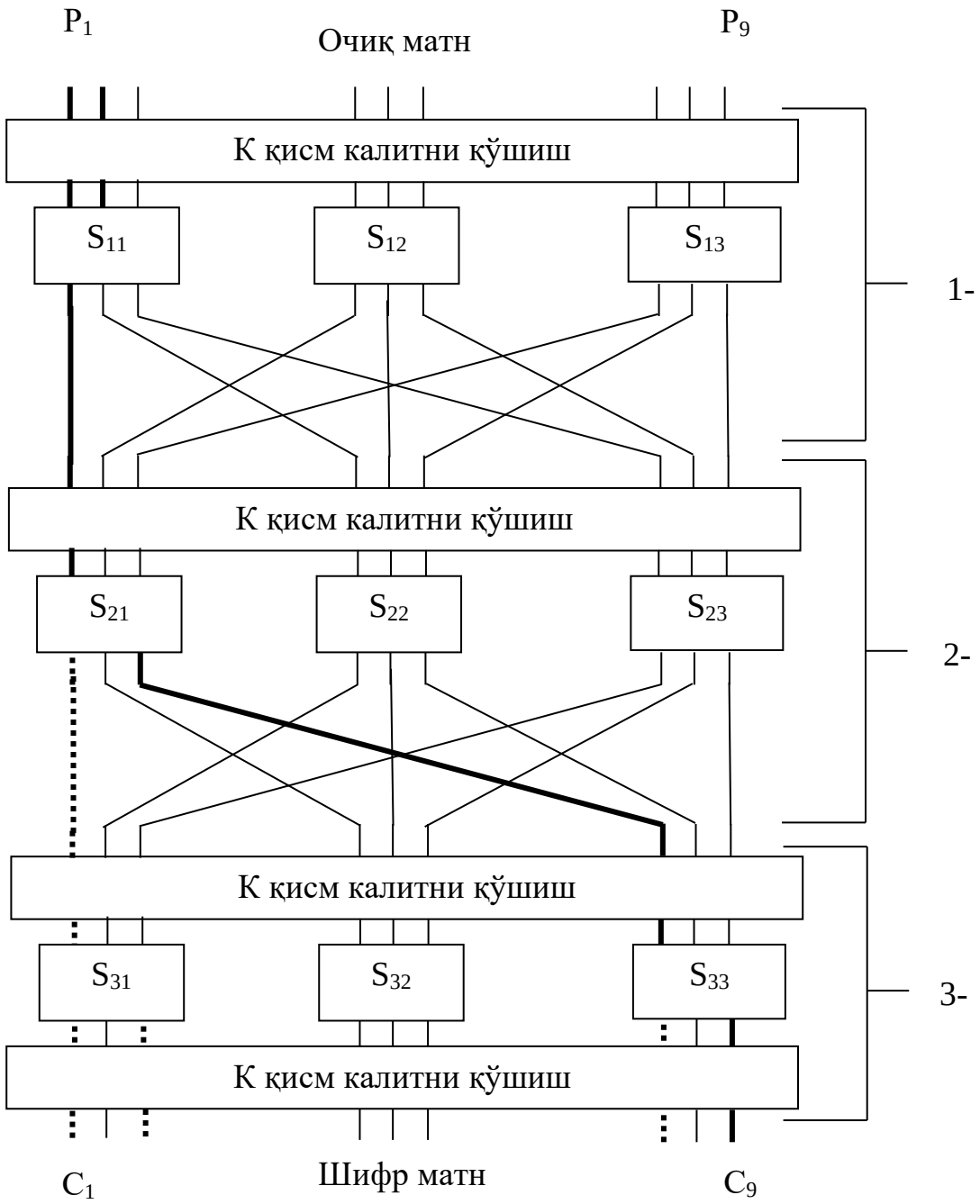
2.3.7-jadval

$\Delta C = b$ / $\Delta A = a$	000	001	010	011	100	101	110	111
000	8	0	0	0	0	0	0	0
001	0	0	0	4	0	0	0	4
010	0	4	0	0	0	4	0	0
011	0	0	4	0	0	0	4	0
100	0	4	0	0	0	4	0	0
101	0	0	4	0	0	0	4	0
110	0	0	0	0	8	0	0	0
111	0	0	0	4	0	0	0	4

ΔA_1-kiruvchi orttirma matnga mos SP-tarmog‘iga asoslangan shifrlash algoritmi 2.2.1-rasmda tasvirlangan bo‘lib, bu yerda S_{11} ,S_{12} , S_{13}, S_{21}, S_{22}, S_{23}, S_{31}, S_{32}, S_{33} –mos ravishda qism bloklarining, tegishli raundlarda foydalanilgan S – bloklari hisoblanadi.

ΔA_1 =110 000 000 birinchi kiruvchi orttirmani qaraymiz.Bu kiruvchi orttirmada S_{11} – blokga 110_2, S_{12} va S_{13}-bloklarga esa 000_2 orttirma kiradi.Shuning uchun S_{12} va S_{13}-bloklardan chiquvchi orttirma ham 000_2 qiymatni qabul qiladi.2.3.6-jadvalga ko‘ra , kiruvchi orttirma hisoblangan 110_2 ga har doim chiquvchi orttirma 100_2 mos keladi. Natijada, 1-raunddan keyin ya’ni o‘rin almashtirish jadvallaridan o‘tgandan so‘ng 2-raundga kiruvchi orttirmaning ko‘rinishi 100 000 000_2 ga teng bo‘ladi.Bu orttirmaga nisbatan S_{21}-blokga 100_2 ga teng bo‘lgan kiruvchi orttirma kirib keladi, S_{22} va S_{23} –bloklarga esa 000_2 ga teng bo‘lgan orttirma kiradi.6-jadvalga ko‘ra 100_2 kiruvchi orttirma 001_2 yoki 101_2 chiquvchi orttirmalarga teng bo‘lishi mumkin.Chiquvchi orttirma o‘rin almashtirish jadvalidan keyin, 3-raundga 000 000 100 yoki 100 000 100 orttirmalar kiradi.

Endi ΔA_i orttirmalarni beradigan ochiq matnlar juftligini aniqlab olamiz va uni maxfiy kalit bilan shifrlaymiz. Shifrlash natijasida hosil bo‘lgan shifr matnning ko‘rinishi 2.3.7-jadvalda keltirilgan.



2.3.1-rasm. O‘rniga quyish va o‘rin almashtirish tarmog‘i asosidagi shifrlash algoritmi uchun differensial kriptotahlil.

Quyidagi jadvalda ΔA_1=110 000 000$_2$ orttirmani beruvchi ochiq matnlar juftligi keltirilgan:

2.3.8-jadval

№	X	Y	X’	Y’
1	100111010	111011110	010111010	110011011
2	011101110	011000100	101101110	010000101
3	000101111	101111111	110101111	101111010
4	101111111	000111000	011111111	000111001
5	100110100	111010101	010110100	111010100

2.3.8-jadvaldagi birinchi juftlik matnni tahlil qilish jarayonini ko‘rib

chiqamiz. Bu kiruvchi ochiq matnga mos keluvchi,chiquvchi shifr matnning orttirmasi $\Delta C = 111011110_2 + 110011011_2 = 001000101_2$ ga teng. Demak, 000_2 ga teng bo‘lmagan orttirmalar S_{31}va S_{33} bloklarda mavjud bo‘ladi.Mazkur bloklarga kiruvchi orttirma esa 100_2 ga teng va bu ifodani beruvchi kiruvchi matnlar quyidagilar:

1. 000⊕ 100	5. 100⊕000
2. 001⊕101	6. 101⊕001
3. 010⊕110	7. 110⊕010
4. 011⊕111	8. 111⊕011

Ushbu kiruvchi har bir juftlik bitlarga mos keluvchi, chiquvchi juftliklar mavjud bo‘lib, qaralayotgan S-bloklarga asosan bu juftliklarning ko‘rinishi quyidagicha:

1. 111⊕010=101	5. 010⊕111=101
2. 000⊕001=001	6. 001⊕000=001
3. 110⊕011=101	7. 011⊕110=101
4. 101⊕100=001	8. 100⊕101=001

S_{31} blokdan chiquvchi orttirma qiymat 001_2 ga teng bo‘lib, u qabul qilishi mumkin bo‘lgan qiymatlar 2,4,6,8 ifodalarda o‘z aksini topgan. S_{31} dan chiqgan qiymatga qism kalit hisoblangan K_1 ni qo‘shganimizda bizga ma’lum bo‘lgan $Y_i, Y_i^{'}$,i=1,…,5 shifr matn hosil bo‘lish kerak.Natijada quyidagi tenglamaga kelamiz:

000⊕ K_1=111	100⊕K_1=111
001⊕K_1=110	101⊕K_1=110
001⊕K_1=111	101⊕K_1=111
000⊕K_1=110	100⊕K_1=110

Ushbu tenglamalardan qism kalit hisoblangan K_1 ni topadigan bo‘lsak, quyidagi 111_2 yoki 110_2 yoki 011_2 yoki 010_2 qiymatlardan birini qabul qilishi mumkin.

S_{33} -blokdan chiquvchi orttirma 101_2 ga teng, uning qabul qiladigan qiymatlari 1,3,5,7 tengliklarda o‘z aksini topgan. S_{33} dan chiqgan qiymatga qism kalit hisoblangan K_3 ni qo‘shganimizda bizga ma’lum bo‘lgan $Y_i, Y_i^{'}$,i=1,…,5 shifr matn hosil bo‘lish kerak.Natijada quyidagi tenglamalarga kelamiz:

111⊕K_3=110	011⊕K_3=110
010⊕K_3=011	110⊕K_3=011
010⊕K_3=110	011⊕K_3=110
111⊕K_3=011	110⊕K_3=011

Ushbu tenglamalardan qism kalit hisoblangan K_3 ni topadigan bo‘lsak, quyidagi 001_2 yoki 100_2 yoki 001_2 yoki 000_2 qiymatlardan birini qabul qiladi.

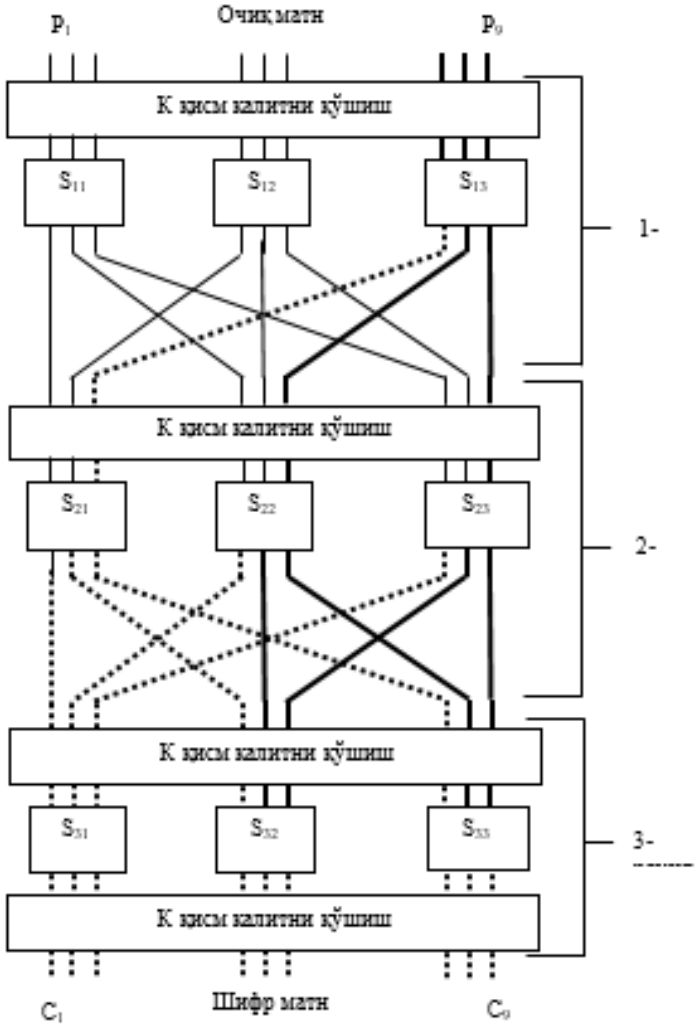
Demak, topilgan qiymatlar bizga mumkin bo‘lgan 8-bit uzunlikdagi kalit bitlarini topishni to‘rtta variantga kamaytirib berdi.

Endi ikkinchi kiruvchi orttirma hisoblangan ΔA_2=000 000 111_2 (2-rasm) qaraymiz.Kiruvchi orttirma hisoblangan ΔA_2 dan faqatgina S_{13} blokga 111_2 soni kiradi, S_{11} va S_{12} bloklarga esa 000_2 orttirma kiradi.Ayirma matritsadan ma’lumki, unga 000_2 orttirma kirganda har doim 000_2 orttirma chiqadi.Shuning uchun faqat S_{13}

blokga e’tiborimizni qaratamiz.

2.3.6-jadvalga ko‘ra, 111_2 orttirma kirganda chiquvchi orttirma 011_2 yoki 111_2 ga teng bo‘lishi mumkin. Natijada, birinchi raund akslantirishlaridan ya’ni o‘rin almashtirishlardan keyin ikkinchi raundga kiruvchi orttirmalarning ko‘rinishi 000 001 001_2 yoki 001 001 001_2 ga teng bo‘ladi.Bunday holat bizga S_{21} , S_{22} va S_{23} – bloklarga 001_2 orttirma kirishini anglatadi. 6-jadvalga ko‘ra esa 001_2 orttirma kirganda chiquvchi orttirmalar 011_2 yoki 111_2 ga teng bo‘ladi.Natijada, ikkinchi raund o‘rin almashtirishlaridan so‘ng, uchinchi raundga {*xxx x*11 *x*11} orttirma kiradi deb tushuniladi.Bu yerda *x* aniqmas bitni ifodalaydi. S_{31} blokga to‘liqligicha noma’lum bitlar kirganligi uchun bu blokni tahlil qilish imkoniyatini bermaydi.Demak, S_{32} va S_{33} bloklarga kiruvchi orttirmalarning qandaydir bitlari aniq, ya’ni *x*11 ga teng bo‘lganligi uchun tahlil qilish imkoniyati bor.Hamda ushbu kiruvchi orttirma 011_2 yoki 111_2 bo‘lishi mumkin.Quyida bu ikkala kiruvchi orttirmalar ustida tahlil olib boramiz.

Yuqorida qaralayotgan orttirmalarni beradigan ochiq matnlar juftligini aniqlab, ularni maxfiy kalit bilan shifrlaymiz. Shifrlash natijasida hosil bo‘lgan shifr matnning ko‘rinishi 2.3.8-jadvalda keltirilgan.



2.3.2-rasm. O‘rniga quyish va o‘rin almashtirish tarmog‘i asosidagi shifrlash algoritmi uchun differensial kriptotahlil.

Quyidagi jadvalda ΔA_1 =000 000 111_2 orttirmani beruvchi ochiq matnlar juftligi keltirilgan:

2.3.9-jadval

№	X	Y	X'	Y'
1	110011110	110000000	110011001	101110010
2	111111011	000001001	111111100	010010010
3	000111010	000011001	000111101	000100010
4	011100000	001101110	011100111	001111100
5	000000010	000011010	000000101	011100001

Birinchi juftlik matnni tahlil qilib ko‘ramiz. Bu kiruvchi ochiq matnga mos keluvchi, chiquvchi shifr matnning orttirmasi ΔC =110000000_2+101110010_2=011110010_2 ga teng. Demak, 000_2 ga teng bo‘lmagan orttirmalar faqat S_{32} va S_{33} bloklarda mavjud. S_{32} blokdan chiquvchi orttirma esa 110_2 ga teng.Oldin aniqlanganidek, S_{32} blokga 011_2 yoki 111_2 orttirmalar kirishi mumkin.6-jadvalga ko‘ra, S_{32} blokga mana shu hol uchun kiruvchi orttirma 011_2 ga teng va bu ifodani beruvchi kiruvchi matnlar quyidagilar:

1. 000⊕ 011
2. 001⊕010
3. 010⊕001
4. 011⊕000
5. 100⊕111
6. 101⊕110
7. 110⊕101
8. 111⊕100

Ushbu kiruvchi har bir juftlik bitlarga mos keluvchi chiquvchi juftliklar mavjud bo‘lib, qaralayotgan S-bloklarga asosan bu juftliklarning ko‘rinishi quyidagicha:

1. 111⊕101=010
2. 000⊕110=110
3. 110⊕000=010
4. 101⊕111=110
5. 010⊕100=110
6. 001⊕011=010
7. 011⊕001=010
8. 100⊕010=110

S_{32} blokdan chiquvchi orttirma qiymat 110_2 ga teng, va u qabul qilishi mumkin bo‘lgan qiymatlar 2,4,5,8 ifodalarda o‘z aksini topgan. S_{32} dan chiqgan qiymatga qism kalit hisoblangan K_2 ni qo‘shganimizda bizga ma’lum bo‘lgan shifr matn hosil bo‘lish kerak.Demak, quyidagi tenglamalarga kelamiz:

000⊕ K_2=000
110⊕K_2=110
110⊕K_2=000
000⊕K_2=110
100⊕K_2=000
010⊕K_2=110
010⊕K_2=000
100⊕K_2=110

Ushbu tenglamalardan qism kalit hisoblangan K_2 ni topadigan bo‘lsak, quyidagi 000_2 yoki 110_2 yoki 100_2 yoki 010_2 qiymatlarni qabul qilishi mumkin.

S_{33} -blokdan chiquvchi orttirma 010_2 ga teng bo‘lib, 2.3.6-jadvalga ko‘ra 010_2 chiquvchi orttirmani beradigan: 011_2 yoki 101_2 kiruvchi orttirma bo‘lishi mumkin.Oldin aniqlanganidek, kiruvchi orttirmalar 011_2 yoki 111_2 ga teng.Mazkur holatga kiruvchi orttirma 011_2 ga teng bo‘ladi. 011_2 ni beradigan esa 8 xil kiruvchi variant mavjud.

S_{33} blokdan chiquvchi orttirma 010_2 ga teng va uning qabul qiladigan qiymatlari 1,3,6,7 tengliklarda o‘z aksini topgan. S_{33} dan chiqgan qiymatga qism

kalit hisoblangan K_3 ni qo‘shganimizda ma’lum bo‘lgan $Y_i, Y_i^{'}, i=1,\ldots,5$ shifr matn hosil bo‘lish kerak.Natijada, quyidagi tenglamaga kelamiz:

$111 \oplus K_3=000$ $001 \oplus K_3=000$
$101 \oplus K_3=010$ $011 \oplus K_3=010$
$101 \oplus K_3=000$ $011 \oplus K_3=000$
$111 \oplus K_3=010$ $001 \oplus K_3=010$

Ushbu tenglamadan qism kalit hisoblangan K_3 ni topadigan bo‘lsak, quyidagi 111_2 yoki 101_2 yoki 001_2 yoki 011_2 qiymatlarni qabul qiladi.

Yuqorida aniqlangan K_3-kalitning qabul qilishi mumkin bo‘lgan to‘rt xil variant bor edi. Bular:$001_2, 100_2, 101_2$ yoki 000_2.

Topilgan kalit variantlaridan ko‘rinadiki, ular soni yana ikkitaga kamaygan,ya’ni:101_2 yoki 001_2.Ular ichida bittasi aslida haqiqiy qism kalitni beradi.

Endi ikkinchi juftlik matnni tahlil qilib ko‘ramiz. Bu kiruvchi ochiq matnga mos keluvchi, chiquvchi shifr matnning orttirmasi $\Delta C = 000001001_2 + 010010010_2 = 010011011_2$ ga teng. Demak, 000_2 ga teng bo‘lmagan orttirmalar S_{32} va S_{33} bloklarda mavjud. S_{32} va S_{33} bloklardan chiquvchi orttirmalar bir xil, ya’ni 011_2 ga teng ekan. Bu chiquvchi orttirmani beruvchi qiymat 2.3.6-jadvalga ko‘ra 001_2 yoki 111_2 orttirmalar kirgan bo‘lishi mumkin. Bu kiruvchi orttirma bizga ma’lum bo‘lgan 111_2 ga teng va bu ifodani beruvchi kiruvchi matnlar quyidagilar:

1. $000 \oplus 111$
2. $001 \oplus 110$
3. $010 \oplus 101$
4. $011 \oplus 100$
5. $100 \oplus 011$
6. $101 \oplus 010$
7. $110 \oplus 001$
8. $111 \oplus 000$

Ushbu kiruvchi har bir juftlik bitlarga mos keluvchi chiquvchi juftliklar mavjud bo‘lib, qaralayotgan S-bloklarga asosan bu juftliklarning ko‘rinishi quyidagicha:

1. $111 \oplus 100=011$
2. $000 \oplus 011=011$
3. $110 \oplus 001=111$
4. $101 \oplus 010=111$
5. $010 \oplus 101=111$
6. $001 \oplus 110=111$
7. $011 \oplus 000=011$
8. $100 \oplus 111=011$

S_{32} va S_{33} blokdan chiquvchi orttirma qiymat 011_2 ga teng, va u qabul qilishi mumkin bo‘lgan qiymatlar 1,2,7,8 ifodalarda hosil bo‘lgan. S_{32} va S_{33} dan chiqgan qiymatga qism kalit hisoblangan K_2 va K_3 ni qo‘shganimizda bizga ma’lum bo‘lgan shifr matn hosil bo‘lish kerak.Natijada, quyidagi tenglamaga kelamiz:

$111 \oplus K_2=111 \oplus K_3=001$ $011 \oplus K_2=011 \oplus K_3=001$
$100 \oplus K_2=100 \oplus K_3=010$ $000 \oplus K_2=000 \oplus K_3=010$
$100 \oplus K_2=100 \oplus K_3=001$ $000 \oplus K_2=000 \oplus K_3=001$
$111 \oplus K_2=111 \oplus K_3=010$ $011 \oplus K_2=011 \oplus K_3=010$

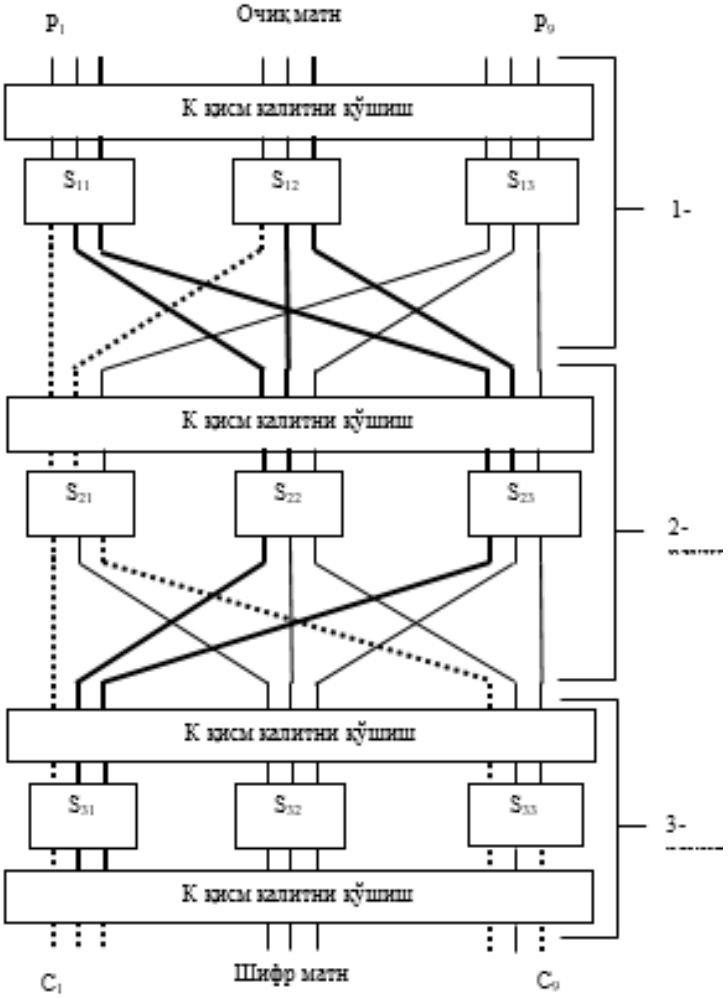
Ushbu tenglamalardan qism kalit hisoblangan K_2 va K_3 ni topadigan bo‘lsak, 110_2 yoki 101_2 yoki 010_2 yoki 001_2 quyidagi qiymatlarni qabul qilishi mumkin.

Bizning qo‘limizda oldin ham aniqlangan K_2 qabul qilishi mumkin bo‘lgan to‘rtta variant bor edi. Bular:$000_2, 110_2, 100_2$ yoki 010_2.

Topilgan variant kalitlaridan ko‘rinadiki, mazkur variantlar soni yana ikkitaga kamaydi,bular:110 yoki 010 bularning bittasi haqiqiy qism kalitni beradi.

Natijada qolgan kiruvchi matnlarni tahlil qilishimiz shart emas, chunki kiruvchi orttirmalar 011_2 yoki 111_2 ga teng.Izlanayotgan qism kalitlar, topilgan qism kalitlar bilan ustma-ust tushadi.

Uchinchi ΔA_3=001 001 000_2 (2.3.3-rasm) kirish orttirmasini qarash bilan olib borilayotgan tahlilga yakun yasaymiz.Kiruvchi orttirma ΔA_3 ning 001_2 qiymati S_{11} va S_{12} bloklarga kiradi, S_{13} ga esa 000_2 orttirma kiradi.Ayirma matritsadan ma’lumki, 000_2 orttirma kirganda har doim 000_2 orttirma chiqadi.Shuning uchun S_{13} blokdan chiquvchi orttirma 000_2 ga teng.6-jadvalga ko‘ra 001_2 orttirma kirganda, chiquvchi orttirma 011_2 yoki 111_2 ga teng bo‘ladi.Natijada,birinchi raund o‘rin almashtirishlaridan keyin ikkinchi raundga {*xx*0 110 110} orttirma kiradi.Bu yerda *x* noma’lum bit hisoblanadi. Shuningdek 6-jadvalga ko‘ra kiruvchi orttirma 110_2 ga teng bo‘lsa, chiquvchi orttirma 100_2 ga teng bo‘ladi.Agar kiruvchi orttirma 010_2 yoki 100_2 bo‘lganda, chiqish orttirmasi 001_2 yoki 101_2 ga teng bo‘ladi.Shunday qilib, o‘rin almashtirishlardan keyin, uchinchi raundga {*x*11 000 *x*0*x*} orttirma kirib keladi.Bunday holda, S_{31} blokga kiruvchi orttirma 011_2 yoki 111_2 ga teng bo‘lishi mumkin. 011_2 orttirma kirganda chiquvchi orttirma 010_2 yoki 110_2 ga teng bo‘lishi mumkin, 111_2 kirganda esa chiquvchi orttirma 011_2 yoki 111_2 bo‘lishi mumkin.



2.3.3-rasm. O‘rniga quyish va o‘rin almashtirish tarmog‘i asosidagi shifrlash

algoritmi uchun differensial kriptotahlil.

Endi berilgan orttirmalarni beradigan ochiq matnlar juftligini aniqlab olamiz va uni maxfiy kalit bilan shifrlaymiz. Shifrlash natijasida hosil bo‘lgan shifr matnning ko‘rinishi 2.3.10-jadvalda berilgan:

2.3.10-jadval

№	X	Y	X’	Y’
1	111010111	011111111	110011111	000111111
2	011001001	101110001	010000001	011110001
3	011101110	011000100	010100110	101000101
4	110101000	110101000	111100000	001101000
5	110100111	001111001	111101111	110111001

2.3.10-jadvaldagi birinchi juftlik matnni tahlil jarayonini ko‘rib chiqamiz. Bu kiruvchi ochiq matnga mos keluvchi, chiquvchi shifr matnning orttirmasi $\Delta C = 011111111_2 + 000111111_2 = 011000000_2$ ga teng. Demak, 000_2 ga teng bo‘lmagan orttirma S_{31} bloklarda mavjud. S_{31} blokdan chiquvchi orttirma esa 011_2 ga teng.Oldin aniqlanganidek, S_{31} blokga 011_2 yoki 111_2 orttirmalar kirishi mumkin.6-jadvalga ko‘ra S_{31} blokdan mazkur orttirmalar chiqishi uchun kiruvchi orttirma 111_2 ga teng bo‘lishi lozim. 111_2 kiruvchi orttirmani beruvchi ifodalar esa quyidagilar:

1. $000 \oplus 111$
2. $001 \oplus 110$
3. $010 \oplus 101$
4. $011 \oplus 100$
5. $100 \oplus 011$
6. $101 \oplus 010$
7. $110 \oplus 001$
8. $111 \oplus 000$

Ushbu kiruvchi har bir juftlik bitlarga mos keluvchi chiquvchi har bir juftliklar mavjud bo‘lib, fiksirlangan S-bloklarga asosan, bu juftliklarning ko‘rinishi quyidagicha:

1. $111 \oplus 100 = 011$
2. $000 \oplus 011 = 011$
3. $110 \oplus 001 = 111$
4. $101 \oplus 010 = 111$
5. $010 \oplus 101 = 111$
6. $001 \oplus 110 = 111$
7. $011 \oplus 000 = 011$
8. $100 \oplus 111 = 011$

S_{31} blokdan chiquvchi orttirma qiymat 111_2 ga teng. U qabul qilishi mumkin bo‘lgan qiymatlar 1,2,7,8 ifodalarda hosil bo‘ladi. S_{31} dan chiqgan qiymatga qism kalit hisoblangan K_1 ni qo‘shganimizda bizga ma’lum bo‘lgan shifr matn hosil bo‘lish kerak.Natijada, quyidagi tenglamalarga kelamiz:

$111 \oplus K_1 = 011$ $\quad$ $011 \oplus K_1 = 011$

$100 \oplus K_1 = 000$ $\quad$ $000 \oplus K_1 = 000$

$100 \oplus K_1 = 011$ $\quad$ $000 \oplus K_1 = 011$

$111 \oplus K_1 = 000$ $\quad$ $110 \oplus K_1 = 000$

Ushbu tenglamalardan qism kalit hisoblangan K_1 ni topadigan bo‘lsak, quyidagi 100_2 yoki 111_2 yoki 000_2 yoki 011_2 qiymatlarni qabul qilishi mumkin.

Bizning qo‘limizda oldin ham aniqlangan K_1 qabul qilishi mumkin bo‘lgan to‘rt xil variant bor edi. Bular:111_2,110_2,011_2 yoki 010_2.

Bu topilgan variant kalitlaridan ko‘rinadiki, ularning soni yana ikkitaga kamaydi,ya’ni:111_2 yoki 011_2. Ularning bittasi aslida haqiqiy qism kalitni beradi.

Shunday qilib, har biri maxfiy kalit hisoblangan: K_1, K_2 va K_3 kalitlarning

ikkitadan qabul qilishi mumkin bo‘lgan qiymatlariga ega bo‘ldik. K_1 uchun bu qiymat 111_2 yoki 011_2 ga, K_2 uchun bu qiymat 110_2 yoki 010_2 ga va K_3 uchun esa bu qiymat 101_2 yoki 001_2 ga teng bo‘ldi.Xulosa qilsak,biz 512 ta mumkin bo‘lgan variantlarni quyidagi 8 variantga kamaytirdik:

1. 111110101
2. 111010101
3. 111110001
4. 111010001
5. 011110101
6. 011110001
7. 011010101
8 .011010001

Ushbu maxfiy kalitlarni berilgan ochiq matnga mos shifr matnlar bilan tekshirib ko‘radigan bo‘lsak, haqiqiy kalit {$K=111010001_2$} ekanligiga ishonch hosil qilamiz.

Amaliy bajarish uchun vazifalar.

1. Simmetrik blokli shifrlash algoritmlari uchun chiziqli kriptotahlilni amalga oshirish.

2. Simmetrik blokli shifrlash algoritmlari uchun differensial kriptotahlilni amalga oshirish.

2. Simmetrik blokli shifrlash algoritmlari uchun chiziqli-differensial kriptotahlilni amalga oshirish.

Adabiyot va Internet saytlar:

1. Шеннон К. Теория и связи в секретных системах. Работы по теории информации и кибернетике. – М.: Иностранная лит. 1963. – 243 б.
2. Авдошин С.М., Савельева А.А. «Криптоанализ: вчера, сегодня, завтра», Государственный университет – Высшая Школа Экономики. Москва – 2007.
3. «Kriptografik tizimlarni kriptoanalizlashning istiqbolli usullarini ishlab chiqish va ularni tadqiq etish» mavzusi bo‘yicha bajarilgan ilmiy-tadqiqot ishining 1-bosqich hisoboti. – O‘zAAA «UNICON.UZ» DUK Toshkent, 2009./

3-amaliy ish. Simmetrik blokli shifrlar kriptotahlili. Algebraik, integral, “Slaydli hujum” va apparat xatoliklarni generatsiyalashga asoslangan kriptotahlil usullari.

Amaliy ishning maqsadi – *Simmetrik blokli shifrlar kriptotahlilida algebraik, integral, “Slaydli hujum” va apparat xatoliklarni generatsiyalashga asoslangan kriptotahlil usullarini qo‘llanilishi bo‘yicha bilim va ko‘nikmasiga ega bo‘lish*.

Nazariy qism

S – blok akslantirishini algebraik ifodalovchi tenglamalar sistemasini tuzish va uni to‘g‘ri tenglama ekanligini tekshirishga quyidagicha misol ko‘rib o‘tish mumkin.

Aytaylik, 2 bit kirish va 1 bit chiqishga ega bo‘lgan quyidagi S – blok jadvali (4.24-jadval) qaralayotgan bo‘lsin:

4.24-jadval

S – blok jadvali

X	0	1	2	3
Y	1	0	0	1

Ushbu S – blok akslantirishiga mos chinlik jadvalining (4.25-jadval) ko‘rinishi quyidagicha bo‘ladi:

4.25-jadval

S – blok chinlik jadvali

№	**x_1**	**x_2**	**y**
1	0	0	1
2	0	1	0
3	1	0	0
4	1	1	1

Qaralayotgan misolda tenglamalar ishlab chiqish uchun mumkin bo‘lgan birhadlarning umumiy soni 7 (ya’ni $t=7$) ta bo‘lib, ular quyidagilardir: x_1, x_2, y, x_1x_2, x_1y, x_2y, η. Demak, birxadlarning $2^7=128$ ta kombinatsiyasi mavjud bo‘lib, ular asosida tuzilgan tenglamalar 4.26-jadvalda keltirilgan.

4.26-jadval

2x1 – o‘lchamli S – blok uchun mumkin bo‘lgan tenglamalar

№	**Tenglama**	**№**	**Tenglama**
1.	$*0=0$	**65.**	$x_1=0$
2.	$*1=0$	**66.**	$x_1 \oplus 1=0$
3.	$x_2y=0$	**67.**	$x_1 \oplus x_2y=0$
4.	$x_2y \oplus 1=0$	**68.**	$x_1 \oplus x_2y \oplus 1=0$
5.	$x_1y=0$	**69.**	$x_1 \oplus x_1y=0$
6.	$x_1y \oplus 1=0$	**70.**	$x_1 \oplus x_1y \oplus 1=0$
7.	$x_1y \oplus x_2y=0$	**71.**	$x_1 \oplus x_1y \oplus x_2y=0$
8.	$x_1y \oplus x_2y \oplus 1=0$	**72.**	$x_1 \oplus x_1y \oplus x_2y \oplus 1=0$
9.	$x_1x_2=0$	**73.**	$x_1 \oplus x_1x_2=0$
10.	$x_1x_2 \oplus 1=0$	**74.**	$x_1 \oplus x_1x_2 \oplus 1=0$
11.	$x_1x_2 \oplus x_2y=0$	**75.**	$x_1 \oplus x_1x_2 \oplus x_2y=0$
12.	$x_1x_2 \oplus x_2y \oplus 1=0$	**76.**	$x_1 \oplus x_1x_2 \oplus x_2y \oplus 1=0$
13.	$x_1x_2 \oplus x_1y=0$	**77.**	$x_1 \oplus x_1x_2 \oplus x_1y=0$
14.	$x_1x_2 \oplus x_1y \oplus 1=0$	**78.**	$x_1 \oplus x_1x_2 \oplus x_1y \oplus 1=0$
15.	$x_1x_2 \oplus x_1y \oplus x_2y=0$	**79.**	$x_1 \oplus x_1x_2 \oplus x_1y \oplus x_2y=0$
16.	$x_1x_2 \oplus x_1y \oplus x_2y \oplus 1=0$	**80.**	$x_1 \oplus x_1x_2 \oplus x_1y \oplus x_2y \oplus 1=0$
17.	$y=0$	**81.**	$x_1 \oplus y=0$

№	Tenglama	№	Tenglama
18.	$y \oplus 1=0$	**82.**	$x_1 \oplus y \oplus 1=0$
19.	$y \oplus x_2y=0$	**83.**	$x_1 \oplus y \oplus x_2y=0$
20.	$y \oplus x_2y \oplus 1=0$	**84.**	$x_1 \oplus y \oplus x_2y \oplus 1=0$
21.	$y \oplus x_1y=0$	**85.**	$x_1 \oplus y \oplus x_1y=0$
22.	$y \oplus x_1y \oplus 1=0$	**86.**	$x_1 \oplus y \oplus x_1y \oplus 1=0$
23.	$y \oplus x_1y \oplus x_2y=0$	**87.**	$x_1 \oplus y \oplus x_1y \oplus x_2y=0$
24.	$y \oplus x_1y \oplus x_2y \oplus 1=0$	**88.**	$x_1 \oplus y \oplus x_1y \oplus x_2y \oplus 1=0$
25.	$y \oplus x_1x_2=0$	**89.**	$x_1 \oplus y \oplus x_1x_2=0$
26.	$y \oplus x_1x_2 \oplus 1=0$	**90.**	$x_1 \oplus y \oplus x_1x_2 \oplus 1=0$
27.	$y \oplus x_1x_2 \oplus x_2y=0$	**91.**	$x_1 \oplus y \oplus x_1x_2 \oplus x_2y=0$
28.	$y \oplus x_1x_2 \oplus x_2y \oplus 1=0$	**92.**	$x_1 \oplus y \oplus x_1x_2 \oplus x_2y \oplus 1=0$
29.	$y \oplus x_1x_2 \oplus x_1y=0$	**93.**	$x_1 \oplus y \oplus x_1x_2 \oplus x_1y=0$
30.	$y \oplus x_1x_2 \oplus x_1y \oplus 1=0$	**94.**	$x_1 \oplus y \oplus x_1x_2 \oplus x_1y \oplus 1=0$
31.	$y \oplus x_1x_2 \oplus x_1y \oplus x_2y=0$	**95.**	$x_1 \oplus y \oplus x_1x_2 \oplus x_1y \oplus x_2y=0$
32.	$y \oplus x_1x_2 \oplus x_1y \oplus x_2y \oplus 1=0$	**96.**	$x_1 \oplus y \oplus x_1x_2 \oplus x_1y \oplus x_2y \oplus 1=0$
33.	$x_2=0$	**97.**	$x_1 \oplus x_2=0$
34.	$x_2 \oplus 1=0$	**98.**	$x_1 \oplus x_2 \oplus 1=0$
35.	$x_2 \oplus x_2y=0$	**99.**	$x_1 \oplus x_2 \oplus x_2y=0$
36.	$x_2 \oplus x_2y \oplus 1=0$	**100.**	$x_1 \oplus x_2 \oplus x_2y \oplus 1=0$
37.	$x_2 \oplus x_1y=0$	**101.**	$x_1 \oplus x_2 \oplus x_1y=0$
38.	$x_2 \oplus x_1y \oplus 1=0$	**102.**	$x_1 \oplus x_2 \oplus x_1y \oplus 1=0$
39.	$x_2 \oplus x_1y \oplus x_2y=0$	**103.**	$x_1 \oplus x_2 \oplus x_1y \oplus x_2y=0$
40.	$x_2 \oplus x_1y \oplus x_2y \oplus 1=0$	**104.**	$x_1 \oplus x_2 \oplus x_1y \oplus x_2y \oplus 1=0$
41.	$x_2 \oplus x_1x_2=0$	**105.**	$x_1 \oplus x_2 \oplus x_1x_2=0$
42.	$x_2 \oplus x_1x_2 \oplus 1=0$	**106.**	$x_1 \oplus x_2 \oplus x_1x_2 \oplus 1=0$
43.	$x_2 \oplus x_1x_2 \oplus x_2y=0$	**107.**	$x_1 \oplus x_2 \oplus x_1x_2 \oplus x_2y=0$
44.	$x_2 \oplus x_1x_2 \oplus x_2y \oplus 1=0$	**108.**	$x_1 \oplus x_2 \oplus x_1x_2 \oplus x_2y \oplus 1=0$
45.	$x_2 \oplus x_1x_2 \oplus x_1y=0$	**109.**	$x_1 \oplus x_2 \oplus x_1x_2 \oplus x_1y=0$
46.	$x_2 \oplus x_1x_2 \oplus x_1y \oplus 1=0$	**110.**	$x_1 \oplus x_2 \oplus x_1x_2 \oplus x_1y \oplus 1=0$
47.	$x_2 \oplus x_1x_2 \oplus x_1y \oplus x_2y=0$	**111.**	$x_1 \oplus x_2 \oplus x_1x_2 \oplus x_1y \oplus x_2y=0$
48.	$x_2 \oplus x_1x_2 \oplus x_1y \oplus x_2y \oplus 1=0$	**112.**	$x_1 \oplus x_2 \oplus x_1x_2 \oplus x_1y \oplus x_2y \oplus 1=0$
49.	$x_2 \oplus y=0$	**113.**	$x_1 \oplus x_2 \oplus y=0$
50.	$x_2 \oplus y \oplus 1=0$	**114.**	$x_1 \oplus x_2 \oplus y \oplus 1=0$
51.	$x_2 \oplus y \oplus x_2y=0$	**115.**	$x_1 \oplus x_2 \oplus y \oplus x_2y=0$
52.	$x_2 \oplus y \oplus x_2y \oplus 1=0$	**116.**	$x_1 \oplus x_2 \oplus y \oplus x_2y \oplus 1=0$
53.	$x_2 \oplus y \oplus x_1y=0$	**117.**	$x_1 \oplus x_2 \oplus y \oplus x_1y=0$
54.	$x_2 \oplus y \oplus x_1y \oplus 1=0$	**118.**	$x_1 \oplus x_2 \oplus y \oplus x_1y \oplus 1=0$
55.	$x_2 \oplus y \oplus x_1y \oplus x_2y=0$	**119.**	$x_1 \oplus x_2 \oplus y \oplus x_1y \oplus x_2y=0$
56.	$x_2 \oplus y \oplus x_1y \oplus x_2y \oplus 1=0$	**120.**	$x_1 \oplus x_2 \oplus y \oplus x_1y \oplus x_2y \oplus 1=0$
57.	$x_2 \oplus y \oplus x_1x_2=0$	**121.**	$x_1 \oplus x_2 \oplus y \oplus x_1x_2=0$
58.	$x_2 \oplus y \oplus x_1x_2 \oplus 1=0$	**122.**	$x_1 \oplus x_2 \oplus y \oplus x_1x_2 \oplus 1=0$
59.	$x_2 \oplus y \oplus x_1x_2 \oplus x_2y=0$	**123.**	$x_1 \oplus x_2 \oplus y \oplus x_1x_2 \oplus x_2y=0$

№	Tenglama	№	Tenglama
60.	$x_2 \oplus y \oplus x_1x_2 \oplus x_2y \oplus 1=0$	**124.**	$x_1 \oplus x_2 \oplus y \oplus x_1x_2 \oplus x_2y \oplus 1=0$
61.	$x_2 \oplus y \oplus x_1x_2 \oplus x_1y=0$	**125.**	$x_1 \oplus x_2 \oplus y \oplus x_1x_2 \oplus x_1y=0$
62.	$x_2 \oplus y \oplus x_1x_2 \oplus x_1y \oplus 1=0$	**126.**	$x_1 \oplus x_2 \oplus y \oplus x_1x_2 \oplus x_1y \oplus 1=0$
63.	$x_2 \oplus y \oplus x_1x_2 \oplus x_1y \oplus x_2y=0$	**127.**	$x_1 \oplus x_2 \oplus y \oplus x_1x_2 \oplus x_1y \oplus x_2y=0$
64.	$x_2 \oplus y \oplus x_1x_2 \oplus x_1y \oplus x_2y \oplus 1=0$	**128.**	$x_1 \oplus x_2 \oplus y \oplus x_1x_2 \oplus x_1y \oplus x_2y \oplus 1=0$

* tenglama emas, lekin mumkin bo‘lgan variantlardan biri hisoblanadi.

Tuzilgan ushbu tenglamalarning to‘g‘ri ekanligini aniqlash uchun, berilgan S – blokga ko‘ra tekshiruv jadvalini tuzish lozim. Shunga ko‘ra, tuzilgan tekshiruv jadvali quyidagi 4.27-jadvalda keltirilgan.

4.27-jadval

2x1 – o‘lchamli S blok tekshiruv jadvali

	1	**2**	**3**	**4**	**5**	**6**	**7**
	x_2	x_1	y	x_1x_2	x_1y	x_2y	η
1	0	0	1	0	0	0	1
2	0	1	0	0	0	0	1
3	1	0	0	0	0	0	1
4	1	1	1	1	1	1	1

Tuzilgan 128 tenglamani mazkur jadval bilan tekshirish asosida, S – blokning har bir kirish va chiqish qiymatlarida (4 ta) bajariluvchi 7 ta to‘g‘ri tenglama hosil qilindi. Ushbu to‘g‘ri tenglamalar quyidagi 4.28-jadvalda keltirilgan.

4.28-jadval

2x1 – o‘lchamli S – blok uchun topilgan to‘g‘ri tenglamalar

№	Tenglama
1.	$x_1y \oplus x_2y=0$
2.	$x_1x_2 \oplus x_2y=0$
3.	$x_1x_2 \oplus x_1y=0$
4.	$x_1 \oplus x_2 \oplus y \oplus 1=0$
5.	$x_1 \oplus x_2 \oplus y \oplus x_1y \oplus x_2y \oplus 1=0$
6.	$x_1 \oplus x_2 \oplus y \oplus x_1x_2 \oplus x_2y \oplus 1=0$
7.	$x_1 \oplus x_2 \oplus y \oplus x_1x_2 \oplus x_1y \oplus 1=0$

Mazkur 7 tenglamani tahlil qilish asosida ulardan 3 tasi chiziqli erkli (masalan, 1-, 2- va 3-tenglamalar) ekanligi ma’lum bo‘ldi. Teorema 4.1. ga ko‘ra ham, 2x1 – o‘lchamli S – blok uchun $r \geq 7-2^2=3$ ta chiziqli erkli tenglama mavjud bo‘ladi. Demak, ushbu chiziqli erkli tenglamalar berilgan S – blok akslantirishini ifodalovchi va kriptoanaliz uchun lozim bo‘lgan dastlabki tenglamalar hisoblanadi.

Algebraik kriptoanalizning ushbu bosqichida bajariladigan amallar soni (1-bosqichning qiyinchilik darajasi) tahlil qilinayotgan akslantirish o‘lchamiga uzviy bog‘liq bo‘ladi. Masalan, 8x8 – o‘lchamli S – blok uchun *t=137* bo‘lib, to‘g‘ri tenglamalarni hosil qilishda (1.1) ifodaga ko‘ra 2^{137} ta tenglamani ko‘rib chiqish kerak bo‘ladi. Lekin, mazkur bosqichni parallel hisoblash orqali ham amalga oshirish mumkin.

S-KN1 shifrlash algoritmi uchun integral kriptoanaliz usulining qo‘llanishiga misol

S-KN1 simmetrik shifrlash algoritmi SP tarmog‘iga asoslangan bo‘lib, blok uzunligi 8 bit ma’lumotni 16 bit uzunlikdagi kalit yordamida shifrlash va deshifrlashga qaratilgan. Algoritmning raundlari soni 3 tani tashkil qiladi. Algoritm dastlabki ma’lumotlarga birinchi raund kaliti K_1 ni qo‘shishdan boshlanadi. Ushbu operatsiyadan keyin uchta raund akslashtirishlari amalga oshiriladi. Har bir raundda xabar ikkita 4 bitli qismga (nibbles) bo‘linadi, ularning har biri S almashtirish blokidan o‘tadi, so‘ngra qismlar birlashtiriladi va keyin L chiziqli akslantirishga beriladi. Har bir raund tegishli kalit bilan 2 modul bo‘yicha qo‘shish amali bilan tugaydi. *L* akslantirishi ikki takrorlashda amalga oshiriladi, shunda bitta nibble bitta takrorlash paytida o‘zgartiriladi, boshqa nibble esa o‘ngga siljiydi. Nibblesdagi hisoblashlar quyidagi formulalar bo‘yicha amalga oshiriladi:

$$r_1 = 3a_0 \oplus a_1;$$
$$r_2 = 3a_1 \oplus a_0; \qquad (4.23)$$

L^{-1} akslantirishidagi hisoblashlar formulalari esa quyidagicha ko‘rinishga ega:

$$a_0 = 3r_1 \oplus r_2;$$
$$a_1 = 3a_0 \oplus r_1; \qquad (4.24)$$

L akslantirishida barcha hisoblashlar $GF(2)[x]/\psi(x)$ maydonda bajariladi, bu yerda $\psi(x) = x^4 + x + 1 \in GF(2)[x]$.

Ishda S va unga teskari bo‘lgan S^{-1} akslantirishida foydalanish uchun ikkita almashtirish jadvali keltirilgan.

4.29-jadval

S akslantirishda foydalaniladigan almashtirish jadvali

Kirish	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
Chiqish	3	6	a	7	f	0	5	b	2	c	1	e	4	9	d	8

4.30-jadval

S^{-1} akslantirishda foydalaniladigan almashtirish jadvali

Kirish	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
Chiqish	5	a	8	0	c	6	1	3	f	d	2	7	9	e	b	4

Ta’kidlab o‘tilganidek, integral kriptoanaliz usulini biror-bir shifrlash algoritmiga qo‘llash uchun, tanlab olingan ochiq matnlar va ularga mos shifrmatnlarning maxsus to‘plami ma’lum bo‘lishi lozim. Ochiq matnlar to‘plamini tanlashning keltirilgan qoidalariga ko‘ra, S-KN1 shifrlash algoritmiga integral kriptoanaliz usulini qo‘llash uchun quyidagicha P_i (i = 0,1,2,...,15) ochiq matnlar to‘plami tanlandi.

P_0= 0000 1100 P_8= 1000 1100
P_1= 0001 1100 P_9= 1001 1100
P_2= 0010 1100 P_{10}= 1010 1100
P_3= 0011 1100 P_{11}= 1011 1100
P_4= 0100 1100 P_{12}= 1100 1100
P_5= 0101 1100 P_{13}= 1101 1100
P_6= 0110 1100 P_{14}= 1110 1100
P_7= 0111 1100 P_{15}= 1111 1100

Ushbu ochiq matnlarning dastlabki yarim bayti qiymati bilan farqlanadi. Ushbu to‘plamni delta to‘plam deb ataymiz. To‘plamdagi bir xil qiymatlarga ega 16 ta ochiq matn qismlarini – passiv bo‘lak deb, 16 ta turli xil qiymatga ega qismlarini – aktiv bo‘lak deb nomlaymiz.

Natijada, chap qismda turgan yarim bayt aktiv bo‘lak, qolgan yarim baytlar esa passiv bo‘laklar bo‘ladi.

Agar barcha bo‘laklar ustida XOR amali bajarilsa, aktiv bo‘lakdagi barcha 16 ta ochiq matnning natijasi 0000 ga teng bo‘ladi, ya’ni:

$$XOR_{active}=0000 \oplus 0001 \oplus 0010 \oplus 0011 \oplus 0100 \oplus 0101 \oplus 0110 \oplus 0111 \oplus 1000 \oplus 1001 \oplus 1010 \oplus 1011 \oplus 1100 \oplus 1101 \oplus 1110 \oplus 1111=0000$$

Shuningdek, XOR amalini passiv bo‘laklar uchun ham bajarilganda, natija 0000 bo‘ladi, ya’ni:

$$XOR_{passive}=1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus \oplus 1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus =0000$$

Tanlab olingan ushbu delta to‘plam balanslashganlik xossasini bajaradi va shuning uchun ham aktiv va passiv bo‘laklardagi har bir pozitsiyaning XOR yig‘indisi 0 ga teng bo‘ladi.

Kriptoanaliz jarayonini shartli 2 bosqichga, ya’ni: ochiq matnlar to‘plamini kuzatish va so‘ngi raund kalitini aniqlash bosqichlariga ajratish mumkin. Ochiq matnlar to‘plamini kuzatish bosqichi, tahlil qilinayotgan

shifrlash algoritmining so‘ngi raundiga kirishida to‘plamning balanslashgan bo‘lagi mavjud yoki mavjud emasligini aniqlashga qaratilgan.

Agar balanslashgan element mavjud bo‘lsa, so‘ngi raundning ushbu bo‘lakka mos qism kalitini aniqlash imkoniyati tug‘iladi.

Shundan kelib chiqib, quyida tanlab olingan delta to‘plamning S-KN1 shifrlash algoritmi payndlaridan o‘tish jarayonini kuzatib boramiz.

Shifrlash algoritmining raund kalitlarini qo‘shish bloki, kuzatilayotgan to‘plam elementlari qiymatning o‘zgarishiga olib keladi, lekin to‘plamning balanslashganligiga ta’sir qilmaydi. Shuning uchun ham kriptoanaliz jarayonida ushbu blok e’tiborga olinmaydi. Ammo, qaralayotgan mazkur misolda, kriptoanaliz so‘ngida aniqlanuvchi kalit bilan solishtirish maqsadida, kalit qo‘shish bloki ham kiritildi.

Algoritmda shifrlash jarayonida foydalanish maqsadida quyidagi keltirilgan kalitlar generatsiya qilindi:

0-raund kaliti: 1010 0010
1-raund kaliti: 0101 0101
2-raund kaliti: 0010 1110
3-raund kaliti: 1001 1100

Algoritmda dastlab kalit bilan 2 modul bo‘yicha qo‘shish amali bajariladi. Quyida raund kalitlari bilan qo‘shish amalidan keyingi qiymatlar keltirilgan.

$$A_0=X(K_0,P_0)=X(1010\ 0010,0000\ 1100)=1010\ 1110$$
$$A_1=X(K_0,P_1)=X(1010\ 0010,0001\ 1100)=1011\ 1110$$
$$A_2=X(K_0,P_2)=X(1010\ 0010,0010\ 1100)=1000\ 1110$$
$$A_3=X(K_0,P_3)=X(1010\ 0010,0011\ 1100)=1001\ 1110$$
$$A_4=X(K_0,P_4)=X(1010\ 0010,0100\ 1100)=1110\ 1110$$
$$A_5=X(K_0,P_5)=X(1010\ 0010,0101\ 1100)=1111\ 1110$$
$$A_6=X(K_0,P_6)=X(1010\ 0010,0110\ 1100)=1100\ 1110$$
$$A_7=X(K_0,P_7)=X(1010\ 0010,0111\ 1100)=1101\ 1110$$
$$A_8=X(K_0,P_8)=X(1010\ 0010,1000\ 1100)=0010\ 1110$$
$$A_9=X(K_0,P_9)=X(1010\ 0010,1001\ 1100)=0011\ 1110$$
$$A_{10}=X(K_0,P_{10})=X(1010\ 0010,1010\ 1100)=0000\ 1110$$
$$A_{11}=X(K_0,P_{11})=X(1010\ 0010,1011\ 1100)=0001\ 1110$$
$$A_{12}=X(K_0,P_{12})=X(1010\ 0010,1100\ 1100)=0110\ 1110$$
$$A_{13}=X(K_0,P_{13})=X(1010\ 0010,1101\ 1100)=0111\ 1110$$
$$A_{14}=X(K_0,P_{14})=X(1010\ 0010,1110\ 1100)=0100\ 1110$$
$$A_{15}=X(K_0,P_{15})=X(1010\ 0010,1111\ 1100)=0101\ 1110$$

S-KN1 shifrlash algoritmining birinchi raundidagi dastlabki akslantirish S (S – blok akslantirishlari jadvali) akslantirishi bo‘lib, ushbu akslantirishidan keyin delta to‘plamning o‘zgarishi qo‘yidagicha bo‘ladi:

$B_0=S(1010\ 1110)=0001\ 1101$ $B_8=S(0010\ 1110)=1010\ 1101$
$B_1=S(1011\ 1110)=1110\ 1101$ $B_9=S(0011\ 1110)=0111\ 1101$
$B_2=S(1000\ 1110)=0010\ 1101$ $B_{10}=S(0000\ 1110)=0011\ 1101$
$B_3=S(1001\ 1110)=1100\ 1101$ $B_{11}=S(0001\ 1110)=0110\ 1101$
$B_4=S(1110\ 1110)=1101\ 1101$ $B_{12}=S(0110\ 1110)=0101\ 1101$
$B_5=S(1111\ 1110)=1000\ 1101$ $B_{13}=S(0111\ 1110)=1011\ 1101$
$B_6=S(1100\ 1110)=0100\ 1101$ $B_{14}=S(0100\ 1110)=1111\ 1101$
$B_7=S(1101\ 1110)=1001\ 1101$ $B_{15}=S(0101\ 1110)=0000\ 1101$

E’tiborga olish kerakki, ushbu akslantirishdan keyin ham faqat bitta aktiv bo‘lak bor va quyidagi tenglik o‘rinli:

$$XOR_{active}= 0000$$
$$XOR_{passive}= 0000$$

Demak, S akslantirishi aktiv va passivligiga yoki ularning balanslashganligiga ta’sir etmaydi.

Keyingi akslantirish L akslantirishi bo‘lib, ushbu akslantirishdagi barcha hisoblashlar $GF(2)[x]/\psi(x)$ $(\psi(x)=x^4+x+1\in GF(2)[x])$ maydonda bajariladi.

Kuzatilayotgan to‘plamning L akslantirishdan keyingi holati quyidagicha bo‘ladi:

S_0=L(0001 1101)=0000 1110 S_8=L(1010 1101)=1010 0000
S_1=L(1110 1101)=1001 1100 S_9=L(0111 1101)=1011 0100
S_2=L(0010 1101)=1100 1011 S_{10}=L(0011 1101)=1000 1000
S_3=L(1100 1101)=0001 1010 S_{11}=L(0110 1101)=1111 0111
S_4=L(1101 1101)=0101 1001 S_{12}=L(0101 1101)=0011 0010
S_5=L(1000 1101)=0010 0110 S_{13}=L(1011 1101)=1110 0011
S_6=L(0100 1101)=0111 0001 S_{14}=L(1111 1101)=1101 1111
S_7=L(1001 1101)=0110 0101 S_{15}=L(0000 1101)=0100 1101

Ko‘rish mumkinki, L akslantirishidan keyin to‘plamda bitta emas, ikkita aktiv bo‘laklar hosil bo‘ldi ya’ni, L akslantirishi 1-ustundagi 1 ta aktiv yarim baytni 2 ta aktiv bo‘lakka kengaytirmoqda.

Ushbu holatda ham aktiv va passiv bo‘laklar ustida XOR amalini bajarsak, quyidagi natijani olamiz:

$$XOR_{active}= 0000$$
$$XOR_{passive}= 0000$$

Ya’ni, kuzatilayotgan to‘plam hali ham balanslashgan.

Shundan so‘ng, yana, X akslantirishi bajariladi. Ushbu akslantirish

natijasi, ya’ni K_1 kalit bilan XOR amali yordamida qo‘shishdan keyingi to‘plamning o‘zgarishi quyidagicha bo‘ladi:

$$D_0=X(K_1,C_0)=X(0101\ 0101,0000\ 1110)=0101\ 1011$$
$$D_1=X(K_1,C_1)=X(0101\ 0101,1001\ 1100)=1100\ 1001$$
$$D_2=X(K_1,C_2)=X(0101\ 0101,1100\ 1011)=1001\ 1110$$
$$D_3=X(K_1,C_3)=X(0101\ 0101,0001\ 1010)=0100\ 1111$$
$$D_4=X(K_1,C_4)=X(0101\ 0101,0101\ 1001)=0000\ 1100$$
$$D_5=X(K_1,C_5)=X(0101\ 0101,0010\ 0110)=0111\ 0011$$
$$D_6=X(K_1,C_6)=X(0101\ 0101,0111\ 0001)=0010\ 0100$$
$$D_7=X(K_1,C_7)=X(0101\ 0101,0110\ 0101)=0011\ 0000$$
$$D_8=X(K_1,C_8)=X(0101\ 0101,1010\ 0000)=1111\ 0101$$
$$D_9=X(K_1,C_9)=X(0101\ 0101,1011\ 0100)=1110\ 0001$$
$$D_{10}=X(K_1,C_{10})=X(0101\ 0101,1000\ 1000)=1101\ 1101$$
$$D_{11}=X(K_1,C_{11})=X(0101\ 0101,1111\ 0111)=1010\ 0010$$
$$D_{12}=X(K_1,C_{12})=X(0101\ 0101,0011\ 0010)=0110\ 0111$$
$$D_{13}=X(K_1,C_{13})=X(0101\ 0101,1110\ 0011)=1011\ 0110$$
$$D_{14}=X(K_1,C_{14})=X(0101\ 0101,1101\ 1111)=1000\ 1010$$
$$D_{15}=X(K_1,C_{15})=X(0101\ 0101,0100\ 1101)=0001\ 1000$$

Kalit qo‘shilganidan keyin ham quyidagi ifoda o‘rinli:

$$XOR_{active}= 0000$$
$$XOR_{passive}= 0000$$

Demak, delta to‘plam haligacha balanslashmagan. Yuqorida aytib o‘tilganidek ushbu natija oldingi natija kabi bo‘lib, kalit qiymatiga bog‘liq emas.

Umumiy holda, ushbu kuzatilayotgan to‘plamning 1– raund akslantirishlaridan keyingi o‘zgarishlari quyidagi 4.31-jadvalda keltirilgan.

4.31–jadval

Kuzatilayotgan to‘plamning 1-raunddan keyingi o‘zgarishi

1-raund				
Aks-sh	**X**	**S**	**L**	**X**
1-blok	1010 1110	0001 1101	0000 1110	0101 1011
2-blok	1011 1110	1110 1101	1001 1100	1100 1001
3-blok	1000 1110	0010 1101	1100 1011	1001 1110
4-blok	1001 1110	1100 1101	0001 1010	0100 1111
5-blok	1110 1110	1101 1101	0101 1001	0000 1100
6-blok	1111 1110	1000 1101	0010 0110	0111 0011
7-blok	1100 1110	0100 1101	0111 0001	0010 0100
8-blok	1101 1110	1001 1101	0110 0101	0011 0000

9-blok	0010 1110	1010 1101	1010 0000	1111 0101
10-blok	0011 1110	0111 1101	1011 0100	1110 0001
11-blok	0000 1110	0011 1101	1000 1000	1101 1101
12-blok	0001 1110	0110 1101	1111 0111	1010 0010
13-blok	0110 1110	0101 1101	0011 0010	0110 0111
14-blok	0111 1110	1011 1101	1110 0011	1011 0110
15-blok	0100 1110	1111 1101	1101 1111	1000 1010
16-blok	0101 1110	0000 1101	0100 1101	0001 1000
(XOR)∑=	0000 0000	0000 0000	0000 0000	0000 0000

Kuzatish jarayonidan, algoritmdagi S akslantirish aktiv bo‘laklarni tarqatmasligi, shuningdek, delta to‘plamning balanslashganligiga ta’sir qilmasligi ma’lum bo‘ldi. L akslantirishi esa, ustundagi bitta aktiv bo‘lakni ikkita aktiv bo‘laklarga tarqatadi. X akslantirish ham balanslashganlikga ta’sir qilmaydi, shuningdek, aktiv bo‘lakni tarqatmaydi. Bu yerda *delta* to‘plamdagi aktiv bo‘laklarning balanslashganligiga va ularning soniga faqat L akslantirishlari ta’sir qilishini ko‘rish mumkin.

Xuddi shu tarzda, S-KN1 shifrlash algoritmining keyingi raundlari uchun ham *delta* to‘plamning o‘zgarishini kuzatib boramiz. Shunga ko‘ra, kuzatilayotgan to‘plamning shifrlash algoritmi 2-raundidan keyingi o‘zgarishi quyidagi 4.32-jadvalda keltirilgan.

4.32 –jadval

Kuzatilayotgan to‘plamning 2-raunddan keyingi o‘zgarishi

Aks-sh	**1-raund so‘ngidagi qiymat**	**2-raund**		
		S	**L**	**X**
1-blok	0101 1011	0000 1110	0001 1110	0011 0000
2-blok	1100 1001	0100 1100	0100 0000	0110 1110
3-blok	1001 1110	1100 1101	0001 1010	0011 0100
4-blok	0100 1111	1111 1000	0010 1010	0000 0100
5-blok	0000 1100	0011 0100	0000 0001	0010 1111
6-blok	0111 0011	1011 0111	0011 1001	0001 0111
7-blok	0010 0100	1010 1111	1100 0010	1110 1100
8-blok	0011 0000	0111 0011	1010 1010	1000 0100
9-blok	1111 0101	1000 0000	0110 1011	0100 0101
10-blok	1110 0001	1101 0110	1011 0010	1001 1100
11-blok	1101 1101	1001 1001	1010 0001	1000 1111
12-blok	1010 0010	0001 1010	1001 1001	1011 0111
13-blok	0110 0111	0101 1011	1001 0100	1011 1010

14-blok	1011 0110	1110 0101	0010 0100	0000 1010
15-blok	1000 1010	0010 0001	1011 0111	1001 1001
16-blok	0001 1000	0110 0010	1101 1000	1111 0110
(XOR)∑=	0000 0000	0000 0000	0000 0000	0000 0000

2-raunddan so‘ng ham delta to‘plam balanslashgan bo‘ladi.

Kuzatilayotgai to‘plamning shifrlash algoritmi 3-raundidan keyingi o‘zgarishi quyidagi 4.33- jadvalda keltirilgan.

4.33 –jadval

Kuzatilayotgan to‘plamning 3-raunddan keyingi o‘zgarishi

Aks-sh	**2-raund so‘ngidagi qiymat**	**3-raund**		
		S	**L**	**X**
1-blok	0011 0000	0111 0011	1010 1010	0011 0110
2-blok	0110 1110	0101 1101	0011 0010	1010 1110
3-blok	0011 0100	0111 1111	1101 0110	0100 1010
4-blok	0000 0100	0011 1111	1110 1010	0111 0110
5-blok	0010 1111	1010 1000	0101 0101	1100 1001
6-blok	0001 0111	0110 1011	0101 0001	1100 1101
7-blok	1110 1100	1101 0100	1101 0000	0100 1100
8-blok	1000 0100	0010 1111	1010 1001	0011 0101
9-blok	0100 0101	1111 0000	1001 0010	0000 1110
10-blok	1001 1100	1100 0100	1001 0011	0000 1111
11-blok	1000 1111	0010 1000	0011 1110	1010 0010
12-blok	1011 0111	1110 1011	0011 1010	1010 0110
13-blok	1011 1010	1110 0001	1110 0000	0111 1100
14-blok	0000 1010	0011 0001	1111 0100	0110 1000
15-blok	1001 1001	1100 1100	0010 1011	1011 0111
16-blok	1111 0110	1000 0101	1001 1110	0000 0010
(XOR)∑=	0000 0000	0011 1000	0111 1101	0111 1101

Demak, qaralayotgan shifrlash algoritmining 3-raund kirishida kuzatilayotgan to‘plamning balanslashgan elementi mavjud bo‘lib, bu hol shifrlash algoritmining 4-raundda foydalanilgan raund kalitini aniqlash imkoniyatini beradi. Kriptoanalizning 1-bosqichini ushbu qadamda to‘xtatish mumkin. Kriptoanalizning keyingi bosqichi kalit variantlarini aniqlash bo‘lib, ushbu jarayonda zarur hisoblangan 3 –raund so‘ngidagi shifr matn to‘plami ham ma’lum.

Kriptoanalizning keyingi jarayoni, ya’ni shifrlash algoritmining so‘ngi raundida foydalanilgan kalit qiymatni aniqlash, so‘ngi raundga kiruvchi to‘plamda aktiv (yoki passiv) bayt mavjudligini hamda so‘ngi raunddan chiquvchi ma’lumot (shifr matn) ni bilgan holda, statistika o‘tkazish yo‘li orqali amalga oshiriladi.

Integral kriptoanaliz mohiyatiga ko‘ra 3 raundli S-KN1 algoritmida so‘ngi raund kaliti qiymatni aniqlash quyidagicha amalga oshiriladi.

1. P_i (i = 0 dan 15 gacha) 16 ta matndan iborat to‘plamlar tanlab olinadi, ular faqat bir-biridan bitta yarim baytlik qismi bilan ajralib turadi.

2. Ushbu ochiq matnlarga mos shifr matnlar T_i hosil qilinadi.

3. Har bir qismdagi bo‘laklar uchun quyidagilar bajariladi:

I. 3-raund so‘ngida foydalanilgan kalit K_3ni topish uchun kalit bo‘laklarining mavjud bo‘lgan barcha $K_3^{'}$ (*0000* dan *1111* gacha) qiymatlari uchun quyidagilar bajariladi:

a) Barcha 16 ta T_i shifr matn uchun

$$R_3 = L^{-1}(S^{-1}(X(K_3^{'}, T_i))) \quad (4.25)$$

qiymat hisoblanadi. Bu 3-raunddagi 16 ta chiqishga mos keladi.

b) Barcha 16 ta R_3 qiymatlar uchun XOR amali bajariladi.

c) Agar XOR=0 bo‘lsa, K_3 ning kutilayotgan bo‘lagi to‘g‘ri topilgan. Aks holda noto‘g‘ri topilgan va uni K_3 bo‘lakning mumkin bo‘lgan qiymatlari ro‘yxatidan chiqarib yuborish kerak.

II. Bo‘laklarning barcha mavjud qiymatlaridan o‘tgandan so‘ng, bitta yoki bir nechta bo‘laklar qoladi, ushbu bo‘laklardan bittasi to‘g‘ri bo‘lakdir.

III. Kalitning to‘g‘ri bo‘lagini topish uchun 1, 2 va 3 qadamlarni boshqa ochiq to‘plami bilan qaytarish kerak. L^{-1}

Ushbu qadamlar ketma-ketligini bajarish jarayonida ko‘rish mumkinki, shifrmatnlar to‘plamini (2) ifodaga ko‘ra L^{-1} akslantirishdan o‘tkazish jarayoni va (3) ifodani hisoblash kalit variantlarini to‘liq tanlash usulidan effektiv emas. Lekin, algoritm akslantirishlarining xususiyatlaridan foydalanib effektiv natijaga erishish mumkin. Quyida L akslantirishining xossasidan foydalanib tuzilgan S-KN1 shifrlash algoritmining kalitini topish uchun effekti algoritm taklif qilingan. Algoritmning qadamlar ketma-ketligini keltirishdan avval soddalik uchun ayrim belgilashlarni kiritib olish maqsadga muvofiq.

a L akslantirishga kiruvchi massiv, *b* L akslantirishdan chiquvchi massiv, *k* so‘nggi raund chiqishida ishlatilgan kalit massivi bo‘lsin.

U holda

$$y = X(b) = X\big(L(a)\big) = L(a) \oplus k \qquad (4.26)$$

tenglik o‘rinli bo‘ladi.

$b = y \oplus k$ va $a = L^{-1}(b)$ ekanligidan, hamda L^{-1} akslantirishining chiziqlilik, ya’ni, $L^{-1}(b \oplus k) = L^{-1}(b) \oplus L^{-1}(k)$ xossasidan

$$a = L^{-1}(b) = L^{-1}(y \oplus k) = L^{-1}(y) \oplus L^{-1}(k) \qquad (4.27)$$

tenglik o‘rinli ekanligi kelib chiqadi.

4.27-tenglikdan esa $x = S^{-1}(a) = S^{-1}(L^{-1}(b)) = S^{-1}(L^{-1}(y \oplus k)) = S^{-1}(L^{-1}(y) \oplus L^{-1}(k))$ ekanligi kelib chiqadi. Demak, $\sum x$ ni hisoblash va uchinchi raund so‘ngida foydalanilgan kalitni topish imkoniyati mavjud.

Uch raundli S-KN1 algoritm uchun integral kriptoanaliz usulida kalitni topish algoritmi quyidagicha:

1. Bir bayti aktiv, qolgan baytlari passiv ochiq matnlar to‘plami tanlab olinsin;

2. To‘plamning barcha massivlari uchun 3 raundli shifrlash amalga oshirilsin;

3. Hosil bo‘lgan shifr matnlar to‘plamining barcha massivlari uchun $a = L^{-1}(y)$ qiymatlar hisoblansin;

4. k' $(k' = L^{-1}(k))$ ning qabul qilishi mumkin bo‘lgan barcha variantlari (0000 0000 dan 1111 1111 gacha) va x to‘plamning barcha $x_i = S^{-1}(a_i \oplus k_i')$ $(i = 0{,}1)$ elementlari uchun $\sum x_i = 0$ tenglik tekshirilsin;

5. Tenglikni qanoatlantiradigan variantlar tanlab olinsin va k' ning mos bayti sifatida qabul qilinsin;

6. Agar k' ning bir bayti yagona qiymat qabul qilmaguncha, 1-5 qadamlar qaytarilsin va har safar k' ning bir bayti uchun qabul qilingan variantlar bilan avval hosil qilingan variantlar kesishmasi olinsin.

7. $L(k')$ hisoblansin va uchinchi raund so‘ngida foydalanilgan kalit sifatida elon qilinsin.

Ushbu keltirilgan algoritm asosida, yuqorida ko‘rib chiqilgan misolda qo‘llanilgan kalitni topishni ko‘rib chiqamiz.

Yuqorida algoritm yordamida shifrlash jarayonini amalga oshirilganda keltirilgan algoritmning 1- va 2- qadamlari bajarilgan va quyidagi shifrmatnlar to‘plami hosil qilingan:

T0=0011 0110	T5=1100 1101
T1=1010 1110	T6=0100 1100
T2=0100 1010	T7=0011 0101
T3=0111 0110	T8=0000 1110
T4=1100 1001	T9=0000 1111

T10=1010 0010 T13=0110 1000
T11=1010 0110 T14=1011 0111
T12=0111 1100 T15=0000 0010

3-qadam bajarilgandan so‘ng, ya’ni $T_i(i=0,...,15)$ massivning barcha qiymatlari uchun $L^{-1}(T_i)$ hisoblangandan so‘ng, massiv qiymatlari ko‘rinishi quyidagicha bo‘ladi:

$U_0=L^{-1}(0011\ 0110)=0110\ 0011$
$U_1=L^{-1}(1010\ 1110)=1111\ 0011$
$U_2=L^{-1}(0100\ 1010)=1110\ 0110$
$U_3=L^{-1}(0111\ 0110)=0101\ 1111$
$U_4=L^{-1}(1100\ 1001)=1101\ 1110$
$U_5=L^{-1}(1100\ 1101)=0001\ 1010$
$U_6=L^{-1}(0100\ 1100)=0100\ 0000$
$U_7=L^{-1}(0011\ 0101)=0011\ 0000$
$U_8=L^{-1}(0000\ 1110)=0001\ 1110$
$U_9=L^{-1}(0000\ 1111)=0010\ 1111$
$U_{10}=L^{-1}(1010\ 0010)=1000\ 1111$
$U_{11}=L^{-1}(1010\ 0110)=0100\ 1011$
$U_{12}=L^{-1}(0111\ 1100)=1000\ 0101$
$U_{13}=L^{-1}(0110\ 1000)=0000\ 0010$
$U_{14}=L^{-1}(1011\ 0111)=0011\ 1001$
$U_{15}=L^{-1}(0000\ 0010)=0110\ 0010$

Algoritmning 4-qadamida bajariladigan hisoblashlar 4.34- va 4.35-jadvallarda keltirilgan.

Natijalardan ko‘rish mumkinki k' ning dastlabki yarim bayti uchun nomzod sifatida qabul qilingan variantlar to‘rttani (**0011, 1001, 1101 va 1111**), ikkinchi yarim bayt uchun nomzodlar esa ikkitani (**0011 va 1110**) tashkil qiladi. Shu sababli, nomzod kalitlar bittani tashkil qilmaguncha 6-qadamda ta’kidlanganidek yuqorida bajarilgan ketma-ketliklar boshqa ochiq matnlar to‘plami uchun ham takrorlanadi. Boshqa ochiq matn juftlari uchun takrorlanishlar natijasi 4.36- va 4.37- jadvallarda keltirilgan.

4.34-jadval

k' ning 1-qismini (yarim baytini) topish jarayoni

Yarim bayt shifr matn	**Mumkin bo‘lgan qism kalitlar to‘plami**															
	0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
	$S^{-1}(k_i' \oplus L^{-1}(T_j))$															
1111	1011	0100	1001	1110	0010	0111	1111	1101	0001	0011	1100	0110	1000	0000	0101	1010
0010	0101	1010	1000	0000	1100	0110	0001	0011	1111	1101	0010	0111	1001	1110	1011	0100
1100	1000	0000	0101	1010	0001	0011	1100	0110	0010	0111	1111	1101	1011	0100	1001	1110
1100	1000	0000	0101	1010	0001	0011	1100	0110	0010	0111	1111	1101	1011	0100	1001	1110
1111	0110	1100	0011	0001	1010	0101	0000	1000	1110	1001	0100	1011	1101	1111	0111	0010
1011	0001	0011	1100	0110	1000	0000	0101	1010	1011	0100	1001	1110	0010	0111	1111	1101
1111	1101	1111	0111	0010	1110	1001	0100	1011	1010	0101	0000	1000	0110	1100	0011	0001
0110	1000	0000	0101	1010	0001	0011	1100	0110	0010	0111	1111	1101	1011	0100	1001	1110
0100	1110	1001	0100	1011	1101	1111	0111	0010	0110	1100	0011	0001	1010	0101	0000	1000
1011	1101	1111	0111	0010	1110	1001	0100	1011	1010	0101	0000	1000	0110	1100	0011	0001
1110	0110	1100	0011	0001	1010	0101	0000	1000	1110	1001	0100	1011	1101	1111	0111	0010
0011	0001	0011	1100	0110	1000	0000	0101	1010	1011	0100	1001	1110	0010	0111	1111	1101
0101	1001	1110	1011	0100	1111	1101	0010	0111	1100	0110	0001	0011	0101	1010	1000	0000
0010	1001	1110	1011	0100	1111	1101	0010	0111	1100	0110	0001	0011	0101	1010	1000	0000
1000	1010	0101	0000	1000	0110	1100	0011	0001	1101	1111	0111	0010	1110	1001	0100	1011
1100	1111	1101	0010	0111	1001	1110	1011	0100	0101	1010	1000	0000	1100	0110	0001	0011
(XOR)∑=	**1101**	**1111**	**0010**	**0000**	**1101**	**1111**	**1101**	**1111**	**0010**	**0000**	**1101**	**1111**	**0010**	**0000**	**0010**	**0000**
k' ning birinchi yarim bayti uchun nomzodlar	**0011, 1001, 1101 ва 1111**															

4.35-jadval

k' ning 2-qismini (yarim baytini) topish jarayoni

Yarim bayt shifr matn	**Mumkin bo‘lgan qism kalitlar to‘plami**															
	0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
	$S^{-1}(k_i' \oplus L^{-1}(T_j))$															
1111	1101	1111	0111	0010	1110	1001	0100	1011	1010	0101	0000	1000	0110	1100	0011	0001
0010	0111	0010	1101	1111	0100	1011	1110	1001	0000	1000	1010	0101	0011	0001	0110	1100
1100	1101	1111	0111	0010	1110	1001	0100	1011	1010	0101	0000	1000	0110	1100	0011	0001
1100	1110	1001	0100	1011	1101	1111	0111	0010	0110	1100	0011	0001	1010	0101	0000	1000
1111	1100	0110	0001	0011	0101	1010	1000	0000	1001	1110	1011	0100	1111	1101	0010	0111
1011	1111	1101	0010	0111	1001	1110	1011	0100	0101	1010	1000	0000	1100	0110	0001	0011
1111	0000	1000	1010	0101	0011	0001	0110	1100	0111	0010	1101	1111	0100	1011	1110	1001
0110	1001	1110	1011	0100	1111	1101	0010	0111	1100	0110	0001	0011	0101	1010	1000	0000
0100	1010	0101	0000	1000	0110	1100	0011	0001	1101	1111	0111	0010	1110	1001	0100	1011
1011	1000	0000	0101	1010	0001	0011	1100	0110	0010	0111	1111	1101	1011	0100	1001	1110
1110	1001	1110	1011	0100	1111	1101	0010	0111	1100	0110	0001	0011	0101	1010	1000	0000
0011	0101	1010	1000	0000	1100	0110	0001	0011	1111	1101	0010	0111	1001	1110	1011	0100
0101	0101	1010	1000	0000	1100	0110	0001	0011	1111	1101	0010	0111	1001	1110	1011	0100
0010	1110	1001	0100	1011	1101	1111	0111	0010	0110	1100	0011	0001	1010	0101	0000	1000
1000	1000	0000	0101	1010	0001	0011	1100	0110	0010	0111	1111	1101	1011	0100	1001	1110
1100	0001	0011	1100	0110	1000	0000	0101	1010	1011	0100	1001	1110	0010	0111	1111	1101
(XOR)∑=	**1111**	**0111**	**1000**	**0000**	**0101**	**0010**	**1101**	**1010**	**1101**	**0101**	**1010**	**0010**	**1000**	**1111**	**0000**	**0111**
k' ning ikkinchi yarim bayti uchun nomzodlar	**0011 ва 1110**															

4.36-jadval

k' ning 1-qismini (yarim baytini) topish jarayoni

Yarim bayt shifr matn	**Mumkin bo‘lgan qism kalitlar to‘plami**															
	0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
	$S^{-1}(k_i' \oplus L^{-1}(T_j))$															
1111	0101	1010	1000	0000	1100	0110	0001	0011	1111	1101	0010	0111	1001	1110	1011	0100
0010	0010	0111	1111	1101	1011	0100	1001	1110	1000	0000	0101	1010	0001	0011	1100	0110
1100	0010	0111	1111	1101	1011	0100	1001	1110	1000	0000	0101	1010	0001	0011	1100	0110
1100	1010	0101	0000	1000	0110	1100	0011	0001	1101	1111	0111	0010	1110	1001	0100	1011
1111	0010	0111	1111	1101	1011	0100	1001	1110	1000	0000	0101	1010	0001	0011	1100	0110
1011	0111	0010	1101	1111	0100	1011	1110	1001	0000	1000	1010	0101	0011	0001	0110	1100
1111	0100	1011	1110	1001	0111	0010	1101	1111	0011	0001	0110	1100	0000	1000	1010	0101
0110	0000	1000	1010	0101	0011	0001	0110	1100	0111	0010	1101	1111	0100	1011	1110	1001
0100	0000	1000	1010	0101	0011	0001	0110	1100	0111	0010	1101	1111	0100	1011	1110	1001
1011	1010	0101	0000	1000	0110	1100	0011	0001	1101	1111	0111	0010	1110	1001	0100	1011
1110	1011	0100	1001	1110	0010	0111	1111	1101	0001	0011	1100	0110	1000	0000	0101	1010
0011	0011	0001	0110	1100	0000	1000	1010	0101	0100	1011	1110	1001	0111	0010	1101	1111
0101	1111	1101	0010	0111	1001	1110	1011	0100	0101	1010	1000	0000	1100	0110	0001	0011
0010	1110	1001	0100	1011	1101	1111	0111	0010	0110	1100	0011	0001	1010	0101	0000	1000
1000	1100	0110	0001	0011	0101	1010	1000	0000	1001	1110	1011	0100	1111	1101	0010	0111
1100	0100	1011	1110	1001	0111	0010	1101	1111	0011	0001	0110	1100	0000	1000	1010	0101
(XOR)∑=	0101	1000	0010	1111	0000	1101	0111	1010	1000	0101	1111	0010	1101	0000	1010	0111
k' ning birinchi yarim bayti uchun nomzodlar	**0100 ва 1101**															

4.37-jadval

k' ning 2-qismini (yarim baytini) topish jarayoni

Yarim bayt shifr matn	**Mumkin bo‘lgan qism kalitlar to‘plami**															
	0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
	$S^{-1}(k_i^{'} \oplus L^{-1}(T_j))$															
1111	1110	1001	0100	1011	1101	1111	0111	0010	0110	1100	0011	0001	1010	0101	0000	1000
0010	1110	1001	0100	1011	1101	1111	0111	0010	0110	1100	0011	0001	1010	0101	0000	1000
1100	1000	0000	0101	1010	0001	0011	1100	0110	0010	0111	1111	1101	1011	0100	1001	1110
1100	0110	1100	0011	0001	1010	0101	0000	1000	1110	1001	0100	1011	1101	1111	0111	0010
1111	0001	0011	1100	0110	1000	0000	0101	1010	1011	0100	1001	1110	0010	0111	1111	1101
1011	1111	1101	0010	0111	1001	1110	1011	0100	0101	1010	1000	0000	1100	0110	0001	0011
1111	1110	1001	0100	1011	1101	1111	0111	0010	0110	1100	0011	0001	1010	0101	0000	1000
0110	1110	1001	0100	1011	1101	1111	0111	0010	0110	1100	0011	0001	1010	0101	0000	1000
0100	0110	1100	0011	0001	1010	0101	0000	1000	1110	1001	0100	1011	1101	1111	0111	0010
1011	0010	0111	1111	1101	1011	0100	1001	1110	1000	0000	0101	1010	0001	0011	1100	0110
1110	1110	1001	0100	1011	1101	1111	0111	0010	0110	1100	0011	0001	1010	0101	0000	1000
0011	0000	1000	1010	0101	0011	0001	0110	1100	0111	0010	1101	1111	0100	1011	1110	1001
0101	0110	1100	0011	0001	1010	0101	0000	1000	1110	1001	0100	1011	1101	1111	0111	0010
0010	1000	0000	0101	1010	0001	0011	1100	0110	0010	0111	1111	1101	1011	0100	1001	1110
1000	0110	1100	0011	0001	1010	0101	0000	1000	1110	1001	0100	1011	1101	1111	0111	0010
1100	0010	0111	1111	1101	1011	0100	1001	1110	1000	0000	0101	1010	0001	0011	1100	0110
(XOR)∑=	0000	1111	0000	1111	1111	0000	1111	0000	1111	0000	1111	0000	0000	1111	0000	1111
$k^{'}$ ning ikkinchi yarim bayti uchun nomzodlar	**0000, 0010, 0101, 0111, 1001, 1011, 1100 ва 1110**															

Bu holatda tanlab olingan ochiq matnlar to‘plami ko‘rinishi quyida keltirilgan.

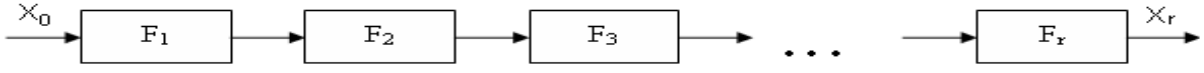
P_0= 0000 0001	P_8= 1000 0001
P_1= 0001 0001	P_9= 1001 0001
P_2= 0010 0001	P_{10}= 1010 0001
P_3= 0011 0001	P_{11}= 1011 0001
P_4= 0100 0001	P_{12}= 1100 0001
P_5= 0101 0001	P_{13}= 1101 0001
P_6= 0110 0001	P_{14}= 1110 0001
P_7= 0111 0001	P_{15}= 1111 0001

4.36- va 4.37- jadvallarda keltirilgan natijalardan ko‘rish mumkinki k' ning tastlabki yarim bayti uchun nomzod sifatida qabul qilingan variantlar ikkitani (**0100 va 1101**), ikkinchi yarim bayt uchun nomzodlar esa sakkiztani (**0000, 0010, 0101, 0111, 1001, 1011, 1100 va 1110**) tashkil qiladi.

Slaydli hujum kriptoanaliz usuli asosan Feystel tarmog‘iga asoslangan shifrlash algoritmlariga qaratilgan. Agar Feystel tarmog‘i bo‘yicha qurilgan shifrlash algoritmlarining kirishiga n bitli ma’lumot kelib tushadigan bo‘lsa, unda qism kalitning uzunligi $n/2$ bitni tashkil qiladi. Shu bois ham shifrlash algoritmida foydalanilgan maxfiy kalitning uzunligi $n/2$ ni tashkil etadi.

Quyida keltirilgan 4.10-rasmda n bitli x_0 ochiq matnni shifrlash jarayoni ko‘rsatilgan, uning natijasida x_r shifrmatn hosil bo‘ladi. Bu yerda x_j j-chi raundan keyingi berilganlarning oraliq qiymatini belgilaydi, $x_j = F_j(x_{j-1}, k_j)$, $j = 1,2,3,...,r$.

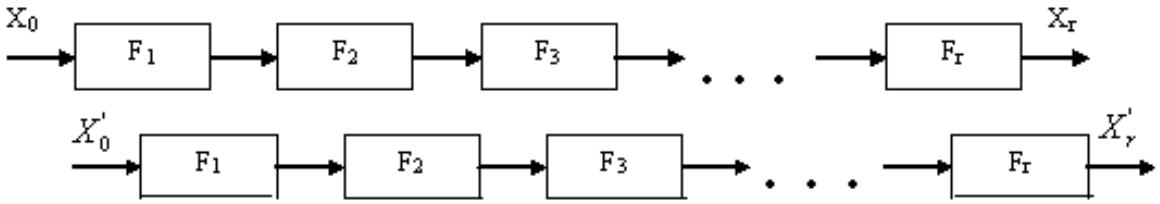
Keyinchalik, ba’zan F funksiyani belgilashda k qiymatni tushurib qoldiramiz $F(x,k)$ yoki $F_j(x,k)$ o‘rniga $F(x)$ yoki $F_j(x)$ deb yozish mumkin.



4.10 - rasm. Oddiy blokli shifrlash algoritmi sxemasi

Ta’rif. F funksiya “kuchsiz” deb ataladi, agar ma’lum $F(x_1,k) = y_1$ va $F(x_2,k) = y_2$ ikki tenglikda k kalitni aniqlash oson bo‘lsa.

Quyidagi 4.11- rasmda bunday turdagi shifrlash algoritmlari uchun slaydli hujumni qo‘llanilishi mumkinligi ko‘rsatilgan.



4.11- rasm. Oddiy slaydli hujum sxemasi

Slaydli hujum usulining g‘oyasi shundaki, jarayonlardan birini ikkinchisidan bir raundga kechiktirib, ikkita shifrlash jarayonini o‘zaro mos qo‘yish asos qilib olinadi. Shunday qilib, jarayonlardan biri ikkinchisidan bir raundga ortda qoladi.

Aytaylik, x_0 va $x_0^{'}$ boshlang‘ich ochiq matnlar va ularning mos ketma-ketliklari $x_j = F_j(x_{j-1})$ va $x_j^{'} = F_j(x_{j-1}^{'}), j = 1,...,r$ berilgan bo‘lsin.

2. *Tasdiq*. Agar $x_1 = x_0^{'}$ qiymatlar juftligiga ega bo‘linsa, u holda ularga mos $x_r = x_{r-1}^{'}$ qiymatlar juftligiga ham ega bo‘linadi.

Aytaylik, $(P, P^{'})$ - ochiq matnlar, $(C, C^{'})$ - esa ularga mos shifrmatnlar berilgan bo‘lsin.

Ta’rif. (P, C) *va* $(\mathrm{P}^{'}, C^{'})$ juftlik slayd juftlik deyiladi, agar quyidagi shartlar bajarilsa:

– $F(P) = C$, $F(P^{'}) = C^{'}$
– $C = P^{'}$
– $F(P) = P^{'}$, $F(C) = C^{'}$

Agar P ochiq matn F funksiyadan o‘tkazilgandan keyingi natijasi C shifrmatnga , $P^{'}$ ochiq matn F funksiyadan o‘tkazilgandan keyingi natijasi $C^{'}$, hamda birinchi ochiq matnni shifrlash natijasi, ya’ni C shifrmatn, ikkinchi ochiq matn $P^{'}$ ga, ya’ni $C = P^{'}$ teng bo‘lsa, u holda $F(P) = P^{'}$, $F(C) = C^{'}$ bo‘ladi.

Slaydli hujum kriptoanaliz usuli quyidagi tarzda amalga oshiriladi.

$2^{n/2}$ juft (P_i, C_i) ochiq-yopiq matnlar juftligini olanadi va ularning orasidan slaydli juftliklar qidiriladi. Topilgan ochiq-yopiq matnlar orasidan “Tug‘ilgan kunlar” paradoksiga ko‘ra hech bo‘lmaganda bir juft shunday $(i, i^{'})$ indekslar topiladiki, qandaydir qism kalit uchun $F(P_i) = P^{'}{}_i$ va $F(C_i) = C^{'}{}_i$ tengliklar bir vaqtda bajariladi. Slaydli juftlik topilgandan

so‘ng, qism kalitning ma’lum bir bitlarini topish mumkin.

Maxfiy kalitning qolgan bitlarini topish uchun keyingi slaydli juftlikni aniqlash va u yordamida tahlil o‘tkazish kerak bo‘ladi. Shunday qilib, maxfiy kalitning bitlarini to‘la aniqlash uchun bir nechta slaydli juftliklarni aniqlash yetarli bo‘ladi. Bu esa kriptotahlilchi oldida turgan murakkab masala hisoblanadi.

Boshlang‘ich berilganlar 4.17-4.20 jadvallarda keltirilgan, ular tahlil qilinayotgan shifrlash algoritmida qo‘llaniladigan kengaytirishli o‘rin almashtirish jadvali, oddiy o‘rin almashtirish va almashtirish jadvalini tashkil etadi. Shuningdek, samarali hujum amalga oshirish uchun slaydli juftlikni aniqlashga yordam beruvchi maska (niqob) jadvali ham berilgan.

4.17-jadval

Kengaytirishli o‘rin almashtirish jadvali

3	1	4	3	2	1	4	2

4.18-jadval

O‘rin almashtirish jadvali

4	2	3	1

4.18-jadval

S1 -blok

	00	01	10	11
00	0	2	1	1
01	1	3	0	2
10	0	3	2	3
11	2	1	3	0

4.19-jadval

S2 -blok

	00	01	10	11
00	0	1	3	2
01	3	2	0	1
10	1	0	1	3
11	3	2	0	2

4.20-jadval

Maska

1	0	1	0

S-DES o‘quv algoritmi Feystel tarmog‘i bo‘yicha qurilgan blokli shifrlash algoritmi bo‘lganligi uchun unga slaydli hujum kriptoanaliz

usulini qo‘llash mumkin. Ishni soddalashtirish maqsadida bir xil fiksirlangan 8 bitli K kalitdan foydalaniladi (ya’ni 10 bitli boshlang‘ich kalitdan 8 bitli qism kalitni ajratib olish protsedurasini tushurib qoldiramiz). Boshlang‘ich va yakuniy almashtirishlar tashlab o‘tiladi, chunki ular algoritmning kriptobardoshligiga ta’sir etmaydi. Shuningdek, almashtirishning 2 raundidan emas 20 ta raunddan foydalaniladi, chunki kriptoanalizning bunday ko‘rinishi algoritmda foydalaniladigan raundlar soniga bog‘liq emas.

Mazkur kriptoanaliz usulini o‘tkazish uchun quyidagidalar kerak bo‘ladi:

– $(X, X^{'})$ -ochiq matnlar juftligi;

– $(Y, Y^{'})$ -shifrmatnlar juftligi;

Yuqorida tanlangan maskani kiritib slaydli juftlik ta’rifiga mos keluvchi matnlar juftligi tanlab olinadi. Maska mumkin bo‘lgan slaydli juftliklar oralig‘ini siqib ishni yengillashtirish uchun kiritiladi. Bu shunday matnlar juftliklari bo‘ladiki, birinchi ochiq matnning o‘ngdagi 4 biti ikkinchi ochiq matning chapdagi 4 bitiga teng bo‘ladi, ular esa maskaga teng. Birinchi shifrmatnning chapdagi 4 biti ikkinchi shifrmatning o‘ngdagi 4 bitiga teng.

Quyidagi 4.21-jadvalda 5 juft slaydli juftlik keltirilgan:

4.21-jadval

Slayd juftliklar

№	X’	Y’	X	Y
1	10001010	10111000	10101000	10111011
2	10011010	10011010	10101001	11011001
3	10111010	10111010	10101000	10111011
4	11111010	10011111	10101001	11011001
5	11111010	10011111	10101111	10001001

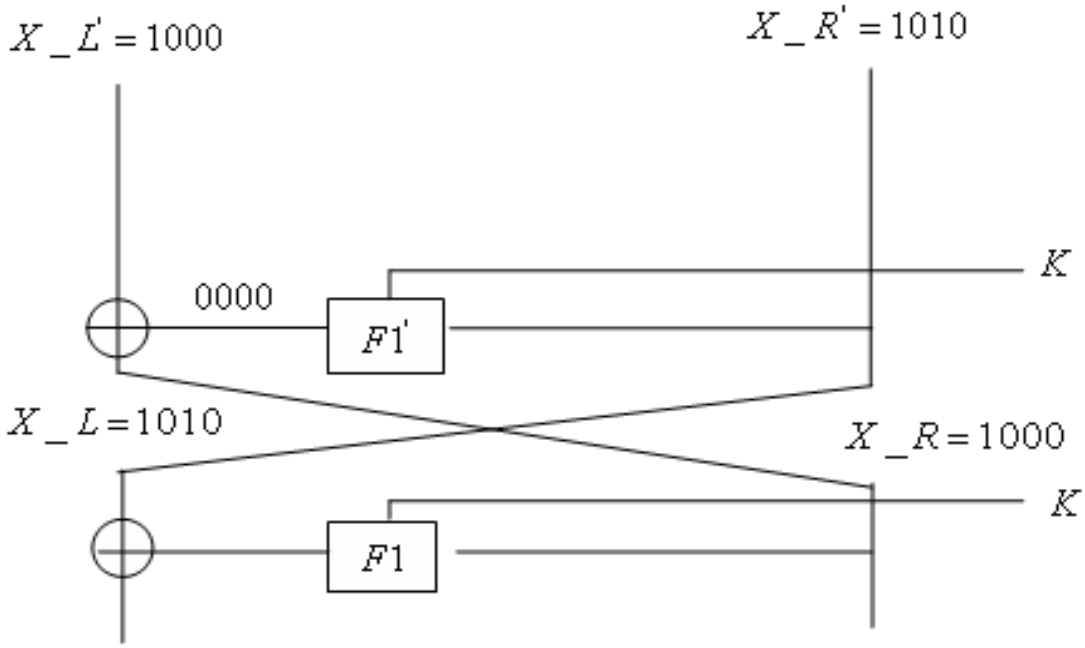
Topilgan juftliklar tahlilida shifrlash algoritmida foydalanilgan almashtirish jadvali bilan ishlashga to‘g‘ri kelganligi sababli ishni yengillashtirish uchun 4.22-jadvalda ko‘rsatilganidek, almashtirish bloklarining kirish va chiqishi taqqoslanadi:

4.22-jadval

S blok kirishi	**S_1 blok chiqishi**	**S_2 blok chiqishi**
0000	00	00
0001	01	11
0010	10	01

S blok kirishi	S_1 blok chiqishi	S_2 blok chiqishi
0011	11	10
0100	01	11
0101	00	00
0110	01	01
0111	10	01
1000	00	01
1001	10	11
1010	11	00
1011	10	00
1100	10	01
1101	11	00
1110	11	11
1111	00	10

Matnning birinchi juftini ko‘rib chiqamiz. Buning uchun, 4.12-rasmda ko‘rsatilgan juftlikning birinchi ikki raundini ko‘rib chiqamiz.



4.12-rasm. Birinchi raund birinchi slaydli juftlik tahlili

Birinchi X_R' ochiq matning o‘ng qismi qiymatlari va ikkinchi ochiq matning chap X_L qism qiymatlari ma’lum bo‘lgani F_1' funksiya kirishi haqida ma’lumot beradi. X_R va X_L' qiymatlar ham ma’lum bo‘lgani uchun F_1 funksiya chiqish qiymatini aniqlash mumkin, u 0000_2 teng

bo‘ladi.

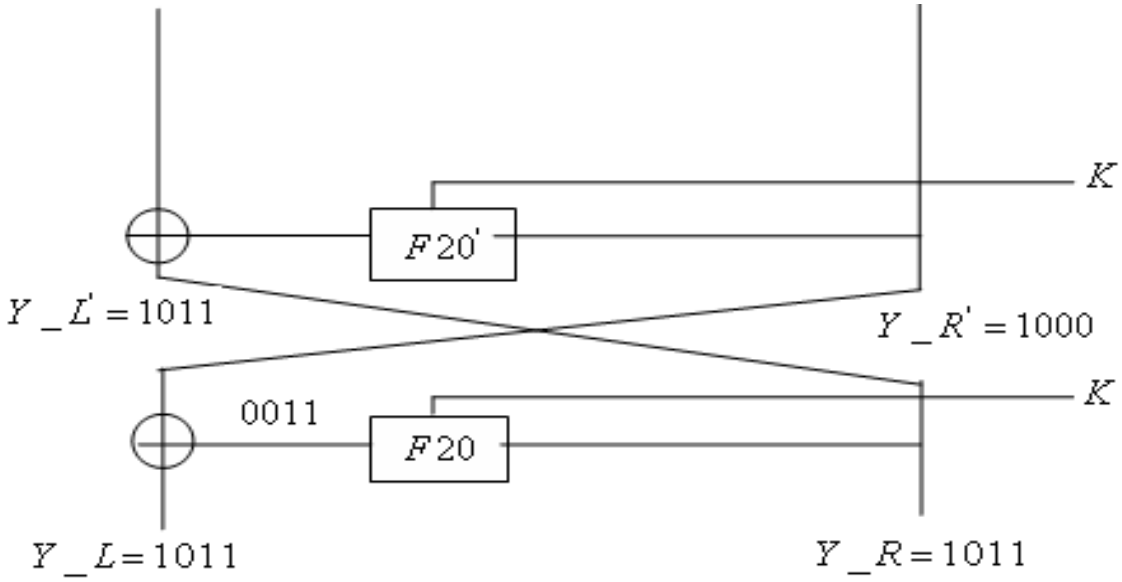
Berilganlar $F_1^{'}$ funksiyadan chiqishdan oldin 4.22-jadvalga muvofiq o‘rin almashsa, bir qadam ortga qaytib, S blok chiqishida 0000_2 qiymat paydo bo‘lishini topamiz, ya’ni 00_2 S_1 blok chiqishi, 00_2 esa S_2 blok chiqishi.

$F_1^{'}$ funksiyaga kiruvchi xabar 4.17-jadvalga muvofiq kengaytirishli o‘rin almashtirishga uchraydi. Demak, 1010_2 kirish 11010100_2 qiymatga o‘zgaradi. Bu esa $K=(k_1,k_2)$ kalitga qo‘shiladi. Shifrlash jarayonida matn ikkita bo‘lakka ajratilib har bir bo‘lagi kalit qismi bilan qo‘shilib keyin esa mos S blok kirishiga kelib tushadi. Biz 8 bitli maxfiy kalitni ikkita k_1 *va* k_2 4 bitli qism kalitlar yig‘indisi sifatida keltiramiz, ya’ni S_1 blokning $1101\oplus k_1$ kirishi chiqishda 00_2 qiymat beradi. S_2 blokning $0100\oplus k_2$ kirishi esa chiqishda 00_2 qiymat beradi.

Yuqoridagi 4.22-jadvaldan foydalanib, aniqlash mumkinki, 00_2 qiymat S_1 blokning chiqishida hosil bo‘ladi, qachonki kirishga quyidagi $0000_2,0101_2,1000_2$ yoki 1111_2 qiymatlardan biri kirgan bo‘lsa. Shunday qilib, har bir kirishi mumkin bo‘lgan qiymatga 1101_2 ni qo‘shib, k_1 kalitning mumkin bo‘lgan qiymatlarini topamiz. Bular $1101_2,1000_2,0101_2$ yoki 0010_2 qiymatlar bo‘ladi.

Xuddi shu tarzda 00_2 qiymat S_2 blok chiqishida paydo bo‘ladi, qachonki kirishga quyidagi $0000_2,0101_2,1010_2$ yoki 1101_2 qiymatlar kelib tushsa. Demak, har bir kirishi mumkin bo‘lgan qiymatiga 0100_2 ni qo‘shib, k_2 ning mumkin bo‘lgan qiymatlarini olamiz. Bular $0100_2,0001_2,1110_2$ yoki 1001_2 qiymatlar bo‘ladi.

Endi shu slaydli juftlik uchun shifrlashning so‘nggi ikki raundini



ko‘rib chiqamiz.

4.13-rasm. So‘nggi raund birinchi slaydli juftlik tahlili

Birinchi shifrmatn Y_L' chap qismi va ikkinchi shifrmatnning Y_R o‘ng qismi qiymatlarining ma’lumligi F_{20}' funksiyaning kirish qiymati haqida ma’lumot beradi. Y_R' va Y_L qiymatlar ham ma’lum bo‘lgani uchun, F_{20} chiqish qiymatini aniqlash mumkin, u 0011_2 ga teng bo‘ladi.

Berilganlar F_{20}' funksiyadan chiqishdan oldin 4.22-jadvalga muvofiq o‘rin almashsa, bir qadam ortga qaytib, S blok chiqishida 0011_2 qiymat paydo bo‘lishini topamiz, ya’ni 00_2 S_1 blok chiqishi, 11_2 esa S_2 blok chiqishi.

F_{20} funksiyaga kiruvchi xabar 4.17-jadvalga muvofiq kengaytirishli o‘rin almashtirishga uchraydi. Demak, 1011_2 kirish 11110110_2 qiymatga o‘zgaradi. Bu esa $K=(k_1,k_2)$ kalitga qo‘shiladi. Shifrlash jarayonida matn ikkita bo‘lakka ajratib, xar bir bo‘lagi kalit qismi bilan qo‘shilib, keyin esa mos S blok kirishiga kelib tushadi. Biz 8 bitli maxfiy kalitni ikkita k_1, *ва* k_2 4 bitli qism kalitlar yig‘indisi sifatida keltiramiz, ya’ni S_1 blokning $1111\oplus k_1$ kirish chiqishda 10_2 qiymat beradi. S_2 blokning $0110\oplus k_2$ kirishi esa chiqishda 10_2 qiymat beradi.

Yuqorida berilgan 4.22-jadvaldan foydalanib, 10_2 qiymat S_1 blokning chiqishida hosil bo‘ladi, qachonki kirishga quyidagi $0010_2,0111_2,1001_2$ yoki 1100_2 qiymatlardan biri kirgan bo‘lsa. Shunday qilib, har bir kirishi mumkin bo‘lgan qiymatga 1111_2 ni qo‘shib, k_1 kalitning mumkin bo‘lgan qiymatlarini topamiz. Bular $1101_2,1000_2,0110_2$ yoki 0011_2 qiymatlar bo‘ladi.

Xuddi shu tarzda aniqlash mumkinki 10_2 qiymat S_2 blok chiqishida paydo bo‘ladi, qachonki kirishga quyidagi $0011_2,0110_2,1011_2$ yoki 1111_2 qiymatlar kelib tushsa. Demak, har bir kirishi mumkin bo‘lgan qiymatiga 0110_2 ni qo‘shib, k_2 ning mumkin bo‘lgan qiymatlarini olamiz. Bular $0101_2,0000_2,1101_2$ yoki 1001_2 qiymatlar bo‘ladi.

Shifrlashning barcha raundlarida bir xil kalit ishlatilgani uchun birinchi raundning k_1 qiymati so‘nggi raundning k_1 qiymatiga mos kelishi va birinchi raundning k_1 kalitiga mos kelishi kerak. Keyin k_1,k_2 ning barcha mumkin bo‘lgan qiymatlarini taqqoslab shuni ko‘rishimiz mumkinki, faqat ikkita $k_1=1101_2$ va $k_1=1000_2$ qiymati mavjud, ularni birinchi raundda ham so‘nggi raunda ham qo‘llash mumkin va bitta

$k_2 = 1001_2$ qiymati mavjud. Buni ham birinchi va so‘nggi raundda qo‘llash mumkin. Shunday qilib, qidirilayotgan kalitning ikkita mumkin bo‘lgan qiymati topildi, $K = 11011001_2$ va $K = 10001001_2$.

Yuqorida K maxfiy kalitning qiymati berilganligi bois olingan ikkita variant bilan taqqoslash natijasida olingan ikkinchisi haqiqiy K maxfiy kalit ekanligi ma’lum bo‘ldi.

Amaliy bajarish uchun vazifalar.

1. Simmetrik blokli shifrlash algoritmlari uchun algebraik kriptotahlilni amalga oshirish
2. Simmetrik blokli shifrlash algoritmlari uchun integral kriptotahlilni amalga oshirish
3. Simmetrik blokli shifrlash algoritmlari uchun slaydli hujum kriptotahlilini amalga oshirish

Adabiyot va Internet saytlar:

1. Шеннон К. Теория и связи в секретных системах. Работы по теории информации и кибернетике. – М.: Иностранная лит. 1963. – 243 б.
2. Авдошин С.М., Савельева А.А. «Криптоанализ: вчера, сегодня, завтра», Государственный университет – Высшая Школа Экономики. Москва – 2007.
3. Авдошин С.М., Савельева А.А. «Криптоанализ: савременное состояние и перспективы развития», Государственный университет – Высшая Школа Экономики.

4-amaliy ish. Asimmetrik kriptotizimlarni kriptotahlil qilish usullari. Faktorlash va diskret logorifmlash muammosining murakkabligiga asoslangan kriptotizimlarning bardoshliligi (2 soat)

Amaliy ishning maqsadi – *Faktorlash va diskret logorifmlash muammosining murakkabligiga asoslangan kriptotizimlarning bardoshliligini baholash bo‘yicha bilim va ko‘nikmasiga ega bo‘lish.*

Nazariy qism

Faktorizatsiyalash muammosini bartaraf etuvchi eksponensial algoritmlar bo'lib, ularning murakkabligi eksponent ravishda kirish parametrlarining uzunligiga bog'liq. Ya’ni tub ko’paytuvchilarga ajratilayotgan N sonining ikkilik ko'rinishdagi uzunligiga bog’liq.

Murakkablik darajasi $O\left(\sqrt{\mathrm{n}}\log n\right)$ yoki $O\left(\sqrt{\mathrm{n}}\, log^2\, n\right)$. Bu yerda hisoblash murakkabligi o’rtacha olganda n soni uchun taxminan $\sqrt{\mathrm{n}}\log n$ ta yoki $\sqrt{\mathrm{n}}\, log^2\, n$ ta amal bajarish nazarda tutilgan. Faktorizatsiya qilinadigan n sonni ketma-ket bo'lishdan iborat bo'lgan eng oddiy va eng aniq faktorizatsiya algoritmlaridan biri bu 2 dan $\sqrt{\mathrm{n}}$ gacha natural sonlarga bo’lib ko’rish hisoblanadi. Rasmiy ravishda, bu oraliqda faqat tub sonlarga bo'lish kifoya, ammo buning uchun bu oraliqdagi tub sonlar to'plamini bilish kerak. Amalda tub sonlar jadvali tuziladi va kichik sonlar

tekshiriladi. Masalan 2^{16} gacha bo'lgan sonlar. Juda katta sonlar uchun hisoblash tezligi pasayishiga olib kelganligi sababli bu algoritmlardan keng foydalanish tavsiya etilmaydi.

Faktorizatsiyalash muammosini bartaraf etuvchi eksponensial turdagi algoritmlarga quyidagilar kiradi:

- Fermaning faktorizatsiya usuli
- Pollardning ρ- algoritmi
- Pollard-Shtrassen algoritmi
- Shanksning kvadratik shakl usuli
- Pollardning P-1 algoritmi
- Leman usuli

Fermaning faktorizatsiya usuli: 1643-yil Per de Ferma tomonidan taklif qilingan bu usul quyidagi teoremaga asoslangan bo'lib, u tub ko'paytuvchilarga ajratish algoritmini ifodalaydi hamda berilgan sonning tub ekanligini aniqlash imkonini beradi.

Teorema. Aytaylik, n >1 toq son bo'lsin. Bu son murakkab son bo'ladi faqat va faqat ikkita ixtiyoriy p va q sonlari uchun □ p, q □ +Z bo'lib, n = $p^2 - q^2$ = (p - q) * (p + q) bo'lsa. Bu yerda p - q > 1.

Ferma usulining mohiyati shundan iboratki, teorema natijasiga ko'ra ixtiyoriy p va q musbat butun sonlar topish kerakki, $n = p^2 - q^2$; $p^2 = n + q^2$ yoki $q^2 = p^2 - n$ bajarilsin. Agar $p^2 = n + q^2$, q = 1, 2, 3 va hokazo qiymatlar uchun $n + q^2$- son biror sonning to'la kvadratidan iborat bo'lmasa, u xolda q = $\frac{n-1}{2}$ qiymat uchun n + q^2 - ni tekshirib ko'riladi va agar u biror sonning kvadratidan iborat bo'lsa. U holda n – tub son bo'ladi. Aks holatda n soni murakkab son deb topiladi va n = (p – q) ∗ (p + q) kabi ko'paytuvchilarga ajraladi deb hisoblanadi.

Misol uchun n = 551 soni uchun quyidagicha hisoblashlar amalga oshiriladi:

n = $p^2 - q^2$ deb tasavvur qilamiz va q ning 1, 2, 3, va hokazo qiymatlari uchun $p^2 = n + q^2$ tenglik o'rinli bo'lish yoki bo'lmasligini tekshirib ko'ramiz.

q = 1 da $p^2 = n + q^2$ → $p^2 = 551 + 1$ → $p^2 = 552$ o'rinli emas.

q = 2 da $p^2 = n + q^2$ → $p^2 = 551 + 4$ → $p^2 = 555$ o'rinli emas.

q = 3 da $p^2 = n + q^2$ → $p^2 = 551 + 9$ → $p^2 = 560$ o'rinli emas.

q = 4 da $p^2 = n + q^2$ → $p^2 = 551 + 16$ → $p^2 = 567$ o'rinli emas.

q = 5 da $p^2 = n + q^2$ → $p^2 = 551 + 25$ → $p^2 = 576$ → p = 24

o'rinli.

U holda n = $p^2 - q^2$ → 551 = $24^2 - 5^2$ → 551 = (24 – 5) * (24 + 5) → 551 = 19 * 29 kabi ko'paytuvchilarga ajralar ekan.

Misol uchun n = 293 soni uchun quyidagicha hisoblashlar amalga oshiriladi:

n = $p^2 - q^2$ deb tasavvur qilamiz va q ning 1, 2, 3, va hokazo qiymatlari uchun $p^2 = n + q^2$ tenglik o'rinli bo'lish yoki bo'lmasligini tekshirib ko'ramiz.

q = 1 da $p^2 = n + q^2$ ➔ $p^2 = 293 + 1$ ➔ $p^2 = 294$ o'rinli emas.

q = 2 da $p^2 = n + q^2$ ➔ $p^2 = 293 + 4$ ➔ $p^2 = 297$ o'rinli emas.

q = 3 da $p^2 = n + q^2$ ➔ $p^2 = 293 + 9$ ➔ $p^2 = 302$ o'rinli emas.

q = 4 da $p^2 = n + q^2$ ➔ $p^2 = 293 + 16$ ➔ $p^2 = 309$ o'rinli emas.

q = 5 da $p^2 = n + q^2$ ➔ $p^2 = 293 + 25$ ➔ $p^2 = 318$ o'rinli emas.

q = 6 da $p^2 = n + q^2$ ➔ $p^2 = 293 + 36$ ➔ $p^2 = 329$ o'rinli emas.

q = 7 da $p^2 = n + q^2$ ➔ $p^2 = 293 + 49$ ➔ $p^2 = 342$ o'rinli emas.

q = 8 da $p^2 = n + q^2$ ➔ $p^2 = 293 + 64$ ➔ $p^2 = 357$ o'rinli emas.

q = 9 da $p^2 = n + q^2$ ➔ $p^2 = 293 + 81$ ➔ $p^2 = 374$ o'rinli emas.

q = 10 da $p^2 = n + q^2$ ➔ $p^2 = 293 + 100$ ➔ $p^2 = 393$ o'rinli emas.

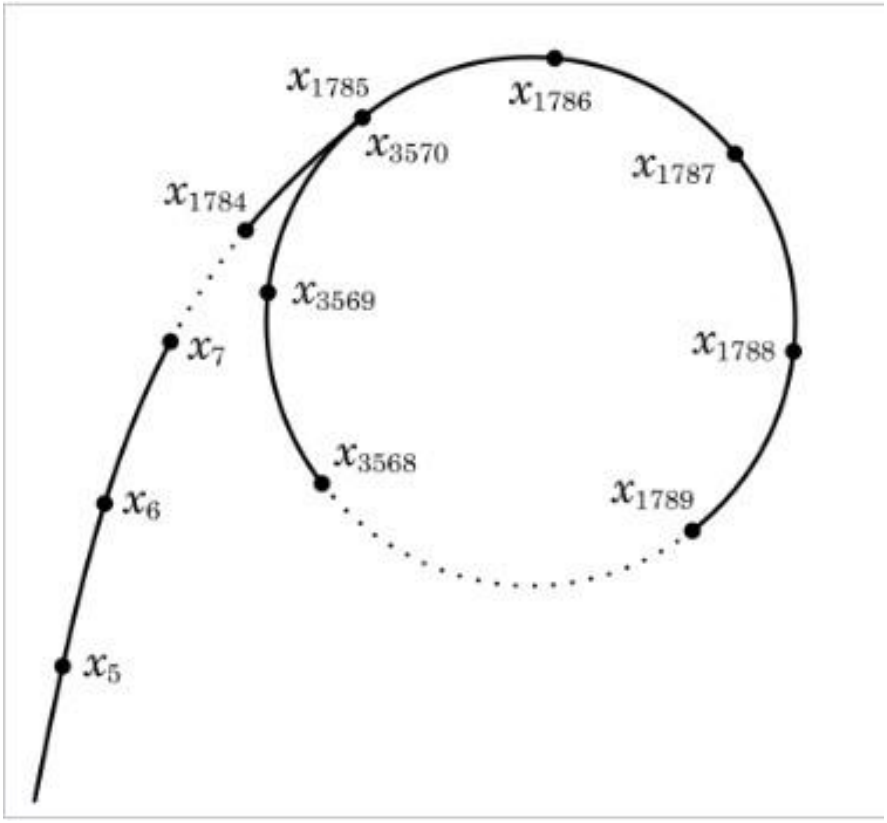
q = 11 da $p^2 = n + q^2$ ➔ $p^2 = 293 + 121$ ➔ $p^2 = 414$ o'rinli emas.

q = 12 da $p^2 = n + q^2$ ➔ $p^2 = 293 + 144$ ➔ $p^2 = 437$ o'rinli emas. ... va hokazolar uchun davom etadi. Bu kabi tekshiruvlar $q = \frac{n-1}{2}$ gacha davom etadi. Agar shu holatgacha shart o'rinli bo'lmasa u holda n soni tub son deb topiladi. Hozirgi holat uchun $q = \frac{293-1}{2} = 146$ ga qadar tekshirish amalga oshiriladi. Hech bir q ning qiymatida shart qanoatlantirmadi. U holda n = 293 soni tub son ekan.

Fermaning faktorizatsiya usuli tub sonlarga ketma-ket bo'lish usuli singari ko'p sonlarni faktorizatsiyalash uchun amalda qo'llanilmaydi, chunki u ham eksponensial murakkablikka asoslangan hisoblash tezligiga ega. Usul bo'lish amalisiz, faqat qo'shish, ayirish va kvadratga ko'tarish amallari bilan amalga oshiriladi. Agar, p va q sonlarkattaligi jihatidan unchalik farq qilmaydigan sonlar bo'lsa, Fermaning faktorizatsiya usuli n sonini yetarlicha tez muddatda ko'paytuvchilarga ajratadi.

Pollardning ρ - algoritmi: Ro-algoritm (ρ – algoritm). 1975-yilda Jon Pollard tomonidan taklif qilingan algoritm bo'lib, u sonni tub ko'paytuvchilarga ajratish uchun xizmat qiladi. Ushbu algoritm Floydning takrorlanuvchi funksiya ketma-ketlikdagi sikl uzunligini va tug'ilgan kun paradoksining ba'zi oqibatlarini topish algoritmiga asoslangan. Kengayishda etarlicha kichik omillarga ega kompozit sonlarni tub ko'paytuvchilarga ajratishda ushbu algoritm eng samarali hisoblanadi. Algoritmning murakkabligi quyidagicha baholanadi: $O(N^{\frac{1}{4}})$.

Pollardning ρ -algoritmi raqamlar ketma-ketligini quradi, uning elementlari ba'zi bir n sonidan boshlab siklni tashkil qiladi, buni algoritmlar oilasining nomi bo'lgan yunoncha ρ harfi ko'rinishidagi raqamlarning joylashishi bilan tasvirlash mumkin(2.1-rasm).



2.1-rasm. Raqamli ketma-ketlik takrorlanishi davomida yunoncha ρ harfiga o'xshab qoladi.

Algoritmning quyidagi ketma-ketlik asosida ishlaydi:

Hisoblash uncha qiyin bo'lmagan $F(x) = (x^k \pm a) \bmod N$ ga o'xshagan funksiya olinadi. Bunda e'tiborli jihati bu funksiya chiziqli bo'lmasligi va ozod hadi a toq son bo'lishi talab etiladi. Argumentning darajasi k esa $N \equiv 1 \bmod k$ shartni qanoatlantirishi lozim. Umumiy holatda k=2 qiymat deyarli barcha tub sonlarda yuqoridagi shartni yetarli darajada qanoatlantiradi.

1. F(x) = (x2 + 1)mod N funksiya olamiz.
2. x0 = 2, va y0 = 2 boshlang'ich qiymatlar olinadi.
3. Har bir i qadam uchun xi = F(xi − 1) va yi = F(F(yi − 1)) qiymatlar hisoblab topiladi.
4. d = EKUB(abs(yi − xi), N), abs(yi − xi) va N sonlarining EKUBi hisoblab topiladi.
5. Agar $d \neq 1$ bo'lsa, N soni d ga qoldiqsiz bo'linadi va d soni N sonining bo'luvchilaridan biri deb hisoblanadi. Bunda yana shuni aytib o'tish lozimki, N sonining bo'luvchilari orasida bir nechta d soni mavjud bo'lishi mumkin shuning uchun N = N / d amal bajariladi toki, $N \neq 0 \bmod(d)$ shart o'rinli bo'lgunga qadar. Agar d =1 bo'lsa, i = i + 1 hisoblanib keyingi qadamga o'tiladi.
6. Hosil bo'lgan N sonini tublikka tekshiramiz. Agar tub bo'lsa, algoritm to'xtaydi, aks holda i = i + 1 hisoblanib keyingi qadamga o'tiladi.

Bunda 1 dan farqli d sonlari va N sonining oxirgi qiymati faktorizatsiya qilinayotgan sonning tub ko'paytuvchilari deb topiladi.

Misol uchun N = 1247 sonini Pollardning ρ -algoritmi yordamida hisoblab ko'ramiz.

N = 1247, F(x) = (x2 + 1)modN, $x_0 = 2$, $y_0 = 2$,				
i	xi = F(xi − 1)	yi = F(F(yi − 1))	|yi − xi|	EKUB(|yi − xi|,N)
1	5	26	21	1
2	26	681	655	1
3	677	1168	491	1
4	681	50	631	1
5	1125	50	1075	43

d = 43 soni topildi u holda N = N / d = 1247 / 43 = 29. 29 soni tub bo'lganligi sababli ishni to'xtatamiz. N soni 1247 = 43 * 29 shaklida ko'paytuvchilarga ajratilar ekan.

Misol uchun N = 5459 sonini Pollardning ρ -algoritmi yordamida hisoblab ko'ramiz.

N = 1247, F(x) = (x2 + 1)modN, x0 = 2, y0 = 2,				
i	xi = F(xi − 1)	yi = F(F(yi − 1))	|yi − xi|	EKUB(|yi − xi|, N)
1	5	26	21	1
2	26	5233	5207	1
3	677	3830	3153	1
4	5233	544	4689	1
5	1946	3724	1778	1
6	3830	2293	1537	53

d = 53 soni topildi u holda N = N / d = 5459 / 53 = 103. 103 soni tub bo'lganligi sababli ishni to'xtatamiz. N soni 5459 = 53 * 103 shaklida ko'paytuvchilarga ajratilar ekan.

Pollardning ρ -algoritmi katta vaqt va xarajatga ega bo'lishi sababli, katta sonlar uchun samarali emas. Shunga qaramay, kichik va o'rta miqdordagi sonlarni tub ko'paytuvchilarga ajratish uchun yaxshi samaradorlikka ega bo'lib, boshqa eksponensial algoritmlarga nisbatan ancha ko'proq samarali hisoblanadi.

Pollard-Strassen algoritmi. Bu, faktorizatsiyalash algoritmi bo'lib, algoritmda Pollardning ρ - algoritmi va Strassen metodi kombinatsiyasi qo'llaniladi. Bu algoritmda, sonning ikki ko'paytuvchilarini topish uchun ancha aqlli, effektiv va samarador usul ishlatiladi. Pollard-Strassen algoritmi sonlarni faktorizatsiya qilishda qo'llaniladi. U quyidagi ketma-ketlik bo'yicha ishlaydi:

1. Kirish sonni belgilash: Faktorizatsiya qilinishi kerak bo'lgan son (n) tanlanadi.

2. Sonning toq sonligini tekshirish: Son toq sonligi ekanligini tekshirib oling. Agar son juft bo'lsa, unda uning bo'luvchilaridan biri 2 ga teng.

3. Sonning tub son ekanligini tekshirish. Agar son tub son bo'lmasa, keying qadamga o'tiladi, aks holda algoritm to'xtatiladi.

4. Tub ko'paytuvchilar ro'yxati shakllantiriladi, n sonining qiymati 1ga teng bo'lgunga qadar, n sonini Pollardning ρ – methodiga qo'yib, tub ko'paytuvchilaridan birini hisoblab topamiz.

5. Hisoblab topilgan sonni tub ko'paytuvchilar ro'yxatiga qo'shib qo'yamiz. n sonini topilgan songa bo'lib, natijani n ga o'zlashtiramiz.

6. Bu amallarni toki n ning qiymati 1 ga teng bo'lib qolgunga qadar davom ettiramiz. So'ngra natija sifatida tub ko'paytuvchilar ro'yxatini qaytaramiz.

Pollard-Strassen algoritmi, sonning tub ko'paytuvchilarini topish va ularni faktorizatsiyalashga yordam beradi. Bu jarayon samarador va effektiv hisoblanadi. Lekin, u har bir son uchun to'g'ri natija beruvchi faktorizatsiyani ta'minlamaydi. Bu algoritmning murakkablik darajasi $O\left(N^{\left(\frac{1}{4}\right)} \log^4 N\right)$ ga teng.

Shanksning kvadrat shakllarini faktorizatsiyasi. Fermaning faktorizatsiya usulini takomillashtirish maqsadida Daniel Shanks tomonidan ishlab chiqilgan butun sonlarni faktorizatsiyalash usuli hisoblanadi.

Ferma usulining muvaffaqiyati $x^2 – y^2 = N$ shartni qanoatlantiruvchi x va y butun sonlarni topishga bog'liq. Bu yerda N faktorizatsiyalanayotgan son. Ferma usulini yaxshilash uchun $x^2 \equiv y^2 \bmod N$ shartni qanoatlantiruvchi x va y butun sonlarni izlashdir. Yuqoridagi shartni qanoatlantiruvchi (x, y) juftlikni topish faktorizatsiyasini kafolatlamaydi, lekin bu shuni anglatadiki, biz topgan juftliklar $N = x^2 – y^2 = (x – y) \cdot (x + y)$ shart bajarilganda, (x - y) va (x + y) sonlar N soni bilan umumiy bo'luvchiga ega bo'lish ehtimoli kattaroq bo'ladi.

$x^2 \equiv y^2 \bmod N$ shartni qanoatlantiruvchi (x, y) juftlarni topish uchun amaliy algoritm Shanks tomonidan ishlab chiqilgan bo'lib, uni *Kvadrat shakllarni faktorizatsiyalash* yoki SQUFOF (Square Forms Factorization) deb nomlangan. Hozirda ancha samarali faktorizatsiya usullari mavjud bo'lsa-da, Shanksning kvadrat shakllar faktorizatsiyasi usulining afzalligi shundaki, u dasturlashtiriladigan kalkulyatorda amalga oshirish uchun etarlicha kichikdir.

Shanksning kvadratik shakl faktorizatsiya algoritmi quyidagi qadamlardan iborat:

1) Faktorizatsiya qilinishi kerak bo'lgan N sonni olamiz.

2) Agar N toq son bo'lsa, u erda N va 1 dan farqli faktorlarni topib chiqamiz.

3) Agar N juft son bo'lsa, N ni 2 ga bo'lib bo'linma hosil qilish mumkin. Ularning ikkalasi ham faktorlardir.

4) x ni N ning kvadrat ildizining yaxlitlab olingan qiymati bilan boshlang'ich qiymatga o'zlashtiramiz.

5) Agar $x^2 = N$ bo'lsa, bu x soni N ning faktori bo'ladi.

6) Aks holda, x ni bir-biriga yaqinroq bo'lgan qiymatlarga o'zgartirib boramiz va y_kvadrat = $x^2 - N$ ni hisoblaymiz.

7) y_kvadrat manfiy bo'lsa, x ning qiymatini 1ga oshirib yana y_kvadrat qiymatni sinab ko'ramiz.

8) y_kvadrat ning kvadrat ildizining butun qismi y ni olib, y^2 = y_kvadrat shartini tekshirib ko'ramiz.

9) $x^2 \equiv y^2 \bmod N$ shartini qanoatlatiradigan $p = x + y$ va $q = x - y$ qiymatlarni topamiz.

10) Agar N ning p va q ga bo'linishi mumkin bo'lsa, u holda p va q sonlarini faktorlar sifatida qaytaramiz.

11) Aks holda, x ning qiymatini yana oshirib qayta qiymatlarni sinab ko'ramiz.

12) Faktorlar topilmagan holda dasturni tugatamiz.

Ushbu algoritmda kvadrat shakllarni olish, kvadrat tenglikni qanoatlantirish, p va q ni topish kabi amallar bajariladi. Dasturning boshqacha funksiyalari esa kvadratning ildizini hisoblash, faktorizatsiyani bajarish va natijalarni chiqarish uchun ishlatiladi.

Misol uchun 703 sonini ushbu algoritm yordamida faktorizatsiya qilib ko'ramiz.

$x = [\sqrt{N}] = [\sqrt{703}] = 26$ $x * x = N$ shartni tekshiramiz: $26 * 26 \neq 703$ shart qanoatlantirmadi.

1) $x = x + 1 = 27$

$y\_kvadrat = x^2 - N = 27^2 - 703 = 729 - 703 = 26$

$y = \left[\sqrt{y\_kvadrat}\right] = \left[\sqrt{26}\right] = 5$

y^2 = y_kvadrat shartni tekshiramiz: $25 \neq 26$, qanoatlantirmadi x ning qiymatini bittaga oshirib yana tekshirib ko'ramiz.

2) $x = x + 1 = 28$

$y\_kvadrat = x^2 - N = 28^2 - 703 = 784 - 703 = 81$

$y = [\sqrt{y\_kvadrat}] = [\sqrt{81}] = 9$ y^2 = y_kvadrat shartni tekshiramiz: $81 \neq 81$, qanoatlantirdi.

$p = x + y$ va $q = x - y \Rightarrow p = 28 + 9 = 37$ va $q = 28 - 9 = 19$

703 sonining faktorlari: 37 va 19 ekan.

Pollardning P-1 algoritmi. Pollardning P-1 algoritmi faktorizatsiya algoritmi bo'lib, berilgan sonning tub omillarini topishda qo'llaniladi.U faktorlarga ajratiladigan son moduli tasodifiy butun sonning tartibini topish g'oyasiga asoslanadi. Algoritm murakkab sonning kichik omillarini samarali topish uchun ishlatilishi mumkin, bu RSA shifrlashlarini buzish uchun foydali bo'ladi. P-1 algoritmi uni 1974 yilda taklif qilgan matematik Jon Pollard sharafiga nomlangan. Algoritm ketma-ket takrorlashlar natijasida hosil bo'lgan raqamlarning eng katta tub omilini topish orqali ishlaydi. Bu hozirgacha hosil bo'lgan sonlarni tub ko'paytuvchilarga ajratish, har bir raqamning tartibini hisoblash va keyin bu tartiblarning eng katta umumiy bo'luvchisini olish orqali amalga oshiriladi. Pollardning P-1 algoritmi katta tub omillarni topish uchun samarali emas, lekin

undan murakkab sonni faktorizatsiyalashda birinchi qadam sifatida foydalanish mumkin. Pollardning P-1 algoritmi tasodifiy butun son a ni tanlash va a^{m-1}mod n ni hisoblash orqali sonning omillarini qidiradi, bu erda n biz ko'paytirmoqchi bo'lgan butun son, m esa omillar bilan silliq sondir. oldindan belgilangan yuqori chegara. Agar a^{m-1}mod n ga mos kelmasa, biz a^{m-1} va n ning eng katta umumiy bo'luvchisini hisoblashga harakat qilamiz, bu esa n omilini ochishi mumkin. Pollardning P-1 algoritmining samaradorligi cheklangan, chunki algoritm muvaffaqiyatini aniqlashda darajaga oshiriladigan son m ning hajmi va P-1 omillarining o'lchami ham hal qiluvchi rol o'ynaydi.

Pollardning P-1 algoritmida yuqori chegarani B ni belgilab, faktorizatsiya qilinayotgan sonning o'zgaruvchilarini yuqori chegaraga qo'llab-quvvatlangan sanoq tizimlarida (arifmetik operatsiyalar, darajalar, toifalar) ishlatib faktorizatsiya jarayonini amalga oshirishga harakat qiladi.

Pollardning P-1 algoritmi quyidagi bosqichlardan iborat:

1) Faktorizatsiya qilinuvchi son va yuqori chegara B ni belgilaymiz.
2) 2 dan B gacha bo'lgan butun sonlardan bitta a son tanlaymiz.
3) $a = a^x$mod n qiymati hisoblanadi. Bu yerda x ning boshlang’ich qiymati 2 ga teng bo’ladi.
4) Agar y = EKUB (a, n) hisoblanadi.
5) Agar y 1 dan farqli son bo’lsa u n sonining tub bo’linuvchilaridan biri bo’ladi.
6) Agar y = 1 bo’lsa x ning qiymatini 1 ga oshirib boraveramiz toki B ga teng bo’lmaguncha.

Leman algoritmi (yoki Sherman Leman algoritmi) berilgan natural sonni deterministik tarzda tub ko’paytuvchilarga ajratadi. Ushbu algoritm N soni uchun $O\left(N^{\left(\frac{1}{3}\right)}\right)$ ta arifmetik amallar muarakkabligiga ega. Algoritm birinchi marta 1974 yilda amerikalik matematik Sherman Leman tomonidan taklif qilingan. Ushbu algoritm taxminiy $O(\sqrt{N})$ qiymatdan kichik bo'lgan birinchi deterministik butun son faktorizatsiya algoritmi edi. Ayni paytda u sof tarixiy ahamiyatga ega va, qoida tariqasida, amalda qo'llanilmaydi. Sababi shundaki bu algoritm ham kichik sonlarda samarali ishlashi mumkin lekin kattaroq sonlarni faktorizatsiya qilishda bu usul vaqt va xarajat jihatidan maqsadga muvofiq emas.

Quyidagi qadamlarda Leman faktorizatsiya algoritmini batafsil tushuntiriladi:

1) N sonining kub ildizini x ga tenglashtiramiz.
2) x ning oltinchi ildizini y ga tenglashtiramiz. Bu qiymat keyinchalik ishlatiladi.
3) k =1 dan boshlab to x ga qadar sikl ochamiz. Bu k qiymatlarini sinovdan o'tkazish uchun foydalanamiz.
4) $4 * k * N$ ning kvadrat ildizini z ga tenglashtiramiz. Bu qiymat keyinchalik ishlatiladi.
5) z ni yuqoriga yaqin butun soniga yaxlitlaymiz va a ga tenglashtiramiz.

6) z ga $\frac{y}{4*\sqrt{k}}$ ni qo'shib o'ng yonidan yaqin butun soniga yaxlitlaymiz va b ga tenglashtiramiz.

7) a dan b gacha i qiymatlari uchun tsikl ochamiz. Bu i qiymatlarini sinovdan o'tkazish uchun foydalanamiz.

8) t ni hisoblaymiz. Uning qiymati $t = a^2 - 4 * k * N$ ga teng bo'ladi.

9) t ning ildizini hisoblaymiz va butun songa yaxlitlaymiz hamda p ga tenglashtiramiz.

10) Agar p^2 qiymat t ga teng bo'lsa quyidagi qadamlarni bajarishimiz mumkin:

11) i + p va N sonlarining eng kichik umumiy bo'luvchisini topiladi va u 1 dan farqli bo'lsa uni tub bo'luvchilardan biri sifatida qaytaramiz.

12) Agar hech qanday faktor topilmagan bo'lsa berilgan son tub deb qaytish bilan dastur tugaydi.

2.1-jadval Faktorizatsiyalash murakkabligini bartaraf etuvchi eksponensial turdagi algoritmlar tahlili

Algoritm nomi	Asosi	Effektiv chegarasi	Hisoblash murakkabligi
Fermaning faktorizatsiya usuli	N sonini ikki sonning kvadratlari ayirmasi sifatida ifodalash	< 16 bit	$O\left(N^{\frac{1}{3}}\right)$
Pollardning ρ-algoritmi	takrorlanuvchi funksiya ketma-ketlikdagi sikl uzunligini va tug'ilgan kun paradoksining ba'zi oqibatlarini topish	< 30 bit	$O\left(N^{\frac{1}{4}}\right)$
PollardShtrassen algoritmi	Pollardning ρ - algoritmi va Strassen metodi kombinatsiyasi	< 24 bit	$O\left(N^{\left(\frac{1}{4}\right)} \log^4 N\right)$
Shanksning kvadratik shakl usuli	N chekli maydonda kvadratlari teng bo'lgan sonlarni topish	< 26 bit	$O\left(N^{\frac{1}{4}+\varepsilon}\right)$
Pollardning P1 algoritmi	ketma-ket takrorlashlar natija-sida hosil bo'lgan raqamlarning eng katta tub omilini topish	< 66 bit	$O\left(N^{\left(\frac{1}{2}\right)} \log^c N\right)$
Leman usuli	natural sonni deterministik tarzda tub ko'paytuvchilarga ajratish	< 16	$O\left(N^{\left(\frac{1}{3}\right)}\right)$

2.2 Faktorizatsiyalash murakkabligini bartaraf etuvchi subeksponensial turdagi algoritmlar

Subeksponensial algoritmlar, eksponensial algoritmlardan farqli ishlash tartibiga ega bo'lgan algoritmlar hisoblanadi. Bunday nomlanishining asosiy sababi, subeksponensial algoritmlarning faktorizatsiya muammolarini yechishda eksponensial algoritmlardan ancha tezroq ishlashi, muhim samaradorlik olishi, katta

sonlar uchun yaxshiroq natija berishidir. Subeksponensial algoritmlar, eksponensial algoritmlardan farqli ishlash prinsiplariga ega bo'lib, yuqori samaradorlikni ta'minlash uchun bir qancha ma'lumot va tekshiruvlarni olib boradi. Bu esa ularni ishlash tartibini va samaradorlik darajasini oshiradi. Shuning uchun, ular subeksponensial algoritmlar deb nomlanadi.

Faktorizatsiyalash muammosini yechishda subeksponensial algoritmlarning foydalari quyidagilardir:

- Ular eksponensial algoritmlardan ancha tezroq ishlaydi va katta sonlar uchun yaxshiroq natija beradi.
- Ular yuqori samaradorlik darajasiga ega bo'lib, katta sonlarni faktorlarga bo'lishda samaradorlikni oshiradi.
- Ular muhim ma'lumotlar va tekshiruvlar asosida ishlaydigan, yangi prinsiplarga asoslangan algoritmlardir.

Shu sababli, subeksponensial algoritmlar faktorizatsiya muammolarini yechishda muhim ahamiyatga ega bo'ladilar. Subeksponensial algoritmlar, faktorizatsiya muammolarini yechish uchun tegishli matematik modellar va prinsiplar asosida ishlaydigan, va natijada eksponensial ishchi vaqtlardan ancha tezroq natijalar olish imkonini beruvchi usullar hisoblanadi. Ularning barchasi o'zining xususiyatlari va ishlash prinsiplariga ega, shuningdek, foydalanilgan matematik konsepsiyalarga va jarayonlarga asoslanadi. Har bir subeksponensial algoritmda unikal usullar va cheklashuvlar mavjud bo'lib, ularni amalga oshirishda ma'lumotlar yig'ish, hisoblashlar va mantiqiy jarayonlar keng qo'llaniladi.

Subeksponensial algoritmlarning hisoblash muarakkabligi L – yozuv (yoki

L - notation) da baholanadi va quyidagiga teng bo’ladi:

$$L(a, c) := O(e^{c+o(1)} \bullet log^{\alpha} n \bullet log^{1-\alpha} \log n$$

Bu yerda n - tub ko’paytuvchilarga ajratilayotgan son, c va α – ba’zi doimiylar.

Subeksponensial faktorizatsiya algoritmlariga quyidagi algoritmlarni misol keltirish mumkin:

- Dikson algoritmi
- Davomli kasrlar bo’yicha koeffisentlarga ajratish usuli
- Kvadrat elak usuli
- Elliptik egri chiziqlar yordamida Lenstra faktorizatsiyasi
- Raqamli dala elak usuli

Dikson algoritmi. Dikson algoritmi faktorizatsiyalash muammosini bartaraf etish uchun ishlatilgan bir subeksponensial turdagi algoritmdir. Uning asosiy maqsadi bir sonni (masalan, N) uning tub bo'luvchilariga ajratib berishdir.

Dikson usuli koeffitsientga mo'ljallangan N butun son moduliga kvadratlarning mos kelishini topishga asoslangan. Fermaning faktorizatsiya usuli tasodifiy yoki psevdo-tasodifiy x qiymatlarini tanlash va $x^2 \bmod N$ butun soni mukammal kvadrat bo'lishiga umid qilish orqali shunday

moslikni topadi:

$$x^2 \equiv y^2 \bmod N \quad x \not\equiv \pm y \pmod N$$

Dikson algoritmi quyidagi tartibda ishlaydi:

1) Dikson algoritmi uchun boshlang'ich sonlardan birini tanlash, masalan, N.

2) Dikson algoritmi qadamli ravishda taxminiy tub bo'lgan bir bo'luvchi sini topishga harakat qiladi. Bu taxminiy tub bo'luvchilar Dikson algoritmi uchun eng muhim qism bo'lgan boshlang'ich tahminiy bo'luvchilaridir.

3) Agar N taxminiy tub bo'luvchiga qoldiq qoldirgan bo'lsa, u holda faktorizatsiyani yakunlash uchun topilgan bo'luvchini qaytaradi.

4) Agar N taxminiy tub bo'luvchiga qoldiq qoldirmasdan o'tgan bo'lsa, Dikson algoritmi davom etish uchun boshqa bir taxminiy tub bo'luvchi sini topish uchun harakat qiladi.

5) Bular davom etishi taxminiy tub sonlar tugaguncha davom etadi.

Dikson algoritmi katta sonlar faktorizatsiyasini amalga oshirishda ishlatiladi. U yordamida katta sonlar o'rniga undan kichik bo'luvchilarga ajratilgan sonlar topiladi. Bu usul hammasi bilan sonlarni ajratishning tezligi va samaradorligi bilan bilinadi. Ammo, Dikson algoritmi katta sonlar uchun ishlovchi jarayonning xisoblanish chegarasi borligi sababli, katta sonlar uchun ishlovchi dasturlash yoki ma'lumotlar to'plami talab qiladi. Dikson algoritmi shifrlash, parolni to'lash, katta sonlar faktorizatsiyasi va boshqa kriptografiya, matematika va dasturlash sohalarida ishlatiladi. U katta sonlarni bo'luvchilariga ajratib berishda ishlatiladi va bu erda amalga oshirish qulay va samarador bo'lishi mumkin.

Davomli kasrlar bo’yicha koeffisentlarga ajratish usuli. Davomli kasrlar bo’yicha koeffisentlarga ajratish usuli yoki CFRAC (Continued Fraction Factorization) algoritmi butun sonlarni ko‘paytuvchilarga ajratish algoritmi bo‘lib, berilgan butun sonning tub ko’paytuvchilarini topish uchun davomli kasrlardan foydalanadi. Bu erda CFRAC algoritmining bosqichma-bosqich tushuntirishi:

1. Faktorlarga ajratmoqchi bo'lgan N butun sonni tanlab olamiz.

2. Kasrni kengaytirish uchun boshlang'ich qiymatni tanlang, odatda N ning kvadrat ildizga yaqinlashishiga o'rnatiladi.

3. Davomli kasrda birinchi had bo'ladigan kasr kengayishining butun son qismini hisoblang.

4. Oldingi kasrdan butun sonni ayirish orqali kasrni yangilang. Bu keyingi muddat uchun ishlatiladigan kasr qismini beradi.

5. Oldingi bosqichda olingan kasr qismining o'zaro nisbatini hisoblang.

6. Tub bo’luvchisi topilmaguncha yoki ma'lum bir shart bajarilmaguncha (masalan, takrorlashlarning maksimal soni) 3-5-bosqichlarni takrorlang.

7. Agar tub ko’paytuvchilardan biri topilsa, uni natija sifatida qaytaring.

Aks holda, keyingi bosqichga o'ting.

8. Kasrni kengaytirishning boshlang'ich qiymatini sozlang va 3-7bosqichlarni yangi boshlang'ich qiymat bilan takrorlang.

9. Agar har xil boshlang'ich qiymatlarga ega bo'lgan bir necha marta takrorlashdan keyin tub bo’luvhcilardan biri topilmasa, algoritm tugatilishi mumkin.

Shuni ta'kidlash kerakki, CFRAC algoritmi barcha butun sonlar uchun tub ko’paytvchilarni topishga kafolat bermaydi. Uning muvaffaqiyati turli omillarga, jumladan faktorlangan sonning xususiyatlariga va kasrni kengaytirish uchun boshlang'ich qiymatlarni tanlashga bog'liq.

Kvadrat elak algoritmi. Kvadrat elak algoritmi murakkab sonning tub omillarini topish uchun ishlatiladigan faktorizatsiya usulidir. Bu yarim tub sonlar (ikki tub sonning ko'paytmasi) bo'lgan katta sonlarni faktoring qilish uchun samarali algoritmdir. Kvadrat elak algoritmining qisqacha tavsifi quyidagicha:

1. Faktorlar bazasining o'lchamini aniqlaydigan B ni tanlang. Faktorlar bazasi kichik tub sonlardan iborat bo'lib, faktorlarga ajratiladigan sonni ushbu tub sonlarning kichik darajalarga ko'paytmasi sifatida ifodalash mumkin.
2. Faktorlar bazasidagi tub sonlarni modul bo‘yicha kvadratik qoldiqlar to‘plamini hosil qiling. Bular har bir tub modul bo'yicha mukammal kvadratlar sifatida ifodalanishi mumkin bo'lgan raqamlardir.
3. Kvadrat qoldiqlardan foydalanib, A matritsasini tuzing, bunda har bir satr faktorlar asosi tubiga va har bir ustun koeffitsientga ajratiladigan songa mos keladi. Matritsadagi yozuvlar mos keladigan sonni faktorizatsiya qilishda har bir tub sonning ko'rsatkichini ifodalaydi.
4. Chiziqli mustaqil qatorlar to‘plamini topish uchun A matritsada Gaussning yo‘q qilishini bajaring. Bu matritsani qator-satr shakliga qisqartiradi.
5. A matritsaning qator-satr shakli bilan ifodalangan chiziqli sistemaning tub yechimini toping. Bu chiziqli tenglamalar tizimini modul 2 yechish orqali amalga oshiriladi.
6. Tub yechimdan foydalanib, moslik munosabatini tuzing. Bu munosabat to'liq kvadrat modul bo'lgan sonlar ko'paytmasini faktorlarga ajratiladigan sonni beradi.
7. Sonning tub omilini topish uchun moslik munosabatining kvadrat ildizini oling.
8. Kerakli omillar topilguncha jarayonni turli bazis va omil asoslari bilan takrorlang.

Kvadrat elak algoritmini amalga oshirish raqamlar nazariyasi va ilg'or matematikani chuqur tushunishni talab qiladi. Bu murakkab matematik operatsiyalar va optimallashtirishni o'z ichiga oladi. U odatda C++ yoki Python kabi dasturlash tillarida samarali modulli arifmetik va chiziqli algebra operatsiyalari uchun maxsus kutubxonalar yordamida amalga oshiriladi. E'tibor bering, Kvadrat elek algoritmi davom etayotgan tadqiqot va takomillashtirish mavzusidir. Amalga oshirish tafsilotlari va optimallashtirishlar aniq variant yoki foydalanilgan dasturga qarab farq qilishi mumkin.

Elliptik egri chiziqlar yordamida Lenstra faktorizatsiyasi. Elliptik egri chiziqlar yordamida Lenstra faktorizatsiyasi, subeksponensial turdagi faktorizatsiya algoritmidir. Ushbu algoritmning asosiy qismi, Lenstra tuzilganida, faktorlashtirishga urinishning eng oson turi sifatida qaraladi. Quyidagi qadam

ma'lumotlari yordamida Lenstra faktorizatsiyasi usulining algoritmi tasvirlangan:

1. Kirishda faktorizatsiya uchun butun murakkab sonimiz N ni tanlashimiz kerak. Bu son, ikki toq sonning ko'paytmasi bo'lishi kerak.
2. Ixtiyoriy bir elliptik egri chiziqlarni tanlab, chiziqning to'rtinchi darajasini N ga nisbatan modulga olib, chiziqning boshlanish nuqtasini aniqlaymiz.
3. Shuningdek, ixtiyoriy bir nuqta P ni elliptic egri chiziqqa qo'yamiz va uning to'rtinchi darajasini N ga nisbatan modulga olib olamiz. Agar P nuqta egri chiziq tomonidan qabul qilinsa, biz boshqa bir nuqta tanlashimiz kerak.
4. Nuqtalar jadvallarini tuzib, a'zo nuqtalarning yig'indisini aniqlab, N ga nisbatan modulga olib olamiz. Agar yig'indi N ni kattalashtirgan bo'lsa, biz boshqa nuqta tanlaymiz.
5. Nuqta va chiziqdagi sonlar bilan jadvallar yordamida oxirgi darajaga kelguncha nuqtalarni hisoblab chiqamiz.
6. Har safar nuqtalar jadvallarini yangilab, oxirgi darajaga kelguncha hisoblamalar amalga oshiriladi. Agar oxirgi darajali nuqtalardan biri nolga teng bo'lsa, faktor topilgan hisoblanadi.
7. Agar faktor topilmagan bo'lsa, biz boshqa boshlang'ich nuqta va chiziqni tanlaymiz va ushbu qadamdan qaytib qayta amalga oshiramiz.

Lenstra faktorizatsiyasi amaliyotda shu tartibda bajariladi. Uning natijasida faktorizatsiya uchun qidirilayotgan faktorlar topiladi. Biroq, ma'lumki, bu faktorizatsiya usullari muammolarga duch kelsa ham, ba'zi sonlar uchun samarali bo'lishi mumkin. Lenstra faktorizatsiyasini amaliyotda dasturlash uchun, katta sonlar bilan ishlashda yuqori darajali arifmetik operatsiyalarni amalga oshirishga imkoniyat beruvchi til, masalan, Python yoki C++ kabi, foydalanish tavsiya etiladi.

Raqamli dala elak usuli. Raqamli dala elak usuli (Number Field Sieve) bir faktorizatsiya algoritmidir, uning asosiy maqsadi katta sonlarni faktorlashtirishdan iboratdir. Raqamli dala deyishining asosiy sababi, faktorizatsiya amalini osonlashtirish va ishni yuqori darajada sodda hisoblash imkoniyatini yaratishdir. Raqamli dala, odatda, sonning ko'pincha elementli algebraik jism sifatida tanlanadi. Bu esa sonning faktorizatsiyasini, kvadrat elak usuli yoki boshqa usullardan foydalanishdan ko'ra yuqori darajali oson bo'lishini ta'minlaydi. Bu algoritmda sonlar raqamli dalalar yordamida ishlab chiqiladi va faktorizatsiya uchun ularga yordam beriladi. Quyidagi qadam ma'lumotlari yordamida Raqamli dala elak usuli faktorizatsiyasi haqida umumiy tushunchani berish mumkin:

1. Kirishda faktorizatsiya uchun faktorlashtiriladigan sonimiz N ni tanlashimiz kerak. Bu son, ikki toq sonning ko'paytmasi bo'lishi kerak.
2. Raqamli dala elak usuli uchun raqamli dalalarni tanlash kerak. Ular sonning raqamli tashkil qilinishiga to'sqinlik qiladigan dalalar bo'ladi.
3. Raqamli dalalar orqali sonimizning modulga nisbatan normasini hisoblaymiz. Norma sonimizning sifatlarini o'z ichiga oladi va dalalar orqali sonni faktorlashtirishda yordam beradi.
4. Raqamli dalalar yordamida sonning kvadratlarini hisoblaymiz va ularni normasiga nisbatan modulga olib olamiz.
5. Raqamli dalalar orqali sonimizning kvadratlaridan olinadigan normaga ega sonlarni topish uchun elon qilingan ma'lumotlardan foydalanamiz.

6. Sonlar orasida katta bo'lgan faktorlarni topish uchun o'zgaruvchiladan foydalanamiz. Ular sonning normasiga nisbatan o'zaro bog'liq bo'lgan sonlar bo'ladi.

7. Sonlar orasida katta bo'lgan faktorlarni topgandan so'ng, ular orqali asosiy sonimizni tub ko'paytuvchiga bo'lish amalga oshiriladi.

Raqamli dala elak usuli faktorizatsiyasi juda murakkab algoritm hisoblanadi va katta sonlar uchun samarali bo'lgan faktorizatsiya usulidir.

2.2-jadval Faktorizatsiyalash murakkabligini bartaraf etuvchi subeksponensial turdagi algoritmlar tahlili

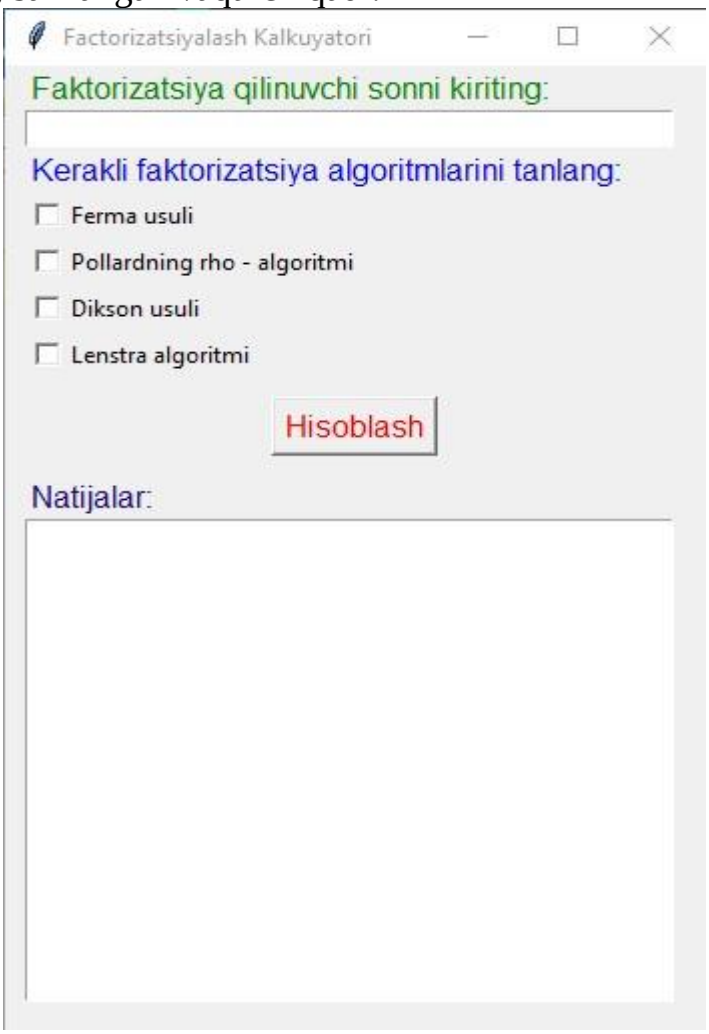
Algoritm nomi	Asosi	Effiktiv chegarasi	Hisoblash murakkabligi
Dikson algoritmi	koeffitsientga mo'ljallangan N butun son moduliga kvadratlarning mos kelishini topish	< 73 bit	$L\left(\frac{1}{2}, 2\sqrt{2}\right)$
Davomli kasrlar bo'yicha koeffisentlarga ajratish usuli	Davomli kasrning yaqinlashuviga asoslangan	< 80 bit	$L\left(\frac{1}{2}, \sqrt{2}\right)$
Kvadrat elak usuli	Fermaning faktorizatsiya usulining umumlashtirish	< 100 bit	$L\left(\frac{1}{2}, 1\right)$
Elliptik egri chiziqlar yorda-mida Lenstra faktorizatsiyasi	elliptik egri chiziqlar yordamida natural sonni tub ko'paytuvchilarga ajratish	< 83 bit	$L\left(\frac{1}{2}, \sqrt{2}\right)$
Raqamli dala elak usuli	umumiy sonli maydon elaklari tub darajalardan tashqari har qanday raqamni omillashtirishga asoslangan	< 110 bit	$L\left(\frac{1}{3}, \sqrt[3]{\frac{64}{9}}\right)$

Faktorizatsiyalash muammosini yechuvchi algoritmlarning qiyosiy tahlilini amalga oshiruvchi dasturiy ta'minot.

Endilikda biz yuqoridagi algoritmlar yordamida faktorizatsiyalash muammosini yechuvchi algoritmlarni qiyosiy tahlil qiluvchi dasturiy vosita ishlab chiqamiz. Bunda Python dasturlash tili hamda uning grafik foydalanuvchi oynalar bilan ishlovchi Tkinter kutubxonasidan uzviy ravishda foydalanamiz. Quyidagi rasmda dasturiy ta'minotimizning asosiy oynasi keltirib o'tigan (2.2-rasm). U quyidagi qismlardan iborat:

1) Faktorizatsiya qilinuvchi sonni kiritish uchun maydon;
2) Kerakli faktorizatsiyalash algoritmlarini tanlash imkonini beruvchi tugmachalar. Bu yerda 2 ta eksponensial (Ferma usuli, Pollardning rho- algoritmi) va 2 ta subeksponensial (Dikson usuli, Lenstra algoritmi) turdagi faktorizatsiyalash algoritmlari keltirilgan;
3) Hisoblash ishlarini boshlash buyrug'ini beruvchi tugmacha;
4) Algoritmlar qaytargan natijalarni ko'rsatuvchi maydon.

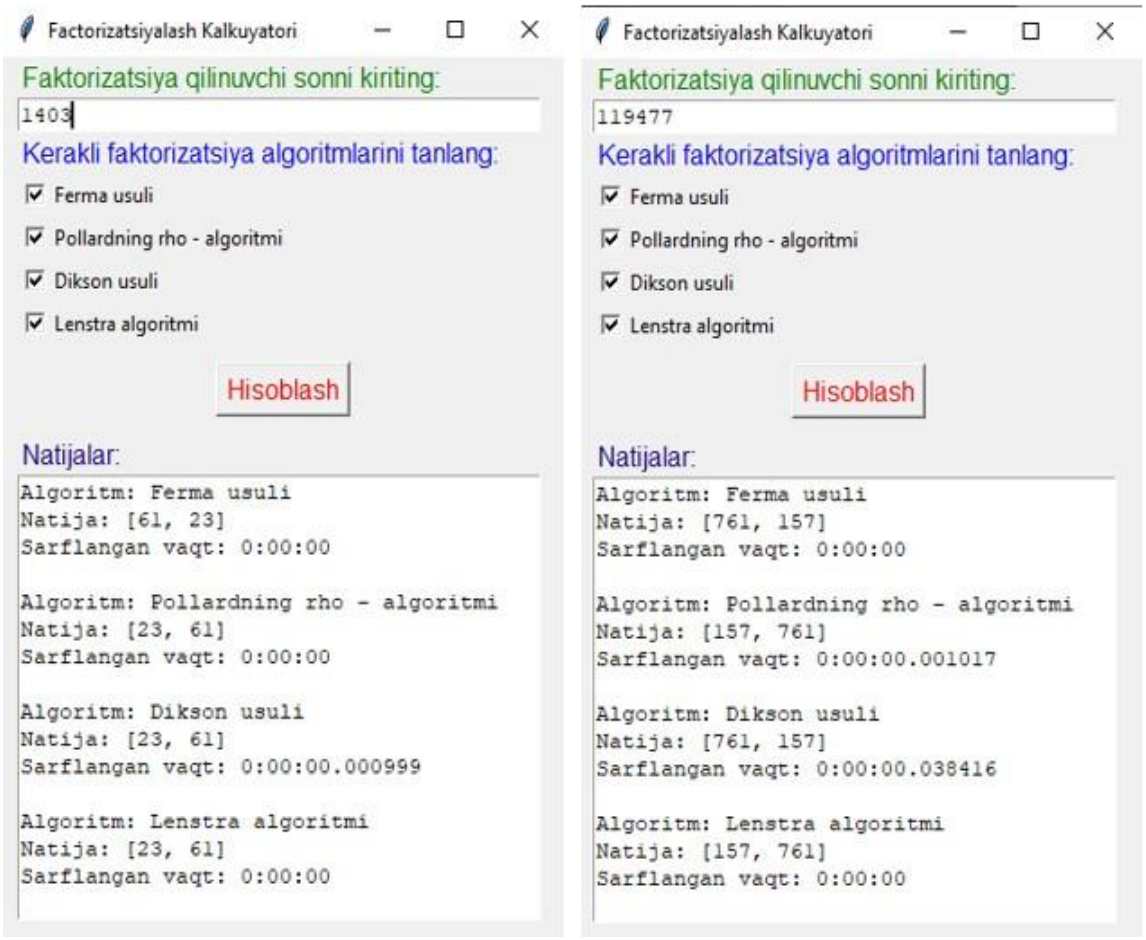
Bu dasturdan foydalanish juda qulay bo’lib, eng avvalo faktorizatsiya qilinuvchi sonni kiritiladi. So’ngra o’zimizga kerakli bo’lgan algoritmlarni tanlaymiz. Bir vaqtning o’zida bir nechta yoki bitta algoritmni tanlash imkoniyati mavjud. Kerakli algoritmlarni tanlagandan so’ng, “Hisoblash” tugmasini bosamiz. Shundan so’ng bizga natijalar maydonida biz tanlagan algoritm nomi, faktorizatsiya natijasi, sarflangan vaqti chiqadi.



2.2-rasm. Dasturiy ta’minotimizning asosiy oynasi

Bu dasturiy ta’minotni ishlab chiqishda men yuqori ko’rib o’tgan faktorizatsiya agoritmlaridan foydalanib Python dasturlash tilida har birining dasturini tuzib chiqqanman. Asosiy dastur ishga tushishi bilan dastur “Hisoblash” tugmasining bosilishini kutadi. Bu holat yuz berganda faktorizatsiyalanuvchi qiymatni kerakli maydondan o’qib olib, belgilangan algoritmlar uchun mos ravishda ishlab chiqilgan funksiyalarni chaqirib ularga faktorizatsiya qilinuvchi sonni uzatadi. Mos algoritmlar funksiyalari kerakli natijani va sarflangan vaqtni qaytargandan so’ng, natijalar maydoniga kerakli formatda mos natijalar va sarflangan vaqtlar chiqariladi.

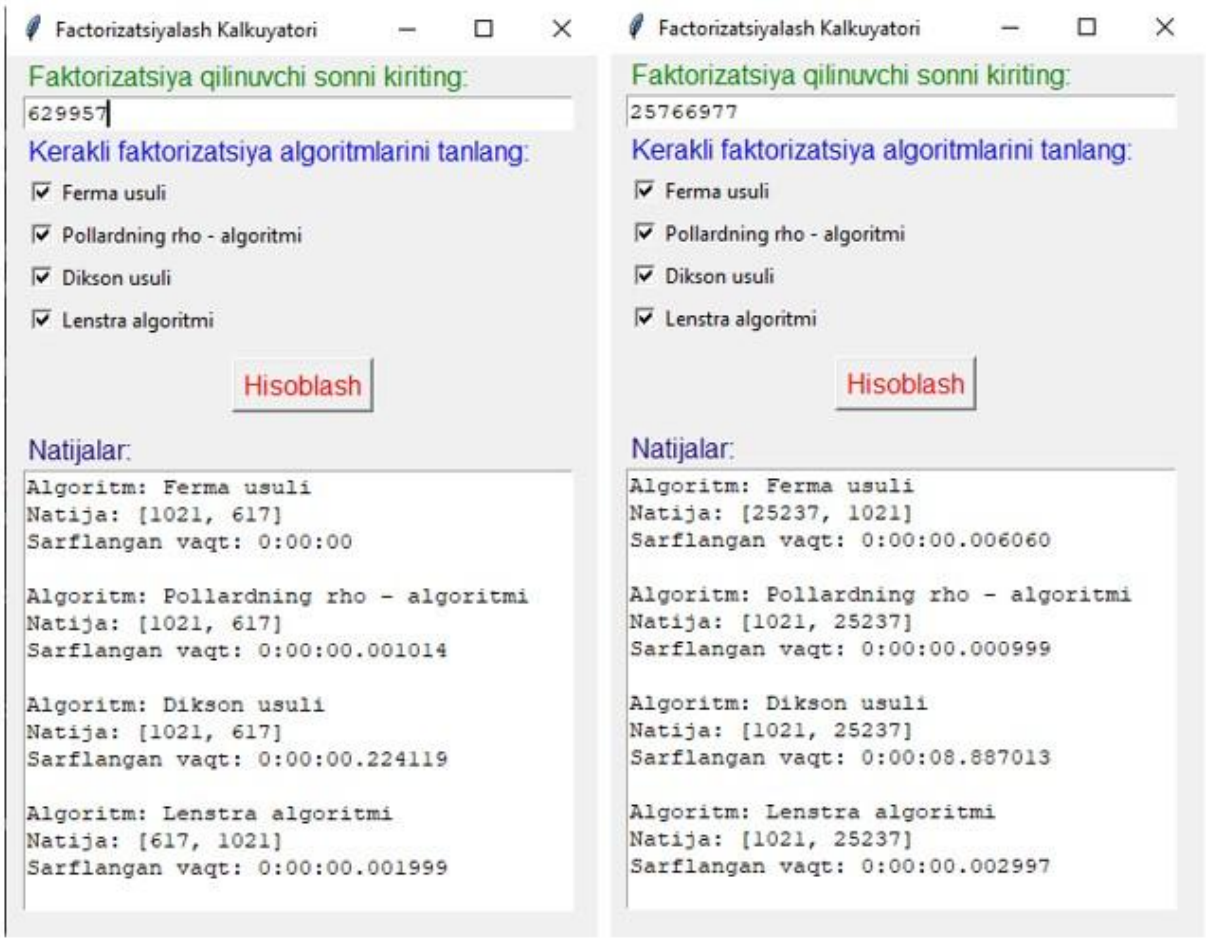
Quyida ushbu dasturiy ta’minot yordamida bir qancha sonlarni faktorizatsiyalashga va natijalar olishga harakat qilamiz:



2.3-rasm. 11 bitli 1403 va 17 bitli 119477 sonlarini dasturiy ta’minotimiz yordamida faktorizatsiya qilingandagi natijalar

Ko’rib turganingizdek, 11 bitli 1403 sonini faktorizatsiya qilganimizda Fema usuli, Pollardning rho – algoritmi va Lenstra algoritmlari deyarli vaqt sarflamasdan ishladi. Dikson algoritmi esa taxminan 1millisekund vaqt sarfladi.

Va yana ko’rib turganingizdek, 17 bitli 119477 sonini faktorizatsiya qilganimizda Fema usuli va Lenstra algoritmlari deyarli vaqt sarflamasdan bajardi. Pollardning rho-algoritmi 1millisekunddan ko’proq, Dikson algoritmi esa taxminan 38 millisekunddan ko’proq vaqt sarfladi.



2.4-rasm. 20 bitli 629957 va 25 bitli 25766977 sonlarini dasturiy ta’minotimiz yordamida faktorizatsiya qilingandagi natijalar.

Ko’rib turganingizdek, 20 bitli 629957 sonini faktorizatsiya qilganimizda Fema usuli deyarli vaqt sarflamasdan ishladi. Pollardning rho – algoritmi 1 millisekunddan ko’proq, Lenstra algoritmi taxminan 2 millisekund va Dikson algoritmi esa 224 millisekunddan ko’proq vaqt sarfladi.

Va yana ko’rib turganingizdek, 25 bitli 25766977 sonini faktorizatsiya qilganimizda Fema usuli 6 millisekunddan ko’proq vaqt sarfladi. Pollardning rho – algoritmi taxminan 1 millisekund, Lenstra algoritmi taxminan 3 millisekund va

Dikson algoritmi esa 8.887 sekunddan ko’proq vaqt sarfladi.

Faktorizatsiya qilinayotgan son kattalashgan sari sarflanayotgan vaqt ham ortib boryapti. Buning juda katta sonlarda quyida ko’rishimiz mumkin:

2.3-jadval 30 bitdan katta sonlarda dasturiy ta’minotning natijalari

N ning uzunligi (bit)	N murakkab son	N ning tub bo’luvchilari	Ferma usuli (s)	Pollardning p-algoritmi (s)	Lenstra usuli (s)
30	873250877	15877*55001	0,003	0,001	0,004
35	25010959333	109961*227453	0,008	0,002	0,002
40	749550288583	434501*1725083	0,202	0,008	0,014

45	308447255087763	7951477*3879119	0,271	0,036	0,004
50	890478947983561	66172661*13456901	8,309	0,040	30,338

Diskret logorifmlash muammosini yechuvchi algoritm turlari

Diskret logorifmlash muammolari, matematika va kriptografiya sohalarida keng qo‘llaniladigan bir muammo turidir. Bu muammo biror modul bo‘yicha diskret yechimni hisoblashni talab qiladi. Diskret logorifmlash muammosi bir qancha maqsadlarda foydalaniladi, ma’lumotlarni himoyalash, shifrlash va deshifrlash.

Diskret logorifmlashning asosiy maqsadi, ma’lum bir gruppada berilgan sonning qanday darajasi berilgan boshqa songa tengligini aniqlashga qaratilgan. Ya’ni:

$$a^x \equiv b \; mod \; p$$

tenglikda x noma’lumni topishga qaratilgan. Bu yerda $p - G$ guruh tartibi, a – guruh generatori, b – guruh elementi.

Diskret logorifmlash muammosini yechishda, ya’ni x noma’lumni topish uchun bir nechta algoritmlar mavjuddir, ba’zi bir modullar bo‘yicha hisoblash amaliy jihatdan imkonsiz deb hisoblanadi, ba’zida esa nisbatan tez yechim topishni ta’minlaydi. Shu sababli, kriptografiyada, bir moduldan tashqari yechim topish mumkin bo‘lgan algoritmlardan foydalaniladi, bu esa shaxslarning ma’lumotlarini himoyalashga yordam beradi.

Diskret logorifmlash, bugungi kunda ma’lumotlar himoyalanishida katta ahamiyatga ega bo‘lib, xususan, kredit kartalari va bank hisob varaqlari kabi shaxsiy ma’lumotlar va shaxsiy identifikatsiyada amalga oshirishda qo‘llaniladi. Shuningdek, kriptovalyuta yaratish va uning operatsiyalari ham diskret logorifmlash murakkabligiga asoslangan. Shuningdek, xabarlar zanjirli tizimi (blockchain) ham diskret logorifmlash murakkabligiga asoslangan.

Diskret logorifmlash muammosini yechish uchun bir qancha algoritmlar ma’lum. Biz algoritmlarni ikkita toifaga ajratamiz, ***umumiy algoritmlar*** va ***guruhga xos*** algoritmlar. Birinchi toifani biz umumiy algoritmlar deb ataymiz, chunki ular odatda har qanday siklik guruhga nisbatan qo‘llaniladi. Umumiy algoritm umumlashtirilgan diskret logorifmlash muammosini (GDLP) hal qiladi. Algoritmlarning ikkinchi toifasi guruhga xos algoritmlardir. Bular guruh elementlaridagi strukturadan foydalanadigan va faqat ma’lum guruhlar oilalarida qo‘llaniladigan maxsus algoritmlardir.

Biz ko‘rib chiqadigan umumiy algoritmlarga Shank algoritmi kiradi, bu algoritm Baby-Step Giant-Step algoritmi, Pollardning Rho va Pollardning Kangaroo algoritmlari deb ham ataladi. Bu algoritmlar har qanday siklik guruhga, shu jumladan elliptik egri guruhlarga va Z_p^* ning kichik guruhlariga nisbatan qo‘llaniladi, bu yerda yaxshiroq usullar qo‘llanilmaydi. Biz muhokama qiladigan guruhga xos algoritmlar indekslarni hisoblash algoritmlaridir. Ular Z_p^* guruhlarida qo‘llaniladi. Shuning uchun indekslarni hisoblash algoritmlari standart diskret logorifmlash muammosini (DLP) hal qiladi.

Diskret logorifmlash muammosini yechuvchi algoritmlarni ***Big O notation*** yordamida, nazariy jihatdan ish vaqti murakkabligini o‘lchaymiz.

Algoritmni ishga tushirish uchun zarur bo‘lgan aniq vaqt, vaqt murakkabligi haqida to‘liq tasavvurga ega bo‘lish uchun yetarli ma’lumot emas. Ushbu muammoni hal qilish uchun siz Big O dan foydalanishingiz mumkin. Big O ko‘pincha turli ilovalarni solishtirish va qaysi biri eng samarali ekanligini aniqlash uchun ishlatiladi, keraksiz tafsilotlarni o‘tkazib yuboradi va algoritmning ishlash vaqtida nima muhimligiga e’tibor beradi.

Turli xil algoritmlarni ishga tushirish uchun zarur bo‘lgan soniyalar vaqtiga bir nechta bog‘liq bo‘lmagan omillar, jumladan protsessor tezligi yoki mavjud xotira ta’sir qilishi mumkin. Boshqa tomondan, Big O apparat diagnostikasi nuqtai nazardan ish vaqtining murakkabligini ifodalash uchun platformani taqdim etadi. Big O bilan siz algoritmingizning ishlash vaqti kirish hajmiga nisbatan qanchalik tez o‘sishi nuqtai nazaridan murakkabligini ifodalaysiz.

Agar n algoritmga kirish hajmi deb faraz qilsak, Big O n va algoritm yechim topish uchun bajaradigan qadamlar soni o‘rtasidagi munosabatni ifodalaydi. Big O bosh harfi “O” dan keyin qavslar ichidagi bu munosabatdan foydalanadi. Masalan, O(n) ularning kiritish hajmiga mutanosib ravishda bir necha bosqichlarni bajaradigan algoritmlarni ifodalaydi.

Big O	**Complexity (Murakkablik)**	**Tavsif**
$O(1)$	*constant (doimiy)*	Ish vaqti kirish hajmidan qat’iy nazar doimiydir. Xesh jadvalidagi elementni topish *doimiy vaqt* ichida bajarilishi mumkin bo‘lgan operatsiyaga misoldir.
$O(n)$	*linear (chiziqli)*	Ish vaqti kirish hajmiga qarab *chiziqli* ravishda o‘sadi. Ro‘yxatning har bir bandidagi shartni tekshiradigan funksiya $O(n)$ algoritmiga misol bo‘la oladi.
$O(n^2)$	*quadratic (kvadratik)*	Ish vaqti kirish hajmining *kvadratik* funktsiyasidir. Har bir element ikki marta tekshirilishi kerak bo‘lgan ro‘yxatdagi takroriy qiymatlarni topishning sodda amalga oshirilishi kvadratik algoritmga misoldir.
$O(2^n)$	*exponential (ko‘rsatkichli)*	Ish vaqti kirish hajmi bilan *eksponent* ravishda o‘sadi. Ushbu algoritmlar juda samarasiz deb hisoblanadi.
$O(logn)$	*logarithmic (logorifmik)*	Ish vaqti *chiziqli* ravishda o‘sadi, kirish hajmi esa *eksponent* ravishda o‘sadi. Misol uchun, ming elementni qayta ishlash uchun bir soniya kerak bo‘lsa, o‘n mingni qayta ishlash uchun ikki soniya, yuz mingni qayta ishlash uchun uch soniya va hokazo. Ikkilik qidiruv logorifmik ish vaqti algoritmiga misoldir.

Diskret logorifmlashning yechimi, bir nechta usullar yordamida amalga oshiriladi, bularga quyidagi usullar keltirsak bo‘ladi:

Brute-Force qidiruvi. Biz umumiy algoritmlarni o‘rganishni eng oddiy usullardan biri bo‘lgan, *brute-force* yoki *to‘liq* qidiruvi bilan boshlaymiz. Bu shunchaki moslik topilmaguncha barcha mumkin bo‘lgan darajani $(g^0, g^1, g^2, \dots)$ sinab ko‘rishdir.

Algoritm: *Brute-Force qidiruvi*

Input: *G – siklik guruh, g – generator, a – guruh elementi*

Output: $g^x = a$ *dan x– darajani topish kerak*

```
1: b = 1
2: x = 0
3: while a ≠ b do
4:     b = b × g
5:     x = x + 1
6: end while
7: return x
```

Eng yomon holatda, $a = g^{N-1}$ bo‘lganida, har bir daraja ya’ni 0 dan $N-1$ gacha sinovdan o‘tkaziladi. Kirishning bit uzunligi bo‘yicha, n, bu eng yomon holatda 2^n guruh operatsiyalarini va taqqoslashni talab qiladi. O‘rtacha holatda, algoritmning yarmini yoki 2^{n-1} guruh operatsiyalarini qidirgandan so‘ng to‘g‘ri darajani topishni kutish mumkin. Ikkala holatda ham algoritmning ishlash vaqti eksponent bo‘lib, $O(2^n)$ bo‘lib, tezda n ni oshirish juda qiyin bo‘ladi.

Boshqa tomondan, algoritm talablari minimaldir. Har bir qadamda biz faqat x va b ni saqlashimiz kerak va ikkalasini ham n bitda ko‘rsatish mumkin. Shuning uchun Brute-Force algoritmining asimptotik space (bo‘sh joy talabi) talabi $O(n)$.

Oldindan hisoblangan jadval algoritmi. Brute-Force qidiruv algoritmining o‘rtacha ikkita ishi barcha N darajani hisoblashga teng ish hajmini talab qiladi. Buning o‘rniga, avval barcha N darajani hisoblab, ularni saqlagan bo‘lsa, bu oldindan hisoblangan jadval algoritmi ortidagi g‘oya. Biz guruh uchun har bir diskret logorifmdan iborat jadval tuzamiz. Jadvalni hisoblagandan so‘ng, individual diskret logorifmni topish uchun faqat bitta jadvaldan qidirish kerak bo‘ladi.

Oldindan hisoblangan jadval algoritmining asimptotik ish vaqti $O(2^n)$. Algoritmning afzalligi shu guruhdagi keyingi diskret logorifmlarning tezkor yechimlari; faqat bitta jadvaldan qidirish talab qilinadi.

Algoritm: *Oldindan hisoblangan jadval algoritmi*

Input: *G – siklik guruh, g – generator, a – guruh elementi*

Output: $g^x = a$ *dan x– darajani topish kerak*

1: $0 \leq x < N$ *uchun* $hash[g^x] = x$ *jadvalini tuzish kerak*

2: $b = 1$

3: **for** $x = 0$ to $N - 1$ **do**

4: $\quad hash[b] = x$

5: $\quad b = b \times g$

6: **end for**

7: // *jadval qidiruvi bajariladi*

8: $x = hash[a]$

9: **return** x

Bu algoritm kriptologik ahamiyatga ega bo‘lgan n ning qiymatlari uchun bajarib bo‘lmaydi, chunki u time (vaqt) va space (bo‘sh joy) murakkabligida eksponent hisoblanadi. Qidiruv jadvali n o‘lchamdagi N ta qiymatga ega bo‘lib, $O(n2^n)$ ning asimptotik o‘lchamini beradi.

Shank algoritmi. Diskret logorifmlash muammosini brute-force qidiruvi yordamida yechish $O(2^n)$ guruh operatsiyalarini talab qiladi. Oldindan hisoblangan jadval yordamida biz buni doimiy vaqtda bajarishimiz mumkin, lekin $O(n2^n)$ bit saqlashni talab qilamiz. Agar biz ushbu ikki ekstremal o‘rtasida optimal nuqtani topsak nima bo‘ladi? Shank algoritmi bizga bunday muvozanatga erishish yo‘lini beradi. Shank algoritmi *baby-step giant-step* algoritmi sifatida ham tanilgan. Algoritm ikki bosqichdan iborat. Algoritmning birinchi bosqichida biz g^i ning birinchi X darajalarini ketma-ket bosib o‘tamiz: $g^0, g^1, g^2, \dots g^{X-1}$ kabi. Bular “baby-steps (chaqaloq qadamlari)” deyiladi. Har bir qadamda biz darajani, i ni, g^i bilan indekslangan xesh jadvalida saqlaymiz. X qadamlardan so‘ng bizda diskret logorifmlar jadvali mavjud, lekin faqat siklik guruhning birinchi X elementlari uchun.

Ikkinchi bosqichda biz $a = g^x$ ni oldindan hisoblangan diskret logorifmlar diapazonimizdagi qiymatga aylantirmoqchimiz. g^x dan boshlab, biz logorifmlarni oldindan hisoblab chiqqan siklning boshiga yetgunimizcha, siklik guruh bo‘ylab bir vaqtning o‘zida X elementlarni bosqichma-bosqich o‘tkazamiz. Ushbu “giant-steps (gigant qadamlar)” ni olish uchun biz shunchaki g^X ga ko‘paytiramiz,

$$g^x\, g^X = g^{x+X},$$
$$g^{x+X}\, g^X = g^{x+2X}$$
$$\vdots$$

Oldindan hisoblangan diapazonda qiymatni topganimizda, biz quyidagi tenglamaga ega bo‘lamiz,

$$g^h = g^{x+yX}$$

x quyidagicha hal qilinadi,

$$h = x + yX \mod N$$
$$x = h - yX \mod N$$

Algoritm: *Shank algoritmi*

Input: *G – siklik guruh, g – generator, a – guruh elementi,*
Oldindan hisoblash uchun darajalar soni: X

Output: $g^x = a$ *dan x– darajani topish kerak*

1: $0 \le i < X$ *uchun* $hash[g^i] = i$ *xesh jadvalini tuzish kerak*
2: $b = 1$
3: **for** $i = 0$ to $X - 1$ **do**
4: $\quad hash[b] = i$
5: $\quad b = b \times g$
6: **end for**
7: *// Xeshda bittasini topilguncha ketma-ket darajalarni hisoblash*
8: $b = a$
9: $y = 0$
10: $h = hash[b]$
11: **while** $g^x = a$ **do**
12: $\quad b = b \times g^X$
13: $\quad y = y + 1$
14: $\quad h = hash[b]$
15: **end while**
16: $x = h - yX \mod N$
17: **return** x

Biz oldindan hisoblangan ketma-ket X darajalar oralig‘ida logorifmni topamiz, chunki biz bir vaqtning o‘zida aynan X darajaga qadam qo‘yamiz.

Endi biz algoritmning ishlash vaqtini ko‘rib chiqamiz. Birinchi bosqich X guruhi operatsiyalarini talab qiladi. Ikkinchi bosqichning ishlash muddati oldindan hisoblangan darajalar oralig‘iga erishish uchun ulkan qadamlar soniga qarab o‘zgaradi. Ko‘p qadamlar $X < x < 2X$ bo‘lganda, x ni oldindan hisoblangan darajalar oralig‘idan tashqariga qo‘yganda kerak bo‘ladi. Bu eng yomon holatda, ikkinchi bosqich $\left[\frac{N}{X}\right]$ guruh operatsiyalarini oladi (g^h ga ko‘paytirish).

Umumiy hisoblash vaqtini minimallashtirish uchun biz X ni tanlashimiz kerak, shunda baby-steps giant-steps soniga teng bo‘ladi. $X = \left[\frac{N}{X}\right]$ bo‘lganda.

$$X = \left[\frac{N}{X}\right],$$
$$X^2 = N,$$
$$X = \sqrt{N},$$
$$X = \sqrt{2^n},$$
$$X = 2^{\frac{n}{2}}.$$

$X = 2^{\frac{n}{2}}$ bo‘lsa, algoritmning ikkala bosqichida $2^{\frac{n}{2}}$ guruh amallari qabul qilinadi. Shuning uchun Shank algoritmining ish vaqti murakkabligi $O\left(2^{\frac{n}{2}}\right)$ ga teng.

Ishlash vaqti hali ham eksponent bo‘lsa-da, bu brute-force qidiruvga nisbatan sezilarli yaxshilanishdir.

Bo‘sh joy talablari brute-force qidiruvi va oldindan hisoblangan jadval algoritmlari o‘rtasidagi o‘rta zamindir. Shank algoritmidagi jadval n-bit o‘lchamdagi X yozuvlarni talab qiladi. Shuning uchun Shank algoritmining bo‘sh joy murakkabligi $O\left(n2^{\frac{n}{2}}\right)$ ga teng.

Pohlig-Hellman algoritmi. Bu algoritm N ning asosiy faktorizatsiyasidan, guruh tartibidan foydalanadi. Asosiy tartib guruhlari uchun bu algoritm hech qanday afzallik bermaydi va Shank algoritmiga ekvivalentdir. Bizning tahlilimiz N tartibida faqat kichik asosiy omillarga ega bo‘lgan holatga qaratiladi. Aynan shu yerda algoritm eng samarali hisoblanadi.

Pohlig-Hellman algoritmining birinchi pog‘onasi guruh tartibi N ni, faktorlari topiladi. Agar N faqat kichik tub sonlarga ega bo‘lsa, faktorizatsiyani osongina topish mumkin. $N = \prod_{i=1}^{k} {p_i}^{n_i}$

Har bir noyob tub son, p_i uchun biz $x_i \equiv x \bmod {p_i}^{n_i}$ ni hal qilamiz. Har bir x_i topilgach, ular qoldiqlar haqidagi Xitoy teoremasi yordamida x ni topish uchun birlashtirilishi mumkin, $O(k \log N)$ guruh operatsiyalari va $O(k \log N)$ bo‘sh joy talab qilinadi.

Algoritm: *Pohlig-Hellman algoritmi*

Input: *G – siklik guruh, g – generator, a – guruh elementi, N – guruh tartibi*

Output: *$g^x = a$ dan x– darajani topish kerak*

```
1: N = ∏_{i=1}^{k} p_i^{n_i} ning tub ko'paytuvchilarini topish
2: // Har bir p_i^{n_i} uchun x_i ≡ x mod p_i^{n_i} ni topish
3: for i = 1 to k do
4:     z = a
5:     h = g^{-1}
6:     q = (p − 1)/p_i
7:     g_i = g^q
8:     for j = 0 to (n_i − 1) do
9:         w = z^q
10:        b_j = log_{g_i} w   // Shank algoritmi yordamida diskret logarifm yechiladi
11:        z = z h^{b_j}
12:        h = h^{p_i}
13:        q = q/p_i
14:    end for
15:    x_i = Σ_j b_j p_i^j
16: end for
17: // Qoldiqlar haqidagi xitoy teoremasi yordamida x topiladi
18: return x
```

x_i ni topish uchun har bir koeffitsientni, b_j ni $x_i = \sum_{j}^{n_i - 1} b_j p_i^j$ quyidagi ifodadan topamiz. Pohlig-Hellman algoritmidan $b_i = log_{g_i} w$, bu yerda log diskret logorifmdir. Asosiy $g_i = g^{(p-1)/p_i}$, shuning uchun g_i tartibi p_i hisoblanadi. Eng

katta tub bo‘luvchisi p_i bo‘lgan guruh uchun dominant qadam Shank algoritmidan foydalangan holda p_i tartibli kichik guruhida diskret logorifmni topish bo‘ladi.

Kichik p_i uchun diskret logorifmlarni oldindan hisoblangan jadvallar yordamida yechish mumkin. Barcha p_i N ga nisbatan kichik bo‘lgan holatda, algoritmning dominant bosqichi $w = z^n$ ni hisoblash bo‘lib, $O(\log N)$ guruh operatsiyalarini talab qiladi. z^n necha marta hisoblash kerak bo‘lsa, $\sum_1^k n_i$, bu tub bo‘luvchilar kichik bo‘lganda $O(\log N)$ bo‘ladi. Bu $O(\log N)^2$ yoki $O(n^2)$ ning umumiy ish vaqtini beradi.

Pollardning Rho algoritmi. Bu Pollardning Rho algoritmi Shank algoritmi bilan bir xil tartibda ishlash vaqtiga ega, ammo bu algoritm eng katta saqlangan jadvaldan qochadi. Rho algoritmi *birthday paradox* (tug‘ilgan kun paradoksi) dan foydalanadi; Ya’ni tasodifiy tanlangan 23 kishidan 2 nafari tug‘ilgan kunini baham ko‘rish ehtimoli 50% dan yuqori. Umuman olganda, elementlarni N ta elementdan tasodifiy tanlaganda, to‘qnashuv kutilgan $\sqrt{\pi N/2}$ tanlanganidan keyin topiladi.

a elementining g asosiga diskret logorifmini topish uchun Pollardning Rho algoritmi a va g darajalarining hosilasi sifatida ifodalanishi mumkin bo‘lgan s^i guruh elementlarining tasodifiy ketma-ketligidan o‘tadi.

$$s_i = a^{a_i} g^{g_i} = g^{xa_i} g^{g_i} = g^{xa_i + g_i}$$

Algoritm ketma-ketlikda sikldan qidiradi, ikkita element s_u, s_v, $u \neq v$ shuning uchun $s_u = s_v$. Bu tenglamani x uchun yechish a ning diskret logorifmini beradi.

$$s_u = s_v$$
$$g^{xa_u + g_u} = g^{xa_v + g_v}$$
$$xa_u + g_u \equiv xa_v + g_v \mod N$$
$$xa_u - xa_v \equiv g_v - g_u \mod N$$
$$x(a_u - a_{v)}) \equiv g_v - g_u \mod N$$
$$x \equiv (a_u - a_{v)})^{-1} g_v - g_u \mod N$$

Ishlash vaqti ketma-ketlikda sikldan qidirish bilan ustunlik qiladi. Sikldan topish har bir elementni ketma-ketlikda bitta takrorlanmaguncha saqlash orqali amalga oshirilishi mumkin. Bu katta hajmdagi saqlashni talab qiladi, uning o‘rniga Pollard *Floyd siklini aniqlash* algoritmidan foydalanadi, bu esa atigi ikkita ketma-ketlik elementini saqlashni talab qiladi s_i va s_{2i}. s_{2i} elementi har doim ketma-ketlikda s_i dan ikki barobar uzoqroq bo‘ladi va $s_i = s_{2i}$ bo‘lganda sikl topiladi. Ikkala ketma-ketlikni oldinga siljitish uchun algoritmning bir bosqichi ketma-ketlikning jami uchta bosqichini talab qiladi. Pollardning hisob-kitoblari i uchun $1.08\sqrt{N}$ o‘rtacha qiymatini berdi. Asimptotik ish vaqti $O(2^{\frac{n}{2}})$ guruh operatsiyalari va faqat $O(n)$ ni saqlashdir.

Pollardning Rho algoritmi Oorschot va Wiener tufayli Pollardning Rho metodining takomillashtirilgan versiyasidir. Ularning usuli siklni ketma-ketliklar bo‘ylab faqat bir marta bosib o‘tish orqali topadi, bu 3 marta tezlashtirishni ta’minlaydi. Bu mumkin, chunki ular alohida nuqtalarni saqlaydi. Ajratilgan nuqtalar – oson ajratiladigan xususiyatga ega bo‘lgan guruh elementlari, masalan, ularning ikkilik tasvirining birinchi c bitlari nolga teng bo‘lgan elementlar. Biz

tasodifiy joydan boshlaymiz va aniq nuqtaga yetgunimizcha ketma-ketlikni bosib o‘tamiz. Biz ajratilgan nuqtani saqlaymiz va yangi tasodifiy joydan qayta boshlaymiz. Biz allaqachon saqlagan muhim nuqtaga erishganimizda, biz siklni topdik va logorifmni hal qila olamiz.

Algoritm: *Pollardning Rho algoritmi*

Input: *G – siklik guruh, g – generator, a – guruh elementi, g ning tartibi: N*

Output: $g^x = a$ *dan x– darajani topish kerak*

1: // *Tasodifiy ketma-ketliklar algoritmi bilan aniqlangan* $S = s_0, s_1, \ldots$ *tasodifiy ketma-ketlikda sikldan qidirish*
2: $success =$ **false**
3: $D = G$ *dan ajratilgan nuqtalar to'plami*
4: **while** $(success =$ **false**$)$ **do**
5: $\quad i = 0$
6: $\quad a_i =$ *(0 va* $p-1$ *oralig'ida tasodifiy tanlangan ko'rsatkich)*
7: $\quad g_i =$ *(0 va* $p-1$ *oralig'ida tasodifiy tanlangan ko'rsatkich)*
8: $\quad s_i = g^{g_i} a^{a_i}$
9: $\quad$ **repeat**
10: $\quad\quad i = i + 1$
11: $\quad\quad$ *Tasodifiy ketma-ketliklar algoritmini qo'llab* s_i, a_i, g_i ni hisoblang
12: $\quad$ **until** $(s_i \in D)$
13: $\quad$ **if** $\left((a_j, g_j) = hash(s_i)\right)$ then
14: $\quad\quad success =$ **false**
15: $\quad$ **else**
16: $\quad\quad hash(s_i) = (a_j, g_j)$
17: $\quad$ **end if**
18: **end while**
19: $m = a_i - a_j \mod N$ 20: $x = m^{-1}(g_j - g_i) \mod N$ 21: **return** x

Algoritm: *Pollardning Rho – Tasodifiy ketma-ketlik algoritmi*

Input: *element:* s_i, *ko'rsatkichlar:* a_i, g_i *quyidagi ifodadan* $s_i = a^{a_i} g^{g_i}$

Output: *element:* s_{i+1}, *ko'rsatkichlar:* a_{i+1}, g_{i+1} *quyidagi ifodadan* $s_{i+1} = a^{a_{i+1}} g^{g_{i+1}}$

1: // *G ning uchta teng o'lchamdagi* S_1, S_2, S_3 *kichik to'plamlarga bo'linishi berilgan*
2: **if** $s_i \in S_1$ **then**
3: $s_{i+1} = as_i$
4: $a_{i+1} = a_i + 1 \mod N$
5: $g_{i+1} = g_i$
6: **else if** $s_i \in S_2$ **then**
7: $s_{i+1} = {s_i}^2$
8: $a_{i+1} = 2a_i \mod N$
9: $g_{i+1} = 2g_i \mod N$
10: **else if** $s_i \in S_3$ **then**
11: $s_{i+1} = gs_i$
12: $a_{i+1} = a_i$
13: $g_{i+1} = g_i + 1 \mod N$
14: **end if**
15: **return** $s_{i+1}, a_{i+1}, g_{i+1}$

Rho algoritmining ushbu versiyasining ishlash vaqti to‘qnashuvni topish uchun vaqt yig‘indisi, T_c, shuningdek, ajratilgan nuqtaga yetib borish vaqti, T_d. Agar ketma-ketlikni tasodifiy xaritalash deb faraz qilsak, u holda to‘qnashuvning kutilgan vaqti $T_c = \sqrt{\pi N/2}$ bo‘ladi. Belgilangan nuqtaga erishish vaqti ajratilgan nuqtalarning chastotasiga bog‘liq. Ba’zi doimiy $c \gg 1$ uchun guruhda $c\sqrt{N}$ farqlangan nuqtalar mavjudligini hisobga olsak, har bir $\frac{N}{c\sqrt{N}} = \frac{\sqrt{N}}{c}$ elementdan biri ajratilgan nuqta hisoblanadi. Ketma-ketlik kutilgan $T_c = \frac{\sqrt{N}}{c}$ qadamlardan keyin ajralib turadigan nuqtaga yetadi. Rho algoritmining umumiy kutilgan ishlash vaqti

$$T_c + T_d = \sqrt{\frac{\pi N}{2}} + \frac{\sqrt{N}}{c} = \left(\sqrt{\frac{\pi}{2}} + \frac{1}{c}\right)\sqrt{N} \approx \sqrt{\frac{\pi N}{2}}.$$

Bit uzunligi n bo‘yicha asimptotik ish vaqti $O\left(2^{\frac{n}{2}}\right)$ ga teng.

Index calculus algoritmi. Bu algoritm, $O\big(\exp\big((sqrt(\log p) * \log\log p)\big)\big)$ vaqtni talab qiladi. Bu algoritm, qaralayotgan modulni faktorlashtirishga asoslangan, shuning uchun ham, jarayon ancha uzun va qiyin.

Number Field Sieve algoritmi. Bu algoritm, $O\big(\exp\big((sqrt(\log p / \log\log p) * \log\log p)\big)\big)$ vaqtni talab qiladi. Bu algoritmning shaxsiy qurilishi, yomon foydalanuvchilarga o‘z kalitlarini yaratish uchun yaxshi xizmat qiladi, chunki katta vaqt talab qiladi.

Adleman-Pomerance-Rumely algorithm. Bu algoritm, 200 bitdan kichik sonlarda muammoni hal qilish uchun yaxshi natija olish mumkim, ammo 200 bitdan katta sonlarda yaxshi samara bermaydi.

Yuqorida sanab o‘tilgan algoritmlar ichida brute force algoritmidan tashqari hech birida, berilgan har qanday diskret logorifmlash muammosining aniq bir yechimini topish amaliy jihatdan mumkin emas. Chunki, har bir taklif qilingan algoritm uchun qo‘yilgan talablar mavjud, masalan qaysidir algoritm faqatgina kichikroq modullar uchun samarali hisoblansa, ayrimlari qaralayotgan modullarni faktorlash bilan bog‘liq shartlar kiritilgan.

Amaliy bajarish uchun vazifalar

1. Faktorlash muammosini yechishning eksponensial algoritmlarini amalga oshirish
2. Faktorlash muammosini yechishning sub-eksponensial algoritmlarini amalga oshirish
3. Chekli maydonda diskret logorifmlash masalasini yechish algoritmlarini amalga oshirish

Adabiyot va Internet saytlar:

4. Шеннон К. Теория и связи в секретных системах. Работы по теории информации и кибернетике. – М.: Иностранная лит. 1963. – 243 б.
5. Авдошин С.М., Савельева А.А. «Криптоанализ: вчера, сегодня, завтра», Государственный университет – Высшая Школа Экономики. Москва – 2007.
6. Авдошин С.М., Савельева А.А. «Криптоанализ: савременное состояние и перспективы развития», Государственный университет – Высшая Школа Экономики.

5-amaliy ish. Xesh funksiyalarning kriptotahlili, Psevdotasodifiy va tasodifiy sonlar generatorlarining tahlilli. Tug‘ilgan kun muammosi, MD4 va MD5 algoritmlarining kriptotahlili. NIST va DIEHARD statistik testlar to‘plami. (2 soat)

Amaliy ishning maqsadi – *Xesh funksiyalarning kriptotahlili, Psevdotasodifiy va tasodifiy sonlar generatorlarining tahlilli. Tug‘ilgan kun muammosi, MD4 va MD5 algoritmlarining kriptotahlili, NIST va DIEHARD statistik testlar to‘plami bo‘yicha bilim va ko‘nikmalarga ega bo‘lish.*

Nazariy qism

MD4 algoritmiga kolliziya hujumi

MD4 algoritmiga kolliziya hujumini 2^{-2} dan 2^{-6} gacha imkoniyatda muvaffaqiyatli amalga oshirish imkoniyati mavjud. Bunda hisoblash murakkabligi 2^8 dan past. Hujum uch qismdan iborat:

1. M va M’ xabarlar uchun kolliziya hosil qiladigan differensial topiladi;

2. Kolliziya differensialini saqlab turishni ta'minlaydigan yetarli

shartlar to'plami ishlab chiqiladi;

3. Har qanday tasodifiy M xabari uchun yuqoridagi shartlar bajarilguncha M ga o'zgartirish kiritib boriladi.

MD4 algoritmi uchun kolliziya differensiali

MD4 algoritmi uchun kolliziya differensiali quyidagicha tanlanadi:

$$\Delta H_0 = 0 \left(\xrightarrow{(M,M')}\right) \Delta H = 0$$

Shu kabi

$$\Delta M = M' - M = (\Delta m_0, \Delta m_1, \ldots., \Delta m_{15})$$

$$\Delta m_1 = 2^{31}, \Delta m_2 = 2^{31} - 2^{28}, \Delta m_{12} = -2^{16}$$

$$\Delta m_i = 0, 0 \leq i \leq 15, i \neq 1,2,12.$$

Kolliziya differensialidagi barcha xususiyatlarni 6.4-jadvalda topish mumkin. Birinchi ustun qadamni bildiradi, ikkinchi ustun M uchun har bir qadamdagi zanjirli o'zgaruvchisi, uchinchisi - har bir qadamda M uchun xabar so'zi, to'rtinchisi – siljish sikli, beshinchi va oltinchi ustunlar - mos ravishda M va M' ma’lumotlari differensiali, yettinchisi esa M' uchun zanjirli o'zgaruvchidir. Ayniqsa, beshinchi va oltinchi ustunlardagi bo'sh elementlar nol farqlarni bildiradi va jadvalda ko'rsatilmagan qadamlar xabar so'zlari va zanjirli o'zgaruvchilar uchun nolga teng differensialga ega.

Ko'rinib turibdiki, kolliziya differensiallari mos ravishda 2-25 qadam va 36-41 bosqichli ikkita ichki moslikdan iborat.

Barcha xususiyatlarni ushlab turishni ta'minlaydigan yetarli shartlar 6.5-jadvalda keltirilgan mantiqiy funktsiyalarning xususiyatlari bilan osongina tekshirilishi mumkin. Bu shuni anglatadiki, agar M 6.5-jadvaldagi barcha shartlarni qanoatlantirsa, M va M' ma’lumotlarning kolliziya qiymatlari topilgan bo’ladi.

Quyida 6.4-jadvalning 9-bosqichidagi yetarlilik shartlarining natijasi keltirilgan. 9-bosqichdagi differensial xarakteristika:

$$(b_2[-13, -14,15], c_2[19,20, -21], d_2[14], a_2)$$

$$\rightarrow (a_3[17], b_2[-13, -14,15], c_2[19,20, -21,22], d_2[14])$$

1. 1-taklifga binoan, $c_{2,13}= d_{2,13}$ va $c_{2,15}= d_{2,15}$ shartlar b_2 dagi 13 va 15-bitlardagi o'zgarishlar hech qanday o'zgarishga olib kelmasligini ta'minlaydi.
2. 1-taklifga binoan, $b_{2,19} = 0$, $b_{2,20} = 0$, $b_{2,21} = 0$ va $b_{2,22} = 0$ shartlar 19-chi, 20-bandlardagi o'zgarishlarni ta'minlaydi. c_2 ning , 19-, 21- va 22-bitlari a_3 ning o'zgarishiga olib kelmaydi.

6.4- jadval

MD4 algoritmi uchun kolliziya differensialidagi xarakteristikalar

Qadam	**M uchun zanjirli qiymat**	$W_{j,i}$	**Siljish**	Δm_i	***i*-bosqichdagi differensial**	***M'* uchun *i*-chi chiqish**
1	a_1	m_0	3			a_1
2	d_1	m_1	7	2^{31}	2^6	d_1[7]
3	c_1	m_2	11	$-2^{28}+2^{31}$	-2^7+2^{10}	c_1[-8,11]
4	b_1	m_3	19		2^{25}	b_1[26]
5	a_2	m_4	3			a_2
6	d_2	m_5	7		2^{13}	d_2 [14]
7	c_2	m_6	11		$-2^{18}+2^{21}$	c_2[19,20-21,22]
8	b_2	m_7	19		2^{12}	b_2[-13,-14,15]
9	a_3	m_8	3		2^{16}	a_3 [17]
10	d_3	m_9	7		$2^{19}+2^{20}-2^{25}$	d_3[20,-21,-22,23-26]
11	c_3	m_{10}	11		-2^{29}	c_3[-30]
12	b_3	m_{11}	19		2^{31}	b_3[32]
13	a_4	m_{12}	3	-2^{16}	$2^{22}+2^{25}$	a_4[23,26]
14	d_4	m_{13}	7		$-2^{26}+2^{28}$	d_4[-27,-29,30]
15	c_4	m_{14}	11			c_4
16	b_4	m_{15}	19		2^{18}	b_{14}[19]
17	a_5	m_0	3		$2^{25}-2^{28}-2^{31}$	a_5[-26,27,-29,-32]
18	d_5	m_4	5			d_5
19	c_5	m_8	9			c_5

Qadam	M uchun zanjirli qiymat	$W_{j,i}$	Siljish	Δm_i	i-bosqichdagi differensial	M' uchun i-chi chiqish
20	b_5	m_{12}	13	-2^{16}	$-2^{29}+2^{31}$	b_5[-30,32]
21	a_6	m_1	3	2^{31}	$2^{28}-2^{31}$	a_6[-29,30,-32]
22	d_6	m_5	5			d_6
23	c_6	m_9	9			c_6
24	b_6	m_{13}	13			b_6
25	a_7	m_2	3	$-2^{28}+2^{31}$		a_7
…	…					…….
36	b_9	m_{12}	15	-2^{16}	2^{31}	b_9[-32]
37	a_{10}	m_2	3	$-2^{28}+2^{31}$	2^{31}	a_{10}[-32]
38	d_{10}	m_{10}	9			d_{10}
39	c_{10}	m_6	11			c_{10}
40	b_{10}	m_{14}	15			b_{10}
41	a_{11}	m_1	3	2^{31}		a_{11}

3. f funksiyaning xossasidan $b_{2,14} = 1$, $d_{2,14} = 0$ va $c_{2,14}$=0 shartlar f($b_{2,14}, d_{2,14}, c_{2,14}$) = 0 ni hosil qiladi. va f($\neg b_{2,14}$, $c_{2,14}$, $\neg d_{2,14}$) = 1. Demak, $\Delta a_3 = 2^{16}$.

4. $a_{3,17} = 0$ sharti $a'_3 = a_3$ bo'lishini ta'minlaydi.

Shunday qilib, yuqoridagi 10 ta shart 9-bosqichdagi differensial xarakteristikalar uchun yetarli shartlar to'plamidan iborat bo'ladi va MD4 algoritmi uchun kolliziya hujumini ifodalaydi.

6.5-jadval

MD4 algoritmida kolliziya uchun yetarlilik shartlar to'plami

a_1	$a_{1,7} = b_{0,7}$
d_1	$d_{1,7} = 0$, $d_{1,8} = a_{1,8} = 1$, $c_{1,11} = a_{1,11}$
c_1	$c_{1,7} = 1$, $c_{1,8} = 1$, $a_{1,8} = 1$, $c_{1,11} = 0$, $c_{1,26} = d_{1,26}$
b_1	$b_{1,7} = 1$, $b_{1,8} = 0$, $b_{1,11} = 0$, $b_{1,26} = 0$
a_2	$a_{2,8} = 1$, $a_{2,11} = 1$, $a_{2,26} = 0$, $a_{2,14} = b_{1,14}$
d_2	$d_{2,14} = 0$, $d_{2,19} = a_{2,19}$, $d_{2,20} = a_{2,20}$, $d_{2,22} = a_{2,21} = d_{2,22} = a_{2,22}$, $d_{2,22}$

	$= 1$
c_2	$c_{2,13} = d_{2,13}, c_{2,13,} = 0 \quad c_{2,15} = d_{2,15,} c_{2,19} = 0, c_{2,20} = 0, c_{2,21} = 1, c_{2,22} = 0$
b_2	$b_{2,13} = 0, \ b_{2,14,} = 1 \ b_{2,15,} = 0, b_{2,17,} c_{2,17,} \ b_{2,19,} = 0, b_{2,20} = 0, b_{2,21,} = 0, b_{2,22,} = 0,$
a_3	$a_{3,13} = 1, \ a_{3,14} = 1 \ a_{3,15} = 1, a_{3,17} = 0, a_{3,19} = 0, \ a_{3,20} = 0, b_{3,20} = 0, a_{3,21} = 0, a_{3,23,} = \ b_{2,23} a_{3,22} = 1, a_{3,26} = b_{2,26}$
d_3	$d_{3,13} = 1, \ d_{3,14} = 1, \ d_{3,15} = 1, d_{3,17} = 0, d_{3,20} = 0, \ d_{3,21} = 1, d_{3,22} = 1, d_{3,23} = 0, d_{3,26} = 1, d_{3,26} = 1, d_{3,30} = a_{3,30}$
c_3	$c_{3,17} = 1, \ c_{3,20} = 0, c_{3,21} = 0, \ c_{3,22} = 0, \ c_{3,23} = 0, c_{3,26} = 0, c_{3,30} = 1, c_{3,32,} \ c_{3,32} = d_{3,32}$
b_3	$b_{3,20} = 0, \ b_{3,21} = 1, b_{3,22} = 1, \ b_{3,23,} = c_{3,23,} \ b_{3,26} = 1, b_{3,30} = 0, \ b_{3,32} = 0$
a_4	$a_{4,23} = 0, \ a_{4,26} = 0, \ a_{4,27} = b_{3,27,} a_{4,29} = b_{3,29,} \ a_{4,30} = 1, a_{4,32} = 0,$
d_4	$d_{4,23} = 0, \ d_{4,26} = 0, \ d_{4,27} = 1, d_{4,29} = 1, d_{4,30} = 0, \ d_{4,32} = 1,$
c_4	$C_{4,19} = d_{4,19}, \ c_{4,23} = 1, c_{4,26} = 1, c_{4,27} = 0, \ c_{4,29} = 0, c_{4,30} = 0,$
b_4	$b_{4,19} = 0, \ b_{4,26} = c_{4,26} = 1, b_{4,27} = 1, \ b_{4,29} = 1, b_{4,30} = 0,$
a_5	$a_{5,19} = c_{4,19}, \ a_{5,26} = 1, a_{5,27} = 1, \ a_{5,29} = 1, a_{5,32} = 1,$
d_5	$d_{5,19} = a_{5,19}, \ d_{5,26} = b_{4,26,} \ d_{5,27} = b_{4,27}, \ d_{5,29} = b_{4,29}, \ d_{5,32} = b_{4,32}, $
c_5	$c_{5,26} = d_{5,26}, \ c_{5,27} = d_{5,27,} \ c_{5,29} = d_{5,29}, \ c_{5,30} = d_{5,30}, \ c_{5,32} = d_{5,32}$,
b_5	$b_{5,29} = c_{5,29}, \ b_{5,30} = 1, b_{5,32} = 0,$
a_6	$a_{6,29} = 1, \ a_{6,32} = 1,$
d_6	$d_{6,29} = b_{5,29}, $
c_6	$c_{6,29} = d_{6,29}, \ c_{6,30} = d_{6,30} + 1, c_{6,32} = d_{6,22} + 1,$
b_9	$b_{9,32} = 1$
a_{10}	$a_{10,32} = 1$

Axborot xavfsizligida tasodifiy sonlar generatoridan hosil bo‘lgan ketma-ketliklarni tasodifiylik darajasini tekshirish uchun mos aniqlash usuli mavjud bo‘lishi zarur. Hozirgi kunda tadqiqotchilar tomonidan qurilmaga yoki dasturiy ta’minotga asoslangan yangi tasodifiy sonlar generatorlari ishlab chiqilmoqda. Biroq, ulardan hosil bo‘lgan tasodifiy qiymatlarga baho bermasdan turib, ularni amalga foydalanish tavsiya etilmaydi.

Tasodifiy sonlar generatoridan hosil bo‘lgan qiymatlarni statistik testlash usullari asosida testlash amalga keng foydalanilib, odatda

quyidagi turdagi statistik testlar to‘plamidan keng qo‘llaniladi (5.1-jadval).

5.1-jadval

Statistik testlar to‘plami va ularning xususiyatlari

№	Manba/ muallif	Testlar to‘plami nomi	To‘plam-dagi testlar soni
7.	Donald Knuth/ Stanford University	The Art Of Computer Programming Vol. 2 Seminumerical Algorithms	11 ta
8.	George Marsaglia/Florida State University	DIEHARD	15 ta
9.	Helen Gustafson, et. al./ Queensland University of Technology	Crypt-XS	6 ta
10	Alfred Menezes, et. al./CRC Press, Inc.	Handbook of Applied Cryptography	
11	Pierre L’Ecuyer, Richard Simard/ Université de Montréal	TestU01’s test batteries	SmallCrush (10) Crush (96 ta) BigCrush (106 ta)
12	Andrew Rukhin, et. al./NIST ITL	NIST Statistical Test Suite	15 ta

Donald Knut tomonidan yozilgan “The Art of Computer Programming, Seminumerical Algorithms, Volume 2” nomli kitobda, muallif qator emperik testlarni keltirib o‘tgan. Jumladan, *chastota* (frequency), *ketma-ketlik* (serial), *oraliq* (gap), *poker* (poker), *kupon to‘plovchi* (coupon collector's), *o‘rin almashtirish* (permutation), *yugirish* (run), *t ning maksimumi* (maximum-of-t), *kolliziya* (collision), *tug‘ulgan kun oralig‘i* (birthday spacings) va *ketma-ketlik korrelasiyasi* (serial correlation) testlar.

DIAHARD testlar to‘plami Djorj Marsaliya tomonidan ishlab chiqilgan bo‘lib, 15 ta statistik testlardan: *tug‘ulgan kun oralig‘i* (birthday spacings), *bog‘liqlikni almashtirish* (overlapping permutations), *matrisa*

rangini o‘lchash (ranks of 31x31, 32x32, 6x8 matrices), *“20-bitli so‘zda maymun” testi* (monkey tests on 20-bit Words, monkey tests OPSO), *OQSO, DNA, ketma-ketlikdagi birlar sonini aniqlash* (count the 1's in a stream of bytes), *maxsus baytdagi birlar sonini aniqlash* (count the 1's in specific bytes), “avtostoyanka” (parking lot), *minimal distansiya* (minimum distance), *tasodifiy sferalar* (random spheres), *siqish* (squeeze), *bog‘liqliklar yig‘indisi* (overlapping sums), *yugurish* (runs) va *kraps* (craps) iborat.

Crypt-XS statistik testlar to‘plami Avstraliyadagi Kvinslend Texnologiyalar universitetining Axborot xavfsizligi tadqiqotlar markazidagi tadqiqotchilar tomonidan ishlab chiqilgan va u *chastota* (frequency), *binar hosila* (binary derivative), *nuqtalarni almashtirish* (change point), *yugirishlar* (runs), *ketma-ketlik murakkabligi* (sequence complexity) va *chiziqli murakkablik* (linear complexity) testlaridan iborat bo‘lgan.

NIST statistik testlar to‘plami (NIST Statistical Test Suite) NIST institutining Kompyuter xavfsizligi va Statistik injineriya bo‘limlari tomonidan ishlab chiqilgan. Ushbu to‘plam o‘zida 15 ta statistik testlarni mujassamlashtirgan:

16. Chastota (Frequency) testi;
17. Bloklar uchun chastota (Frequency Test within a Block) testi;
18. Yugurishlar (Runs) testi;
19. Blok ichidagi eng uzun yugurish (Longest Run of Ones in a Block) testi;
20. Birlik matrisa rangini hisoblash (Binary Matrix Rank) testi;
21. Diskret Furye almashtirishlari (Discrete Fourier Transform) testi;
22. Davriy bo‘lmagan qismlar (Non-overlapping Template Matching) testi;
23. Davriy bo‘lgan qismlar (Overlapping Template Matching) testi;
24. Maurerning «Universal statistik» (Maurer’s «Universal Statistical») testi;
25. Chiziqli murakkablik (Linear Complexity) testi;
26. Davomiylik (Serial) testi;
27. Taxminiy entropiya (Approximate Entropy) testi;
28. Ortib boruvchi yig‘indi (Cumulative Sums) testi;
29. Tasodifiy tashriflar (Random Excursions) testi;
30. Tasodifiy tashriflar varianti (Random Excursions Variant) testi.

Quyida NIST statistik testlar to‘plami bilan yaqindan tanishib chiqiladi. Mazkur testlar to‘plami yordamida yagona tasodifiy qiymatni

tasodifiylikka tekshirish ketma-ketligi 5.2-jadvalda aks ettirilgan. Ushbu ketma-ketlik umumiy testlash senariysini aks ettirgan bo‘lib, NIST statistik testlar to‘plamidan foydalanib testlashda muhim ahamiyatga ega.

5.2-jadval

Yagona binar ketma-ketlikni baholash muolajasi

Qadam va qadam jarayon	**Izoh**
Sizning nollik gipoteza holatingiz	Binar ketma-ketlikni tasodifiy deb faraz qiling
Statistik testlar ketma-ketligini amalga oshirish	Testlash bitlar kesimida amalga oshiriladi
P – qiymatni hisoblash	$P \in [0,1]$ ga tegishli
P – qiymatni α ga solishtirish	$\alpha \in (0.001,0.01]$ kabi kelgilang. Agar $P \geq \alpha$ bo‘lsa, testdan o‘tgan, aks holda o‘ta olmagan

Mazkur testlash to‘plamida kiritilgan har bir test usuli aynan bir maqsadga qaratilgan bo‘lib, aynan bir holat bo‘yicha baho beradi. Quyidagi 5.3-jadvalda har bir testning maqsadi va baho beruvchi asosiy zaiflik tomoni aks ettirilgan.

5.3-jadval

NIST statistik testlar to‘plamining xususiyatlari

№	**Statistik test**	**Zaiflikni aniqlash**
15.	Frequency	Bir yoki nolni juda ko‘pligini
16.	Cumulative Sums	Ketma-ketlik boshlanishida bir yoki nolni juda ko‘pligini
17.	Longest Runs Of Ones	Birlarni uzoq vaqtli davomiyligi taqsimotining og‘ishini
18.	Runs	Bitlar ketma-ketligida tezkor (sekin) birdan nolga va aksincha o‘tishlarni ko‘rsatuvchi yugirishlarning umumiy katta (kichik) sonini
19.	Rank	Mos tasodifiy ketma-ketlikdan qism takroriyligi natijasidagi rang taqsimotini og‘ishini
20.	Spectral	Bitlar ketma-ketligidagi takrorlanish xususiyatini
21.	Non-overlapping Template Matchings	Kesishmagan shablonlarni qanchalik ko‘p paydo bo‘lishini
22.	Overlapping	Birlarning m bitli yugirishlarni paydo

№	Statistik test	Zaiflikni aniqlash
	Template Matchings	bo‘lishini
23.	Universal Statistical	Siqilishni (biror qoniniyatga asoslanishini)
24.	Random Excursions	Tasodifiy yurishda yagona holatga o‘tishlar sonini taqsimotining og‘ishini
25.	Random Excursion Variant	Yagona holatga turli holatlardan o‘tishlarning umumiy soni taqsimotining og‘ishini
26.	Approximate Entropy	*m* bit uzunlikdagi so‘zlar taqsimotining bir xil emasligini.
27.	Serial	*m* bit uzunlikdagi so‘zlar taqsimotining bir xil emasligini. Approximate Entropyga o‘xshash
28.	Linear Complexity	Cheklangan uzunlikdagi (qism) qator uchun chiziqli murakkablikning taqsimotidan og‘ishini

Har bir testni amalga oshirish uchun unga talab etilgan uzunlikdagi tasodifiy qiymat kiritilishi talab etiladi. NIST tomonidan keltirilgan har bir test uchun kiritiladigan tasodifiy qiymatlarga minimal uzunlik talabi qo‘yilgan (5.4-jadval).

5.4-jadval

NIST statistik testlariga kirish qiymatlariga uzunlik talabi

№	Statistik test	Minimal kirish qiymat uzunligi (bit)
16.	Chastota (Frequency) testi	100
17.	Bloklar uchun chastota (Frequency Test within a Block) testi	100
18.	Yugurishlar (Runs) testi	100
19.	Blok ichidagi eng uzun yugurish (Longest Run of Ones in a Block) testi	128
20.	Birlik matrisa rangini hisoblash (Binary Matrix Rank) testi	38912
21.	Diskret Furye almashtirishlari (Discrete Fourier Transform) testi	1000
22.	Davriy bo‘lmagan qismlar (Non-overlapping Template Matching) testi	10^6
23.	Davriy bo‘lgan qismlar (Overlapping Template Matching) testi	10^6

№	Statistik test	Minimal kirish qiymat uzunligi (bit)
24.	Maurerning «Universal statistik» (Maurer's «Universal Statistical») testi	387840
25.	Chiziqli murakkablik (Linear Complexity) testi	10^6
26.	Davomiylik (Serial) testi	128
27.	Taxminiy entropiya (Approximate Entropy) testi	100
28.	Ortib boruvchi yig'indi (Cumulative Sums) testi	100
29.	Tasodifiy tashriflar (Random Excursions) testi	10^6
30.	Tasodifiy tashriflar varianti (Random Excursions Variant) testi	10^6

Tasodifiy ketma-ketliklar entropiyasini o'lchash usullari. Generasiya qilingan psevdotasodifiy ketma-ketliklarni statistik testlar orqali tekshirish bilan har doim ham ularga aniq baho berib bo'lmaydi. Kalitlarni tasodifiy darajasini tekshirishda odatda ularning entropiya qiymatini o'lchash muhim ahamiyat kasb etadi.

NIST SP 800-90B nashridagi entropiyani o'lchash usuli. Ushbu nashrda *min-Entropy – minimal entropiya* usuli keltirilgan bo'lib, uning ketma-ketligi quyidagicha:

7. Tasodifiy sonlar generatoridan hosil qilingan ketma-ketliklar ma'lum bloklarga ajratilib, to'plam shaklida ifodalanadi. Bunda agar blok uchunligi n bit bo'lsa, to'plamdagi bloklar soni N kamida 2^n ga teng bo'lishi zarur.

8. To'plam ichida eng ko'p takrorlangan qiymat C_{max} ga o'zlashtiriladi.

9. Ushbu qiymat uchun ehtimollik $p_{max} = {C_{max}}/{N}$ ga teng bo'ladi.

10. Chegara qiymat $C_{chegara} = C_{max} + 2.3\sqrt{N * p_{max}(1 - p_{max})}$ tenglik orqali hisoblanadi.

11. Chegara qiymat uchun entropiya $H = -\log_2({C_{chegara}}/{N})$ tenglik orqali hisoblanadi.

12. Yakuniy minimal − entropiya = $\min(n, H)$ ga ya'ni, ikki qiymatning eng kichigiga teng bo‘ladi.

/dev/random generatorida entropiyani o‘lchash. Ushbu algoritmda muallif tomonidan isbotga ega bo‘lmagan quyidagi entropiyani hisoblash tengligidan foydalanilgan:

$$\Delta_n^1 = time_n - time_{n-1},$$
$$\Delta_n^2 = \Delta_n^1 - \Delta_{n-1}^1,$$
$$\Delta_n^3 = \Delta_n^2 - \Delta_{n-1}^2,$$
$$\Delta_n = \min(|\Delta_n^1|, |\Delta_n^2|, |\Delta_n^3|),$$
$$entropy_n = log_2(\left[\frac{\Delta_n}{2}\right] (mod\ 2^{12})).$$

$time_n$ o‘zgaruvchisi biror manbadagi tashqi hodisani vaqt belgisini ifodalaydi. Har bir manba o‘zining $\{time_n\}_{n\geq 0}$ ketma-ketliklariga ega. $mod\ 2^{12}$ dan foydalanish esa entropiya qiymatini ko‘pi bilan 12 bitga teng bo‘lishini bildiradi.

Yarrow generatorida entropiyani o‘lchash. Mualliflar tomonidan mazkur algoritm uchun entropiyani to‘plash uchun o‘zgacha usuldan foydalanilgan. Har bir hodisalar manbasi uchun alohida entropiyani o‘lchash sanog‘i qo‘yilgan bo‘lib, har bir genetorning ichki holati yangilangandan so‘ng, ular nolga olib kelingan.

Ushbu generatorning keyingi avlodi sanalmish *Fortuna* generatorida esa hodisalar manbasidan kelgan qiymatlarni 32 ta pulga taqsimlangan holda saqlash va ulardan generator ichki holatini yangilashda o‘zgacha usuldan foydalanish orqali entropiyani hisoblashdan qochilgan.

Bundan tashqari entropiyani hisoblashda ko‘plab usullardan foydalanilgan bo‘lib, ular ichida EGD (Entropy Gathering Daemon) entropiya to‘plovchisida foydalanilgan yondashuv muhim ahamiyat kasb etadi. Ushbu yondashuvga ko‘ra manbadan olingan har bir bayt uchun bir bit entropiyaga ega deb faraz qilingan.

Umumiy holda mavjud entropiyani o‘lchash usullarini turli statistik usullarga va farazlarga asoslanilganini yoki uni hisoblashdan qochilganiga ko‘rish mumkin.

Amaliy bajarish uchun vazifalar

1. Xesh funksiyalarga nisbatan kolliziya hujumini amalga oshirish
2. MD4 algoritmiga nisbatan hujumlarni amalga oshirish
3. Psevdotasodifiy sonlar generatorini tasodifiylikka tekshirish

Adabiyot va Internet saytlar:

7. Шеннон К. Теория и связи в секретных системах. Работы по теории информации и кибернетике. – М.: Иностранная лит. 1963. – 243 б.

8. Авдошин С.М., Савельева А.А. «Криптоанализ: вчера, сегодня, завтра», Государственный университет – Высшая Школа Экономики. Москва – 2007.

9. Авдошин С.М., Савельева А.А. «Криптоанализ: савременное состояние и перспективы развития», Государственный университет – Высшая Школа Экономики.

V-BO‘LIM

KEYSLAR BANKI

V. KEYSLAR BANKI

1-keys mavzusi: “RSA shifrini tahlil qilish va hujum strategiyasini ishlab chiqish”

Maqsad: RSA algoritmining ishlash mexanizmini va uning zaif tomonlarini tahlil qilish.

Vaziyat tavsifi: O‘quvchilar RSA algoritmi yordamida shifrlangan matnni deshifrlash uchun hujum strategiyasini ishlab chiqishlari kerak. Faktorlashtirish algoritmlari va hisoblash murakkabligi nazariyasidan foydalanish topshiriladi.

Keys savollari:

1. Berilgan ochiq kalit va shifrlangan ma’lumot yordamida yopiq kalitni toping.
2. Faktorlashtirish usullaridan birini tanlab, izohlang.
3. Natijani tahlil qilib, RSA algoritmini kuchaytirish bo‘yicha takliflar bering.

№	*Nomi*	*natija*	*Izoh*
1			
2			
3			

1) Keysdagi muammoni keltirib chiqargan asosiy sabablarni va ularning oqibatlarini belgilang.

№	Sabab	Oqibat
1		
2		

2) Maqsad, kutiladigan natijalar, vaqt oraliqlari kabi parametrlar bo‘yicha muammoni bartaraf etish chora tadbirlarini ishlab chiqing.

2-keys mavzusi: “Tug‘ilgan kun paradoksini qo‘llab, xesh funksiya tahlili”

Maqsad: Xesh funksiyalari zaifliklarini aniqlash va ulardan foydalanish usullarini tushuntirish.

Vaziyat tavsifi: Tinglovchilarga xesh funksiya natijalari va tug‘ilgan kun paradoksiga asoslangan qoidalar beriladi. Maqsad - xesh qiymatlari bir xil bo‘lish ehtimolini hisoblash.

Keys savollari:

1) Berilgan xesh qiymatlari ichidan ikki xil ma’lumot uchun bir xil xesh qiymatini toping.
2) Tug‘ilgan kun paradoksining matematik asoslarini tushuntiring.
3) Xesh funksiyalari xavfsizligini oshirish bo‘yicha takliflar bering.

№	*Misol*	*Natijasi*	*Izoh*
1			
2			
3			
4			
5			

4) Tug’ilgan kun paradoksi usulidan foydalanish konsepsiyasini ishlab chiqish.
5) Xesh funksiyalarni ushbu hujum usuliga bardoshli qilish uchun berilgan tavsilarni sanab bering..

3-keys mavzusi: “Klassik shifrlarni sodda usullar bilan buzish”

Maqsad: Klassik shifrlarning (masalan, Sezar shifri, Vigenere shifri) ishlash mexanizmini tushunish va ularni kriptotahlil qilish.

Senariy: Bir guruh shifrlangan xabarlar Sezar shifri bilan kodlangan. Ushbu xabarlarni deshifrlash uchun shifrning kalitini topish talab etiladi. O‘quvchilarga shifrlangan matn va alohida shifrlar bo‘yicha qo‘llanma beriladi.

Topshiriq:

1. Sezar shifrida foydalanilgan kalitni toping va shifrlangan xabarni oching.
2. Vigenere shifri uchun kalit uzunligini aniqlang va shifrni deshifrlang.
3. Shifrlarning himoyalanganligi haqida qisqa tahlil yozing va zamonaviy algoritmlar bilan solishtiring.

Resurslar: Shifrlangan matnlar, ochiq matnlar va Sezar/Vigenere shifrlarining tavsifi.

Muammo yechimi: Sezar shifrida kalitni brutforce (hamma ehtimoliy kalitlarni sinash) usuli bilan topish, Vigenere shifri uchun Kasiski testi yoki chastota tahlilini qo‘llash.

4-keys mavzusi: “MD5 xesh funksiyasining zaifliklarini tahlil qilish”

Maqsad: MD5 algoritmining zaif tomonlarini aniqlash va bu zaifliklardan foydalanib, kolliziyalarni topish.

Stsenariy: O‘quvchilarga turli ma’lumotlarning MD5 xesh qiymatlari taqdim etiladi. Maqsad - ikki xil ma’lumot uchun bir xil xesh qiymatini topish (kolliziya) va buni amalda qo‘llash usulini tahlil qilish.

Topshiriq:

1. Berilgan xesh qiymatlari orasidan ikki xil ma’lumot uchun bir xil xesh qiymatini toping.
2. MD5 funksiyasining zaif tomonlarini tahlil qiling.
3. Xesh funksiyasining xavfsizligini oshirish uchun boshqa algoritmlar bilan solishtirish o‘tkazing.

Resurslar: MD5 xesh qiymatlari, tug‘ilgan kun paradoksining izohi, zamonaviy xesh algoritmlari tavsifi.

Muammo yechimi: MD5 kolliziyalarini yaratish uchun zamonaviy hujum usullaridan foydalanish (masalan, Google tomonidan yaratilgan “SHAttered” usuli).

5-keys mavzusi: “Psevdotasodifiy sonlar generatorlarining tahlili”

Maqsad: Psevdotasodifiy sonlar generatorlarining (PTSG) xavfsizlik darajasini baholash va tasodifiylikni sinovdan o‘tkazish.

Stsenariy: Psevdotasodifiy sonlar generatori ma’lum statistik xatoliklarga ega. O‘quvchilarga bu generator tomonidan ishlab chiqarilgan sonlar taqdim etiladi va NIST testlarini qo‘llash topshiriladi.

Topshiriq:

1. PTSG tomonidan ishlab chiqarilgan sonlarning tasodifiyligini NIST testlari yordamida sinovdan o‘tkazing.
2. PTSG zaifliklarini aniqlang va ularni bartaraf etish bo‘yicha takliflar bering.
3. Tasodifiy sonlarning himoyalanganligini oshirish uchun qanday texnologiyalarni qo‘llash mumkinligini baholang.

Resurslar: PTSG orqali yaratilgan sonlar, NIST va DIEHARD testlar to‘plami.

Muammo yechimi: NIST testlarini qo‘llash orqali PTSG zaif tomonlarini aniqlash va yangi algoritm tavsiyalarini ishlab chiqish.

VI-BO‘LIM

GLOSSARIY

VI. GLOSSARIY

Tushunchaning o‘zbek tilidagi ko‘rinishi	Ma’nosi o‘zbek tilida	Tushunchaning ingliz tilidagi tarjimasi
Kriptologiya	Shifrlash va shifrlangan ma’lumotlarni tahlil qilishni o‘rganuvchi fandir.	Cryptology
Kriptografiya	Ma’lumotlarni shifrlash orqali himoya qilish usullari bilan shug‘ullanuvchi yo‘nalish.	Cryptography
Kriptotahlil	Shifrlangan ma’lumotlarni tahlil qilish va ularning zaif tomonlarini aniqlash usullari.	Cryptanalysis
Klassik shifrlarning kriptotahlili	An’anaviy shifrlash usullari (masalan, Sezar shifri) zaifliklarini tahlil qilish.	Cryptanalysis of classical ciphers
Kriptotahlilning sodda usullari	Shifrlash usullarining sodda zaifliklarini ochish uchun qo‘llaniladigan asosiy usullar.	Basic cryptanalysis methods
Kriptografik bardoshlilik tushunchasi	Algoritmning hujumlarga qarshi chidamlilik darajasi.	Cryptographic resilience
Hisoblash murakkabligi nazariyasi	Algoritmni buzish uchun talab qilinadigan hisoblash resurslari nazariyasi.	Theory of computational complexity
Simmetrik blokli shifrlar	Blok bo‘yicha shifrlash amalga oshiriladigan simmetrik algoritmlar.	Symmetric block ciphers
Statistik usullar	Shifrlash algoritmlarining statistik zaif tomonlarini tahlil qilish usullari.	Statistical methods
Chiziqli kriptotahlil	Shifrlash algoritmlaridagi chiziqli munosabatlarni tahlil qilish usuli.	Linear cryptanalysis
Differensial kriptotahlil	Shifrlash algoritmining kiritish va chiqarish ma’lumotlari farqlarini tahlil qilish usuli.	Differential cryptanalysis
Algebraik kriptotahlil	Shifrlash algoritmlarini algebraik tenglamalar orqali tahlil qilish usuli.	Algebraic cryptanalysis
Integral kriptotahlil	Blok shifrlash algoritmlaridagi ma’lum bitlar munosabatini tahlil qilish usuli.	Integral cryptanalysis
“Slaydli hujum”	Shifrlash algoritmidagi takroriy naqshlarni aniqlashga asoslangan hujum usuli.	Slide attack

Apparat xatoliklariga asoslangan usullar	Qurilmaning xatoliklarini tahlil qilib shifrlash kalitini aniqlash usullari.	Fault-based cryptanalysis
Faktorlash muammosi	Katta sonlarni tub ko‘paytuvchilarga ajratish qiyinligi muammosi.	Factoring problem
Diskret logarifmlash muammosi	Diskret logarifmlarni hisoblashning murakkabligi.	Discrete logarithm problem
Xesh funksiyalari	Ma’lumotlarning ixcham, o‘zgarmas qiymatini hosil qiluvchi algoritmlar.	Hash functions
Psevdotasodifiy sonlar generatori	Haqiqiy tasodifiylikni taqlid qiluvchi algoritmlar.	Pseudorandom number generator
Tug‘ilgan kun muammosi	Xesh qiymatlarining bir xil bo‘lish ehtimoli masalasi.	Birthday problem
MD4 va MD5 algoritmlarining kriptotahlili	MD4 va MD5 xesh funksiyalarining zaif tomonlarini tahlil qilish.	Cryptanalysis of MD4 and MD5
NIST statistik testlar to‘plami	Tasodifiylikni baholash uchun ishlatiladigan testlar to‘plami.	NIST statistical test suite
DIEHARD statistik testlar	Psevdotasodifiy sonlar generatorlarini sinovdan o‘tkazuvchi testlar to‘plami.	DIEHARD statistical tests
Oqimli shifrlash algoritmlari	Ma’lumotlarni oqim shaklida shifrlovchi algoritmlar.	Stream ciphers
Qo‘shimcha kanallardan foydalanishga asoslangan kriptotahlil	Qurilmalarning yon ma’lumotlarini (masalan, quvvat iste’moli yoki vaqt) tahlil qilish usullari.	Side-channel cryptanalysis
Yangi texnologiyalardan foydalanish	Zamonaviy texnologiyalar yordamida shifrlash algoritmlarini tahlil qilish.	Use of emerging technologies
Shor algoritmi	Katta sonlarni faktorizatsiya qilish uchun kvant algoritmi. RSA va boshqa ochiq kalitli algoritmlarga tahdid tug‘diradi.	Shor’s algorithm
Post-kvant kriptografiya	Kvant kompyuterlari hujumlariga qarshi bardoshli bo‘lgan kriptografik algoritmlar yo‘nalishi.	Post-quantum cryptography
Panjara asosli kriptografiya	Kvant hujumlariga bardoshli bo‘lgan algoritmlar sinfi, panjaraviy (lattice) strukturalarga asoslangan.	Lattice-based cryptography
Kod asosli kriptografiya	Xatolarni tuzatish kodlariga asoslangan kvant bardoshli kriptografik algoritmlar.	Code-based cryptography

Xesh asosli kriptografiya	Ma’lumotlarni xavfsiz himoya qilish uchun xesh funksiyalariga asoslangan algoritmlar.	Hash-based cryptography
Kvant kompyuterlari	Kvant mexanikasi qonunlariga asoslangan, yuqori hisoblash quvvatiga ega bo‘lgan kompyuterlar.	Quantum computers
Yon kanal hujumi	Qurilmalarning yon ma’lumotlari (quvvat, vaqt, elektromagnit nurlanish) orqali shifrlash tizimini buzish usuli.	Side-channel attack
Quvvat tahliliga qarshi himoya	Yon kanal hujumlarini bartaraf etish uchun elektr quvvatidan foydalanishni himoyalovchi texnikalar.	Power analysis resistance
Tasodifiylashtirish texnikalari	Yon kanal hujumlariga qarshi ma’lumotlarni shifrlashda qo‘shimcha tasodifiylik kiritish texnologiyasi.	Randomization techniques
Bulutli kriptotahlil	Bulutli platformalar yordamida katta hajmdagi ma’lumotlarni tezkor tahlil qilish usullari.	Cloud-based cryptanalysis
Distributsiyali hisoblash	Bir nechta qurilmalar hisoblash quvvatini birlashtirib, kriptografik tahlillarni amalga oshirish usuli.	Distributed computing
Homomorfik shifrlash	Ma’lumotlarni ochmasdan ular ustida hisoblashni amalga oshiruvchi shifrlash texnologiyasi.	Homomorphic encryption
Integral chiziqli tahlil	Blokli shifrlash algoritmlaridagi bir xil statistik naqshlarni topish usuli.	Integral linear analysis
Tugun (nod)	Ma’lumotlar tarmog‘idagi asosiy birlashuv nuqtasi yoki bloklar.	Node
Kvant superpozitsiyasi	Kvant kompyuterida bir vaqtning o‘zida bir nechta holatda bo‘lish imkoniyati.	Quantum superposition
Kriptografik protokollar	Ma’lumotlarni xavfsiz uzatish va tasdiqlash uchun ishlab chiqilgan algoritmlar to‘plami.	Cryptographic protocols
Ko‘p partiyali hisoblash	Bir nechta tomonlar o‘rtasida ma’lumotlarni oshkor qilmasdan hisoblashni amalga oshirish texnologiyasi.	Multi-party computation
Kvant qulash effekti	Kvant holatining o‘lchov paytida yagona qiymatga o‘tish jarayoni.	Quantum collapse effect

AES (Advanced Encryption Standard)	Zamonaviy simmetrik blokli shifrlash algoritmi, xavfsiz va tez ishlash uchun yaratilgan xalqaro standart.	Advanced Encryption Standard (AES)
RSA algoritmi	Katta sonlarni faktorizatsiya qilishga asoslangan, ochiq kalitli shifrlash algoritmi.	RSA algorithm
Tug‘ilgan kun paradoksi	Ikkita o‘xshash xesh qiymatini topish ehtimoli kutilganidan yuqori bo‘lishi tushunchasi.	Birthday paradox
MD5	Xesh funksiyasi, xabarlarni ixcham shaklda ifodalash uchun ishlatiladi, ammo zamonaviy hujumlarga bardoshli emas.	MD5
NIST testlar	Kriptografik algoritmlar va tasodifiy sonlar generatorlarining xavfsizligini baholash uchun testlar to‘plami.	NIST tests

VII-BO‘LIM

ADABIYOTLAR RO‘YXATI

VII. ADABIYOTLAR RO'YXATI

I. O‘zbekiston Respublikasi Prezidentining asarlari:

1. Mirziyoyev SH.M. Buyuk kelajagimizni mard va olijanob xalqimiz bilan birga quramiz. – T.: “O‘zbekiston”, 2017. – 488 b.

2. Mirziyoyev SH.M. Milliy taraqqiyot yo‘limizni qat’iyat bilan davom ettirib, yangi bosqichga ko‘taramiz. 1-jild. – T.: “O‘zbekiston”, 2017. – 592 b.

3. Mirziyoyev SH.M. Xalqimizning roziligi bizning faoliyatimizga berilgan eng oliy bahodir. 2-jild. –T.: “O‘zbekiston”, 2018. – 507 b.

4. Mirziyoyev SH.M. Niyati ulug‘ xalqning ishi ham ulug‘, hayoti yorug‘ va kelajagi farovon bo‘ladi. 3-jild.– T.: “O‘zbekiston”, 2019. – 400 b.

5. Mirziyoyev SH.M. Milliy tiklanishdan – milliy yuksalish sari. 4-jild.– T.: “O‘zbekiston”, 2020. – 400 b.

II. Normativ-huquqiy hujjatlar:

6. O‘zbekiston Respublikasining Konstitusiyasi.–T.:O‘zbekiston, 2018.

7. O‘zbekiston Respublikasining 2020-yil 23-sentabrda qabul qilingan “Ta’lim to‘g‘risida”gi O‘RQ-637-sonli Qonuni.

8. O‘zbekiston Respublikasi Prezidentining 2017-yil 7-fevral “O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasi to‘g‘risida”gi 4947-sonli Farmoni.

9. O‘zbekiston Respublikasi Prezidentining 2018-yil 21-sentabr “2019-2021 yillarda O‘zbekiston Respublikasini innovatsion rivojlantirish strategiyasini tasdiqlash to‘g‘risida”gi PF-5544-sonli Farmoni.

10. O‘zbekiston Respublikasi Prezidentining 2019-yil 27-may “O‘zbekiston Respublikasida korrupsiyaga qarshi kurashish tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi PF-5729-son Farmoni.

11. O‘zbekiston Respublikasi Prezidentining 2019-yil 27-avgust “Oliy ta’lim muassasalari rahbar va pedagog kadrlarining uzluksiz malakasini oshirish tizimini joriy etish to‘g‘risida”gi PF-5789-sonli Farmoni.

12. O‘zbekiston Respublikasi Prezidentining 2019-yil 8-oktabr “O‘zbekiston Respublikasi oliy ta’lim tizimini 2030-yilgacha rivojlantirish konsepsiyasini tasdiqlash to‘g‘risida”gi PF-5847-sonli Farmoni.

13. O‘zbekiston Respublikasi Prezidentining 2024-yil 15-avgustdagi “O‘zbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-293-son Qarori.

14. O‘zbekiston Respublikasi Prezidenti Shavkat Mirziyoyevning 2020-yil 25-yanvardagi Oliy Majlisga Murojaatnomasi.

15. O‘zbekiston Respublikasi Vazirlar Mahkamasining 2001-yil 16-avgustdagi “Oliy ta’limning davlat ta’lim standartlarini tasdiqlash to‘g‘risida”gi

343-sonli Qarori.

16. O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015-yil 10-yanvardagi “Oliy ta’limning Davlat ta’lim standartlarini tasdiqlash to‘g‘risida”gi 2001-yil 16-avgustdagi “343-sonli qororiga o‘zgartirish va qo‘shimchalar kiritish haqida”gi 3-sonli qarori.

III. Maxsus adabiyotlar:

17. O.P.Axmedova, Z.T.Xudoykulov, O. Allanov, I.M.Boyquziyev Kriptoanaliz. O‘quv qo‘llanma. T.: “Iqtisod-Moliya”, 2022. 171 b.

18. Kuryazov D.M., Sattorov A.B., Axmedova B.B. Blokli simmetrik shifrlash algoritmlari bardoshligini zamonaviy kriptotahlil usullari bilan baholash. O‘quv qo‘llanma. T.: “Aloqachi”. 2017, 228 bet.

19. Xasanov P.F., Xasanov X.P., Axmedova O.P., Davlatov A.B. Kriptotahlil va uning maxsus usullari, O‘quv qo‘llanma, Toshkent, 2010

20. Akbarov D.YE. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanishlari. Toshkent. ”O‘zbekiston markasi“, 2009

21. Л.К.Бабенко, Е.А.Ищукова. Современные алгоритмы блочного шифрования и методы из анализа: учеб. пособие для студентов вузов, обучающихся по группе специальностей в обл. информ. безопасности – М.: Гелиос АРВ, 2006. – 376 с.

22. M.Stamp. Applied cryptanalysis: Breaking Ciphers in the Real World. John Wiley & Sons, Inc, 2007, -P. -417.

23. Б.Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – Москва: ТРИУМФ, 2002.

24. Xasanov P., Xasanov X., Axmedova O., Davlatov A. Kriptotahlil va uning maxsus usullari. O‘quv qo‘llanma.– Toshkent, 2010.

IV. Internet saytlar:

25. http://edu.uz – O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta’lim vazirligi.

26. http://lex.uz – O‘zbekiston Respublikasi Qonun hujjatlari ma’lumotlari milliy bazasi.

27. http://bimm.uz – Oliy ta’lim tizimi pedagog va rahbar kadrlarini qayta tayyorlash va ularning malakasini oshirishni tashkil etish Bosh ilmiy-metodik markazi.

28. http://ziyonet.uz – Ta’lim portali ZiyonET.

29. http://natlib.uz – Alisher Navoiy nomidagi O‘zbekiston Milliy kutubxonasi.

30. http://jnicholl.org/Cryptanalysis/Tools/

31. https://www.cryptool.org/en/cto/

32. https://resources.infosecinstitute.com/topic/cryptanalysis-tools/

33. http://rumkin.com/tools/cipher/
34. https://blackarch.org/crypto.html
35. https://www.guballa.de/vigenere-solver
36. https://www.simonsingh.net/The_Black_Chamber/substitutioncrackingtool.html
37. https://www.guru99.com/how-to-make-your-data-safe-using-cryptography.html
38. https://www.cs.bu.edu/~goldbe/teaching/CS558S17/Lab1.pdf