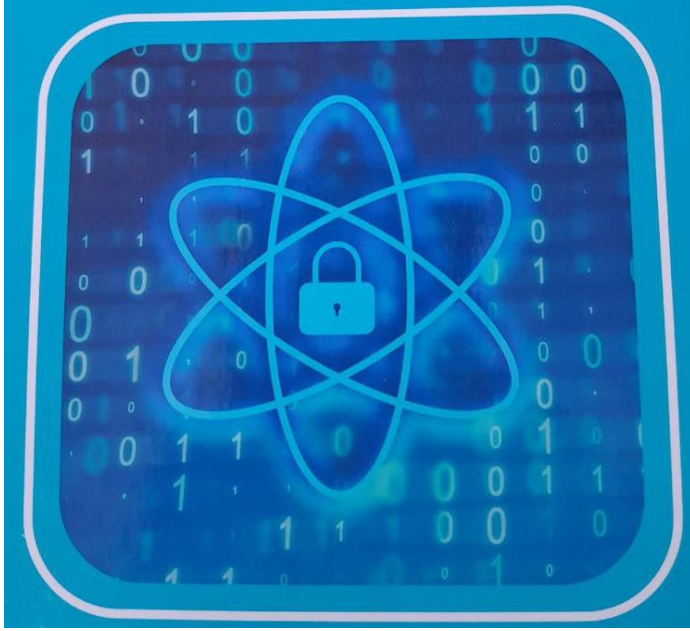
AXMEDOVA O.P., XUDOYKULOV Z.T.,
ALLANOV O.M., BOYQUZIYEV I.M.

KRIPTOANALIZ



O‘ZBEKISTON RESPUBLIKASI RAQAMLI
TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT
AXBOROT TEXNOLOGIYALARI UNIVERSITETI

AXMEDOVA O.P., XUDOYKULOV Z.T.,
ALLANOV O.M., BOYQUZIYEV I.M.

KRIPTOANALIZ

Muhammad Al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti tomonidan o‘quv qo‘llanma sifatida tavsiya etilgan

TOSHKENT
“METODIST NASHIYOTI”
2024

UDK: 003.26.09(075.8)
BBK: 32.811.4ya7
K 81

Axmedova O.P.
Kriptoanaliz / Xudoykulov Z.T., Allanov O.M., Boyquziyev I.M./. O'quv qo'llanma. – Toshkent: "METODIST NASHIYOTI", 2024. – 200 b.

Mazkur o'quv qo'llanma 70610301-Kriptografiya va kriptoanaliz (sohalar bo'yicha) mutaxassisligi talabalari uchun mo'ljallangan. O'quv qo'llanmada kriptoanaliz asoslari, kriptoanalizning universal usullari, klassik shifrlash algoritmlariing kriptoanalizi, simmetrik blokli shifrlash algoritmlarining kriptoanalizi, simmetrik oqimli shifrlash algoritmlarining kriptoanilizi, xesh funksiyalarning kriptoanalizi, ochiq kalitli kriptotizimlarning kriptoanalizi masalalarining nazariy va amaliy asoslari muhokama etilgan.

O'quv qo'llanmada keltirilgan ma'lumotlardan nafaqat magistratura bosqichi talabalari, balki axborot xavfsizligi muammolari bilan qiziquvchilarning keng ommasi foydalanishlari mumkin.

Taqrizchilar:

B.F. Abduraximov– fizika matematika fanlari doktori, professor, O'zbekiston Milliy universiteti Amaliy matematika va kompyuter tahlili kafedrasi professori.

Sh.R. G'ulomov – PhD, dotsent, Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Axborot xavfsizligi kafedrasi mudiri.

Muhammad Al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universitetining 2023-yil 10-maydagi 500-sonli buyrug'iga asosan nashr qilishga ruxsat berilgan.

ISBN 978-9910-03-218-9

MUQADDIMA

Hozirgi kunda har qanday rivojlangan davlatda axborot va kommunikatsiya texnologiyalarining jamiyatda tutgan o'rni tobora ortib bormoqda. Respublikamizda davlat va xo'jalik boshqaruv organlarida axborotni himoyalashning kriptografik mexanizmlarini tatbiq etish, hususan, davlat xizmatlaridan masofadan foydalanishda foydalanuvchilarning haqiqiylıgini tekshirish va ma'lumotlar konfidensialligini ta'minlashga qaratilgan keng qamrovli chora-tadbirlar amalga oshirilmoqda. 2022-2026-yillarga mo'ljallangan Yangi O'zbekistonning taraqqiyot strategiyasida "Kiberjinoyatchilikning oldini olish tizimini yaratish" vazifasi belgilangan. Ushbu vazifalarni amalga oshirishda kiberxavfsizlik sohasining asosini tashkil etuvchi kriptografik algoritmlarni xavfsizlik nuqtai nazaridan baholash va ularni takomillashtirish muhim vazifalardan biri hisoblanadi.

O'zbekiston Respublikasi Prezidentining 2018-yil 14-martdagi PF-5379-son "O'zbekiston Respublikasining davlat xavfsizligi tizimini takomillashtirish chora-tadbirlari to'g'risida"gi farmonlari, 2007-yil 3-apreldagi PQ-614-son "O'zbekiston Respublikasida axborotni kriptografik muhofaza qilishni tashkil etish chora-tadbirlari to'g'risida"gi qarori va O'zbekiston Respublikasi Vazirlar Mahkamasining 2007-yil 21-noyabrdagi "Axborotning kriptografik himoya vositalarini loyihalashtirish, tayyorlash, ishlab chiqarish, realizatsiya qilish, ta'mirlash va ulardan foydalanish faoliyatini litsenziyalash to'g'risida"gi nizomni tasdiqlash haqida hamda mazkur faoliyatga tegishli boshqa meyoriy-huquqiy hujjatlarda belgilangan vazifalarni amalga oshirishda mazkur o'quv qo'llanma ma'lum darajada xizmat qiladi.

Taqdim etilayotgan o'quv qo'llanma axborot xavfsizligi va kriptografiya yo'nalishida tahsil olayotgan magistratura bosqichidagi talabalar uchun mo'ljallangan. Shuningdek ushbu o'quv qo'llanmadan axborot xavfsizligi yo'nalishida bakalavrlar tayyorlash jarayonida hamda kriptografiya yo'nalishida ilmiy-tadqiqot olib borayotgan tadqiqotchilar, ilmiy xodimlar va soha mutaxassislari foydalanishlari mumkin. Ushbu o'quv qo'llanma "Kriptografiya va kriptoanaliz" mutaxassisligining o'quv ta'lim standarti va o'quv dasturiga muvofiq ishlab chiqilgan.

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.

1.5. 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 $O(t^{f(n)})$ 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.

1.1. Asosiy tushunchalar va ta'riflar

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.

1.2. Kriptologiyaning ilmiy yo'nalishlari

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.

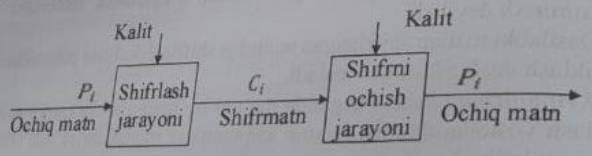
Kriptonaliz shifrlash usullarining kuchli, zaif tomonlarini baholash va kriptotizimlarni buzish usullarini ishlab chiqish bilan shug'ullanuvchi fan sohasi bo'lib, asosiy maqsadi shifrlangan xabarlarning mazmunini kalitsiz oshkor qilish hisoblanadi.

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

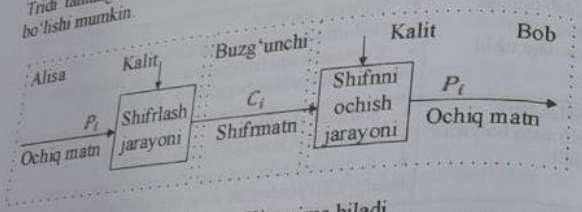
Kriptoanaliz turlari

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.

1.3. Kriptoanalizning zarurati

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.

1.4. Kriptografik algoritmlar bardoshliligi 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 bardoshliliigi 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

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:

$0; 1; 00; 01; 10; 11; 000; 001;\ \ldots\ ; 111; \ldots ; 00\ldots0; 00\ldots1; \ldots ; 11\ldots1;$

chekli sondagi 0 va 1 belgilarning ketma-ketliklari bloklaridan (vektorlaridan) tuzilgan to'plamni Σ deb belgilanadi. Barcha o'lchami n ga teng bo'lgan ikkilik sanoq tizimining so'zlari to'plamini Σ^n deb belgilanadi. Murakkablik nazariyasida Σ 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 $R(x,u)$: $\Sigma x \Sigma \to \{0,1\}$ – 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

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

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?

II BOB. KRIPTOANALIZNING UNIVERSAL USULLARI

2.1. 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.

2.2. 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.

Parollarni tanlash natijalari 2.2-jadval

Tanlash murakkabligi	Tanlash vaqti	Protsessor turi
$2{,}08\cdot10^{11}$	15 minut	486DX/4-100
$3{,}68\cdot10^{16}$	8 soat	Pentium-120

2.3. 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.

2.4. «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 $\alpha \in n$ predmetlar n ta predmet orasidan qaytarilish bilan tanlansa, ikki predmetning bir xil bo'lish ehtimoli $p = 1 - e^{-\alpha^2/2}$ ga teng.

Faraz qilinsinki, ochiq matn x va uning shifrogrammasi u ma'lum. x uchun tasodifiy tarzda kalitlar to'plami z_i va shifrogrammalar $w = F(z_i, x)$ 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_{i1} kalitni olib, u shifrmatn ochiladi va natija $v = F(z_{i1}, u)$ ni MB bilan taqqoslanadi. Agar v biror w bilan teng chiqsa, kalit z_{i1} izlangan kalit z_i 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.

2.5. 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.

Nazorat savollari

1. Klassik kriptoanaliz usullarini sanab bering
2. To'liq tanlash usuli va uning mohiyatini tushuntirib bering
3. Chastotaviy tahlil usulida ochiq matnni topish nimaga asoslanadi?
4. «O'rtada uchrashish» hujum usulini tushuntirib bering.
5. Xesh-funksiyalar uchun kolliziya hujumi usuli haqida ma'lumot bering.

3.1. 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 bloktagi 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.

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

Harf	Soni		Harf	Chastotasi
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
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:

GBSXUCGSZQGKGSQPKQKGLSKASPCGBGBKGUKGCEUKU
ZKGGBSQEICACGKGCEUERWKLKUPKQQGCIICUAEUVSHQ
KGCEUPCGBCGQOEVSHUNSUGKUZCGQSNLSHEHIEEDCUO
GEPKHZGBSNKCUGSUKUASERLSKASCUGBSLKACRCACUZ
SSZEUSBEXHKRGSHWKLKUSQSKCHQTXKZHEUQBKZAENN
SUASZFENFCUOCUEKBXGBSWKLKUSQSKNFKQQKZEHGEG
BSXUCGSZQGKGSQKUZBCQAEIISKOXSZSICVSHSZGEGBSQ
SAHSGKHMERQGKGSKREHNKIHSLIMGEKHSASUGKNSHCA
KUNSQQKOSPBCISGBCQHSLIMQGKGSZGBKGCGQSSNSZXQ
SISQQGEAEUGCUXSGBSSJCQGCUOZCLIENKGCAUSOEGCK
GCEUQCGAEUGKCUSZUEGBHSKGEHBCUGERPKHEHKHNS
ZKGGKAD.

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	1	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_1 va 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 holat "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:

P_1	L	I	K	E
	100	010	011	000
K	110	011	101	111
C_1	010	001	110	111

Va

P_2	K	I	T	E
	011	010	111	000
K	110	011	101	111
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.

3.4. 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.

3.2- -rasm. Zimmermann telegrami

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.

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.

3.5. 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.

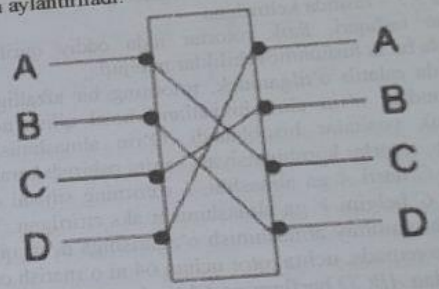
Kriptomuhandislik nuqtai nazaridan, rotorning ajoyibligi sodda elektromexanik qurilmadan bardoshli usulda katta sondagi alohida o'rin almashtirishlarni hosil qilishning mumkinligi. Bu qarash kompyuter erasidan oldingi era uchun juda muhim edi. Shunisi aniqki, Enigma haqiqatda qurilmaning mustahkam qismi 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

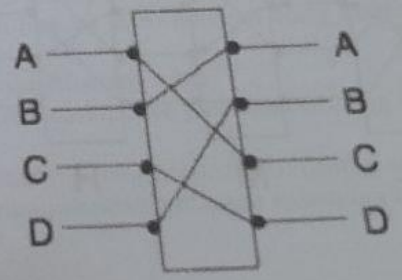
mashina bir xil sozlanish bilan shifrlash yoki deshifrlash uchun foydalanilgan.

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.



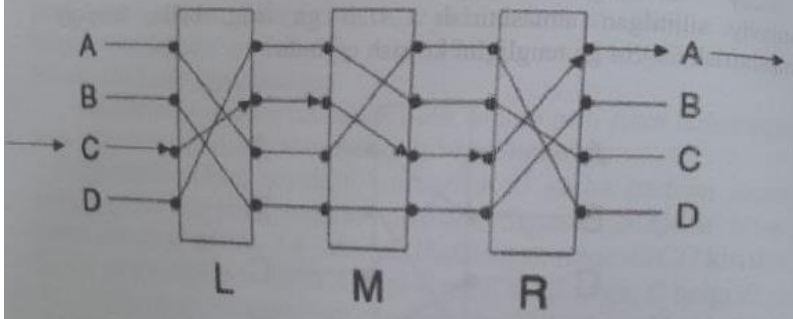
3.5 – rasm. Harakatlangan rotor

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 (2,3,1,2) (2,2,3,1) ga teng. *CADB* almashtirish uchun esa bu qadamlar (2,3,1,2) ga teng va u 3.5 – rasmda keltirilgan.

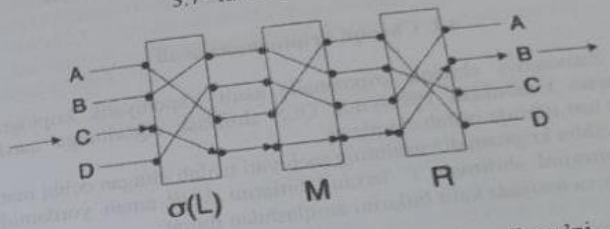
Bundan tashqari, fizik rotorlar juda oddiy qurilma, ammo, abstrakt holda ba'zi tushunmovchiliklar mavjud.

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.

Nazorat savollari

1. O'rin almashtirishga asoslangan shifrlash usullarining kriptoanalizi haqida ma'lumot bering.
2. O'rniga qo'yishga asoslangan shifrlash usullarining kriptoanalizi haqida ma'lumot bering.
3. Bir martali bloknot shifri nima va uning kriptoanalizi qanday amalga oshiriladi?
4. Zimmermann telegrami nima?
5. Enigma mashinasi qachon yaratilgan va uning vazifasi nimadan iborat bo'lgan
6. Enigma mashinasining kriptoanalizi qanday amalga oshirilgan
7. Enigma mashinasida shifrlangan axbotning kriptobardoshlili qanday bo'lgan?

IV BOB. SIMMETRIK BLOKLI SHIFRLARNING KRIPTOANALIZI

4.1. Chiziqli kriptoanaliz 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:

$$M[i_1, i_2, \dots, i_n] \oplus C[j_1, j_2, \dots, j_n] = K[k_1, k_2, \dots, k_n],$$
$$\text{bu yerda } M[i_1, i_2, \dots, i_n) = M[i_1) \oplus M[i_2) \oplus \dots M[i_n)$$
$$S[i_1, i_2, \dots, i_n) = S[i_1) \oplus S[i_2) \oplus \dots S[i_n)$$
$$K[i_1, i_2, \dots, i_n) = K[i_1) \oplus K[i_2) \oplus \dots K[i_n)$$

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, $X[x_1, x_2, \dots x_n)$ – akslantirishga kiruvchi bitlarni, $Y[y_1, y_2, \dots y_n)$–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:

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

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 $x_0x_1x_2 = 000$ qiymati kiritilganda undan $y_0y_1 =$ 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 bloklarig hujum foydaliroq bo'lishi uchun bu yodashuvni kengaytirishga haral qilish kerak. Natijada kalitni topishga qaratilgan chiziqli tenglamala yechish imkoniyatiga ega bo'linadi. Xuddi differensial tahlilda bo'l

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.

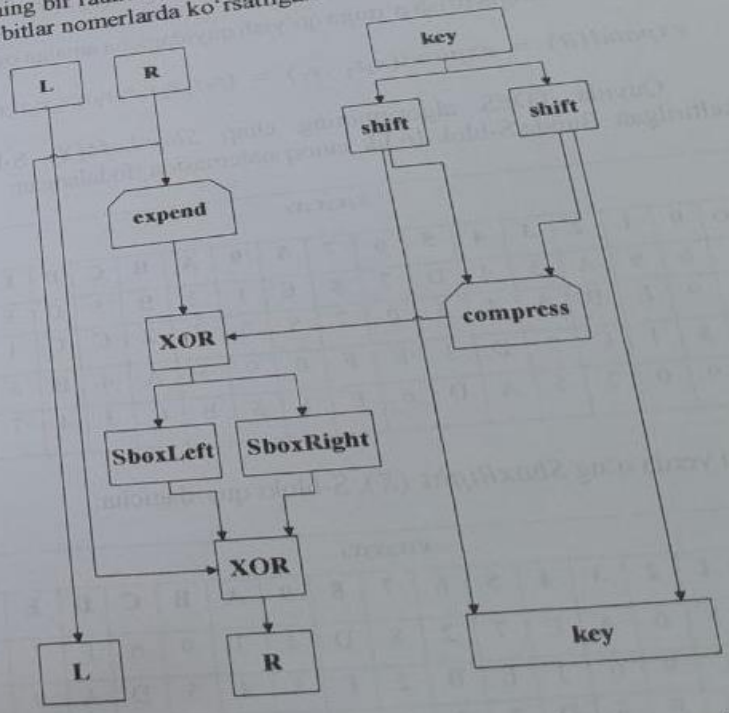
Kalit va blok uzunligining kichikligi TDES algoritmining xavfsizlikni ta'minlay olmasligini bildiradi va tahlil natijasi qanday bo'lishidan qat'iy nazar kerakli algoritm bo'lolmasligini bildiradi. Shunga qaramay, TDES algoritmini chiziqli va differensial tahlilda

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_0x_5 \ $x_1x_2x_3x_4$	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_0x_5 \ $x_1x_2x_3x_4$	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

$$y_1 = x_2 \; va \; y_2 = x_3 \tag{4.1}$$

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:

$$expend(R_0) = expend\,(r_0r_1r_2r_3r_4r_5r_6\,r_7) = r_4r_7r_2r_1r_5r_7r_0\,r_2r_6r_5r_0\,r_3. \tag{4.2}$$

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:

$$r_4r_7r_2r_1r_5r_7\,r_7 \oplus k_2k_4k_3k_6k_7k_1.$$

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

$$y_1 = r_2 \oplus k_5 \; va \; y_2 = r_1 \oplus k_6. \tag{4.3}$$

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:

$$r'_1 = r_2 \oplus k_5 \oplus l_1 \; va \; r'_2 = r_1 \oplus k_6 \oplus l_2. \tag{4.4}$$

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:

$$k_0 \oplus k_1 = c_1 \oplus p_{10} \tag{4.}$$

va

$k_7 \oplus k_2 = c_2 \oplus p_9$. (4.6)

Yuqoridagi tenglamalarning har ikkalasi ham $(3/4)^3$ 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.

TDES algoritmining chiziqli tahlili 4.3-jadval

$(L_0R_0) = (p_0 \dots p_7 p_8 \dots p_{15})$	1 va 2 bitlar (raqamlar 0 dan boshlangan)	Bajarilish ehtimolligi
$L_1 = R_0$ $R_1 = L_0 \oplus F(R_0, K_1)$	p_9, p_{10} $p_9 \oplus p_{10} \oplus k_5$, $p_2 \oplus p_9 \oplus k_6$	1 3/4
$L_2 = R_1$ $R_2 = L_1 \oplus F(R_1, K_2)$	$p_1 \oplus p_{10} \oplus k_5$, $p_2 \oplus p_9 \oplus k_6$ $p_9 \oplus k_6 \oplus k_7$, $p_1 \oplus k_5 \oplus k_0$	3/4 $(3/4)^2$
$L_3 = R_2$ $R_3 = L_2 \oplus F(R_2, K_3)$	$p_2 \oplus k_6 \oplus k_5$, $p_1 \oplus k_3 \oplus k_0$ $p_{10} \oplus k_0 \oplus k_1$, $p_9 \oplus k_7 \oplus k_2$	$(3/4)^2$ $(3/4)^3$
$L_4 = R_3$ $R_4 = L_3 \oplus F(R_3, K_4)$ $C = (L_4, R_4)$	$p_{10} \oplus k_0 \oplus k_1$, $p_9 \oplus k_7 \oplus k_2$ $c_1 = p_{10} \oplus k_0 \oplus k_1$, $c_2 = p_9 \oplus k_7 \oplus k_2$	$(3/4)^3$ $(3/4)^3$

4.3-jadval natijalariga asoslangan holda chiziqli hujumni amalga oshirish sodda hisoblanadi. Ma'lum ochiq matn $P = p_0 p_1 p_2 .. p_{15}$ va unga mos shifrmat $C = c_0 c_1 c_2 .. c_{15}$ 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.

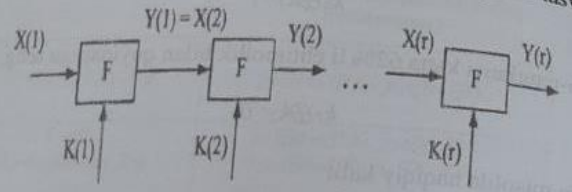
Yuqoridagi chiziqli kriptoanalizda kalit ma'lumotining ikki bitini tiklash keltirilgan. Butun K kalitni qayta tiklash uchun qolgan noma'lum bitlarni ham to'liq aniqlash kerak. Bu taxminan 2^{13} ta shifrlashni bajarish va chiziqli kriptoanalizni amalga oshirishni talab qiladi. Bu hujum juda muhim ahamiyatga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

4.2. Differensial kriptoanaliz 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

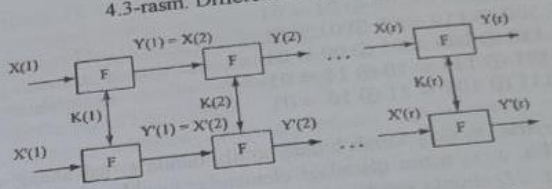
Bu yerda $K = (K(1), K(2), \dots, K(r))$ kalitlar K_0 kalitdan biror qonuniyat asosida yasalgan yoki xar bir raund uchun alohida tanlangan kalitlar, $X(1)$ va $X'(1)$ ochiq matn juftliklari.

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 $\Delta X(1)$ 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:

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

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
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

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

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

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

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 kengayirishdan oldin $X_1 \oplus X_2 = 0000\ 0010$ bo'lgan bo'lsa, keyin

$$expand(X_1) \oplus expand(X_2) = expand(X_1 \oplus X_2) = expand(00000010) = 000000\ 001000 \quad (4.10)$$

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

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

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

$$R_2 \oplus R'_2 = (L_1 \oplus F(R_1, K_2)) \oplus (L'_1 \oplus F'(R'_1, K_2))$$
$$= (L_1 \oplus L'_1) \oplus (F(R_1, K_2) \oplus F(R', K_2))$$
$$= (R_0 \oplus R'_0) \oplus (F(R_1, K_2) \oplus F(R'_1, K_2))$$
$$= 0000\ 0010 \oplus 0000\ 0010$$
$$= 0000\ 0000$$

$(3/4)^2=4/16=0.5625$ 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.

TDES ning differensial tahlili 4.6-jadval

$(L_0, R_0) = P$	$(L'_0, R'_0) = P'$	$(L_0, R_0) = P$	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
$L_2 = R_1$ $R_2 = L_1 \oplus F(R_1, K_2)$	$L'_2 = R'_1$ $R'_2 = L'_1 \oplus F(R'_1, K_2)$	$(L_2, R_2) \oplus$ $(L'_2, R'_2) = 0x0200$	$(¾)^2$
$L_3 = R_2$ $R_3 = L_2 \oplus F(R_2, K_3)$	$L'_3 = R'_2$ $R'_3 = L'_2 \oplus F(R'_2, K_3)$	$(L_3, R_3) \oplus$ $(L'_3, R'_3) = 0x0002$	$(¾)^2$
$L_4 = R_3$ $R_4 = L_3 \oplus F(R_3, K_4)$ $C = (L_4, R_4)$	$L'_4 = R'_3$ $R'_4 = L'_3 \oplus F(R'_3, K_4)$ $C = (L'_4, R'_4)$	$(L_4, R_4 \oplus)$ $(L'_4, R'_4) = 0x0202$ $C \oplus C' = 0x0202$	$(¾)^3$

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

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

Tenglamani quyidagicha qayta yozib olish mumkin

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

Agar $C \oplus C = 0x0202$ (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

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

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

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

va yuqoridan quyidagi ham ma'lum

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

Demak

$L_4=l_0l_1l_2l_3l_4l_5l_6l_7$ va $L'_4=l'_0l'_1l'_2l'_3l'_4l'_5l'_6l'_7$

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

$$0000\ 0010=(SboxLeft(l_4l_7l_2l_1l_5l_7 \oplus k_0k_2k_3k_4k_5k_7),\ SboxRight(l_0l_2l_6l_5l_0l_3 \oplus k_{13}k_{14}k_{15}k_9k_{10}k_{11})) \oplus (SboxLeft(l'_4l'_7l'_2l'_1l'_5l'_7 \oplus k_0k_2k_3k_4k_5k_7),\ SboxRight(l'_0l'_2l'_6l'_5l'_0l'_3 \oplus k_{13}k_{14}k_{15}k_9k_{10}k_{11}) \quad (4.16)$$

4.16-ifodaning chap qismidagi 4 ta bitlari quyidagini beradi

$$0000=(SboxLeft(l_4l_7l_2l_1l_5l_7 \oplus k_0k_2k_3k_4k_5k_7) \oplus (SboxLeft(l'_4l'_7l'_2l'_1l'_5l'_7 \oplus k_0k_2k_3k_4k_5k_7$$

$l_i=l'_i$ 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-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-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-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

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

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.

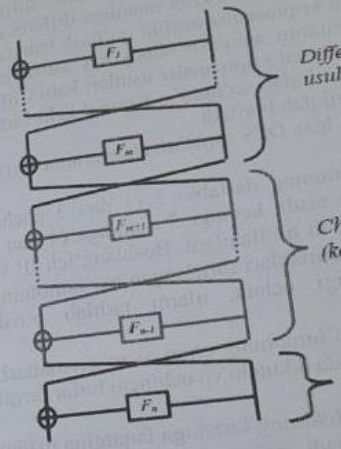
Ushbu usul bilan butun K ni qayta tiklash uchun kutilgan jami hisoblashlar soni taxminan 2^{11} ta shifrlashni amalga oshiramiz, shuningdek taqqoslaganda juda muhim bo'lmagan differemsial hujum ham talab qilinadi. Natijada, biz butun 16-bit kalitni topishimiz uchun kalitni to'liq qidiruv usuli $2^{16}/2=2^{15}$ 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.

4.3. Chiziqli-differensial kriptoanaliz 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.

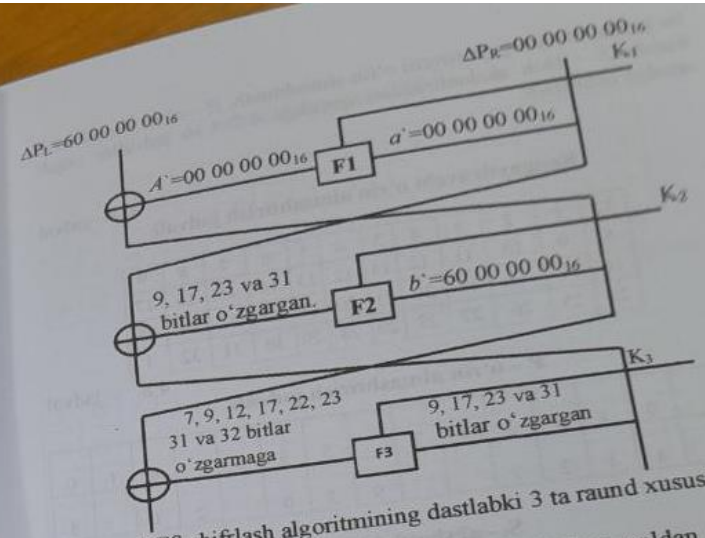
Bu holda shifrlash algoritmining daslabki 3 (1 dan 3 gacha) raundiga differensial kriptoanaliz usuli, keyingi 3 raundiga (4 dan 6 gacha) esa chiziqli kriptoanaliz usuli qo‘llaniladi. Boshlang‘ich IP va oxirgi IP^{-1} o‘rin almashtirish akslantirishlari shifrlangan ma’lumotning kriptobardoshligiga ta’siri 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_i akslantirish blokining kirishiga faqatgina ushbu ayirma kiritilgan holat e’tiborga olinadi, qolgan bloklar kirishiga esa nolga teng bo‘lgan ayirma beriladi.

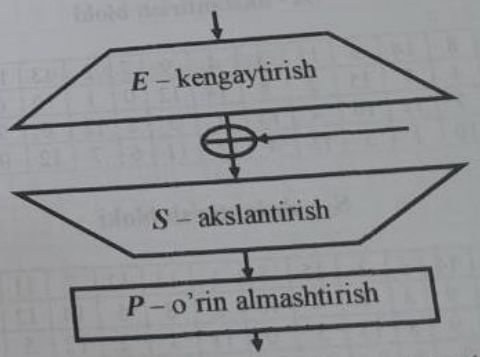
Ushbu holatda ayirmani chap qismi, ikkinchi va uchinchi (ikkita ma’lumotning XOR yig‘indisi bo‘lgan) o‘rinlardan tashqari nollardan iborat bo‘ladi. O‘ng qismda esa kiruvchi ma’lumotlar farqli bo‘lmagani tufayli ularning ayirmasi nolga teng bo‘ladi.

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:

Kengaytiruvchi o‘rin almashtirish jadvali

4.7 – jadval

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

P – o‘rin almashtirish jadvali

4.8 – jadval

6		0	1	9	2	8	7		5	3	6		8	1	0
		4	4	2	7			9	3	0		2	1		5

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

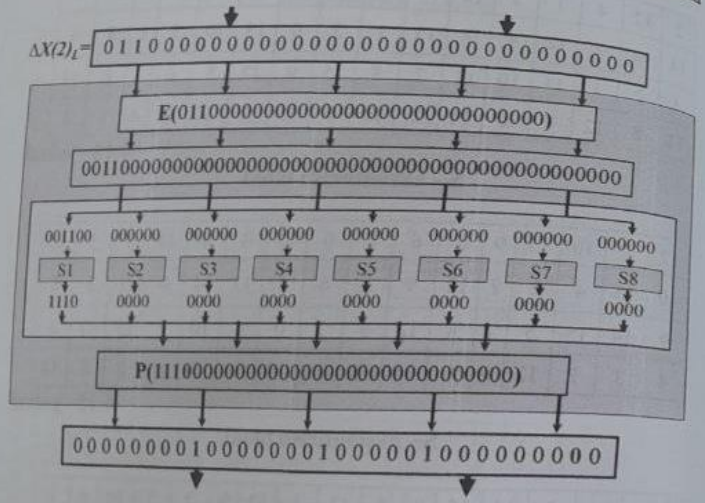
S_7- akslantirish bloki

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

S_8- akslantirish bloki 4.16– jadval

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.

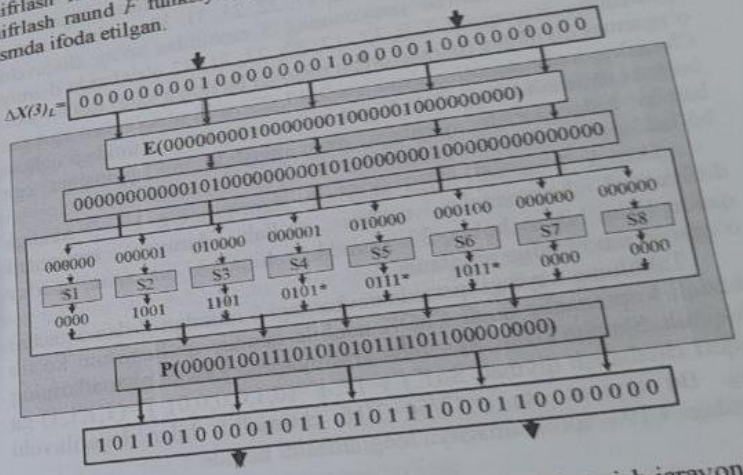


4.7-rasm. *F(2)* – funksiyaga kiruvchi orttirmaning o‘zgarish jarayoni

Demak, 4.7 – rasmda ko‘rsatilgan akslantirishlar natijasiga ko‘ra, 2–raund F–funksiya chiqishida Δ=00000000100000001000001000000000 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_7 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.

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

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.

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

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.

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

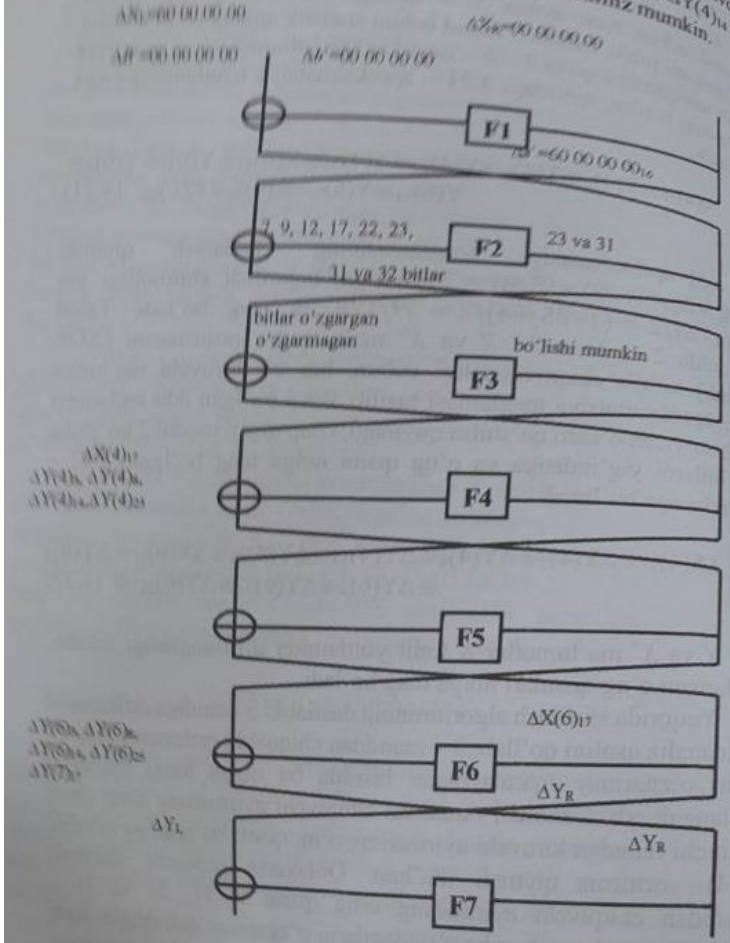
4.21–aproksimatsiya tenglamasining chetlanish qiymati $\Delta = \Delta_1 * \Delta_2 = (5/8) * (5/8) = 25/64$ ga, bajarilish ehtimolligi esa $r = (1-\Delta)/2 = (1-25/64)/2 = 39/128$ ga teng bo'ladi. Tahlil jarayonida 2 ta kiruvchi X va X` ma'lumotlar orttirmasini (XOR yig'indi) ko'rib chiqayotganligi 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.

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

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.



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

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.

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.

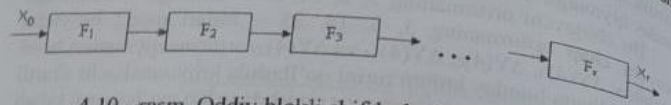
Demak 1.4 – tenglama bitta $\Delta X(6)_{17}$ noma'lumga bog'liq bo'lgan tenglamani ifodalagani uchun, $\Delta X(6)_{17}$ orttirma qiymatini oson aniqlash mumkin. 1.4 – tenglikning ehtimolligi X va X` ma'lumotlar uchun tuzilgan aproksimatsiya tenglamalar ehtimolligi ko'paytmasiga teng, ya'ni: p=(39/128)*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

4.4. "Slaydli hujum" kriptoanaliz 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.

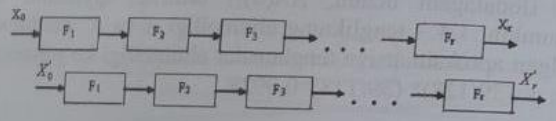


4.10 - rasm. Oddiy blokli shifrlash algoritmi sxemasi

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 $x_j'=F_j(x_{j-1}'), j=1,\dots r$ 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* (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

S1 -blok 4.18-jadval

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

S2 -blok 4.19-jadval

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

Maska 4.20-jadval

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:

Slayd juftliklar 4.21-jadval

№	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:

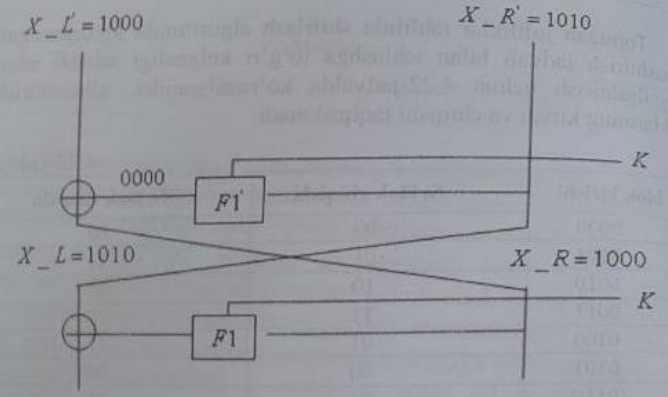
4.22-jadval

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

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

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.



4.12-rasm. Birinchi raund birinchi slaydli juftlik tahlili

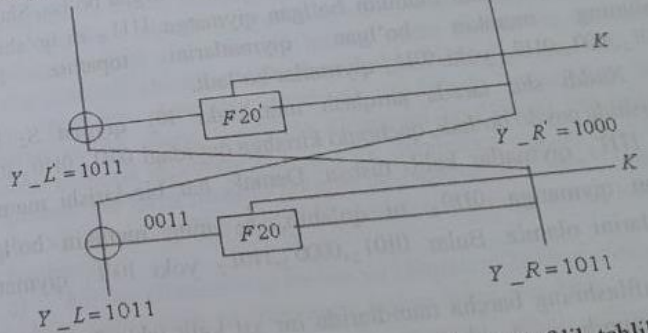
F_1' funksiyaga kiruvchi xabar 4.17-jadvalga muvofiq kengaytirishli o'rin almashtirishga uchraydi. Demak, 1010_2 kirish 11010100_2 qiymatga o'zgaradi. Bu esa $K=(k_1,k_2)$ kalitga qo'shiladi. Shifrlash jarayonida matn ikkita bo'lakka ajratilib har bir bo'lagi kalit qismi bilan qo'shilib keyin esa mos 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. r_R va r_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, *va* 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.

4.5. Algebraik kriptoanaliz 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:

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

ko'rinishidagi tengamaga aytiladi. Bu yerda, f – noma'lum $x_1, x_2, x_3, \dots, x_n$ 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'lad

Ushbu chinlik jadvalining umumiy ko'rinishi 4.23-jadvalda keltirilgan bo'lib, 2^s ta satr va t ta ustundan iborat.

Tekshiruv jadvali 4.23-jadval

	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. $n \times m$ – o'lchovli ixtiyoriy $F:(x_1,\dots,x_n) \to (y_1,\dots,y_m)$ – 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.

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 $r=7$) 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.	$x_1\oplus y=0$
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.	$x_1\oplus y\oplus x_1x_2\oplus x_1y\oplus x_2y=0$

№	Tenglama	№	Tenglama
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.	$x_1\oplus x_2\oplus y\oplus x_1x_2\oplus x_2y=0$
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.

2x1 – o‘lchamli S blok tekshiruv jadvali 4.27-jadval

	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.

2x1 – o‘lchamli S – blok uchun topilgan to‘g‘ri tenglamalar 4.28-jadval

№	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

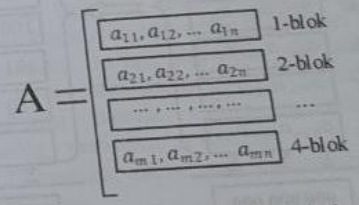
akslantirish o‘lchamiga uzviy bog‘liq bo‘ladi. Masalan, 8x8 – o‘lchamli S – blok uchun $t=137$ bo‘lib, to‘g‘ri tenglamalarni hosil qilishda (1.1) ifodaga ko‘ra 2^{137} ta tenglamani ko‘rib chiqish kerak bo‘ladi. Lekin, mazkur bosqichni parallel hisoblash orqali ham amalga oshirish mumkin.

4.6. Integral kriptoanaliz 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 $a_{1j} \neq a_{2j} \neq a_{3j} \dots \neq a_{mj}$ bajarilsa, ochiq matnlardagi a_{ij} $(i=1 \dots m,\ j=const)$ elementlar *aktiv elementlar* hisoblanadi;

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

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

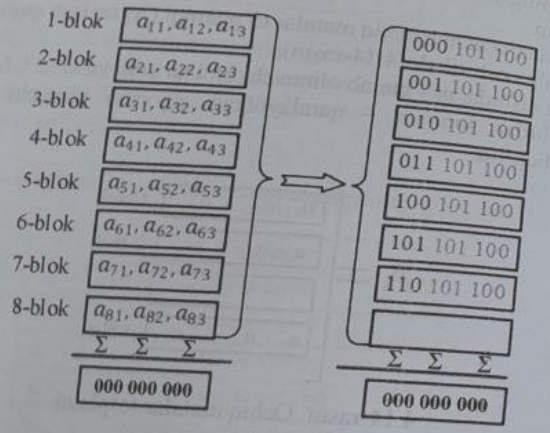
$$\sum_{i=1}^{m} a_{ij} \qquad (4.22)$$

bu yerda $j=1,2,3,\ldots, n$.

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):

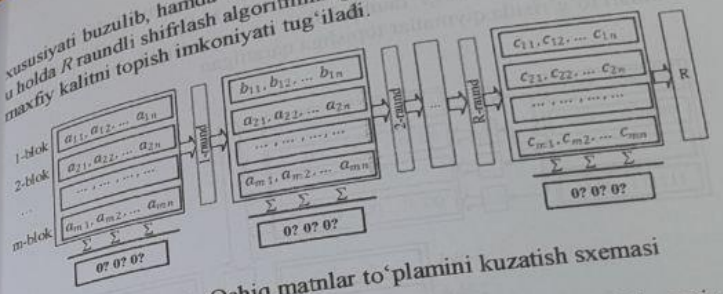


4.15-rasm. Ochiq matnlar to‘plami

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

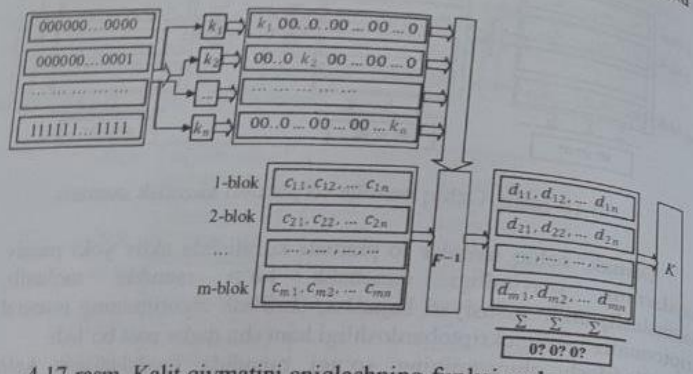
Demak, ochiq matnlar to‘plamini kuzatishda aktiv yoki passiv baytlarning mavjudligi qanchalik ko‘p raundda saqlanib, balanslashganlik xususiyati bajarilsa, shifrlash algoritmining integral kriptoanaliz usuliga kriptobardoshligi ham shu qadar past bo‘ladi.

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.

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'lumotlarni solishtirish orqali oxirgi raund kaliti va keyinchalik barcha raund kalitlari to'g'risida qiymatlar topishga qaratilgan.



4.17-rasm. Kalit qiymatini aniqlashning funksional sxemasi

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_1ni 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:

$$r_1 = 3a_0 \oplus a_1; \qquad (4.23)$$
$$r_2 = 3a_1 \oplus a_0;$$

L^{-1} akslantirishidagi hisoblashlar formulalari esa quyidagicha ko'rinishga ega:

$$a_0 = 3r_1 \oplus r_2; \qquad (4.24)$$
$$a_1 = 3a_0 \oplus r_1;$$

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_1= 0001 1100

P_2= 0010 1100
P_3= 0011 1100
P_4= 0100 1100
P_5= 0101 1100
P_6= 0110 1100
P_7= 0111 1100
P_8= 1000 1100
P_9= 1001 1100
P_{10}= 1010 1100
P_{11}= 1011 1100
P_{12}= 1100 1100
P_{13}= 1101 1100
P_{14}= 1110 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:

$$XOR_{passive}=1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus \oplus 1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus 1100 \oplus =0000$$

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 paydlaridan 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:

$B_0=S(1010\ 1110)=0001\ 1101$
$B_1=S(1011\ 1110)=1110\ 1101$
$B_2=S(1000\ 1110)=0010\ 1101$
$B_3=S(1001\ 1110)=1100\ 1101$
$B_4=S(1110\ 1110)=1101\ 1101$
$B_5=S(1111\ 1110)=1000\ 1101$
$B_6=S(1100\ 1110)=0100\ 1101$
$B_7=S(1101\ 1110)=1001\ 1101$
$B_8=S(0010\ 1110)=1010\ 1101$
$B_9=S(0011\ 1110)=0111\ 1101$
$B_{10}=S(0000\ 1110)=0011\ 1101$
$B_{11}=S(0001\ 1110)=0110\ 1101$
$B_{12}=S(0110\ 1110)=0101\ 1101$
$B_{13}=S(0111\ 1110)=1011\ 1101$
$B_{14}=S(0100\ 1110)=1111\ 1101$
$B_{15}=S(0101\ 1110)=0000\ 1101$

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_1=L(1110 1101)=1001 1100
S_2=L(0010 1101)=1100 1011
S_3=L(1100 1101)=0001 1010
S_4=L(1101 1101)=0101 1001
S_5=L(1000 1101)=0010 0110
S_6=L(0100 1101)=0111 0001
S_7=L(1001 1101)=0110 0101
S_8=L(1010 1101)=1010 0000
S_9=L(0111 1101)=1011 0100
S_{10}=L(0011 1101)=1000 1000
S_{11}=L(0110 1101)=1111 0111
S_{12}=L(0101 1101)=0011 0010
S_{13}=L(1011 1101)=1110 0011
S_{14}=L(1111 1101)=1101 1111
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, Lakslantirishi 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

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.

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.

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

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_3 ni 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

$R_i = L^1(S^{-1}(X(K_i, T)))$

qiymat hisoblanadi. Bu 3-raunddagi 16 ta chiqishga mos keladi. (4.25)

b) Barcha 16 ta R_i qiymatlar uchun XOR amali bajariladi.

c) Agar XOR=0 bo'lsa, K_i ning kutilayotgan bo'lagi to'g'ri topilgan. Aks holda noto'g'ri topilgan va uni K_i 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
T1=1010 1110
T2=0100 1010
T3=0111 0110
T4=1100 1001
T5=1100 1101
T6=0100 1100
T7=0011 0101
T8=0000 1110

$T9=0000\ 1111$
$T10=1010\ 0010$
$T11=1010\ 0110$
$T12=0111\ 1100$
$T13=0110\ 1000$
$T14=1011\ 0111$
$T15=0000\ 0010$

3-qadam bajarilgandan so‘ng, ya’ni $T_i(i=0,\ldots,15)$ 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 ketmaketliklar 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															
	000 0	000 1	001 0	001 1	010 0	010 1	011 0	011 1	100 0	100 1	101 0	101 1	110 0	110 1	111 0	111 1
	$S^{-1}(k_i' \oplus L^{-1}(T_j))$															
1111	1011	0100	1001	1110	0010	0111	1111	1101	0001	0011	1100	0010	0111	1101	1000	0101	1011	0
0010	0101	1010	1000	0000	1100	0001	0011	1100	0110	0010	0111	1111	1101	0100	1001	1110	1010	0
1100	1000	0000	0101	1010	0001	1010	0101	0000	1000	1110	1001	0100	1011	1010	0101	1111	0000	0
1100	1000	0000	0101	1010	0001	1010	0101	0000	1000	1110	1001	0100	1011	1010	0101	1111	0000	0
1111	0110	1100	0011	0001	1010	0000	0101	1010	1011	0100	1010	0101	0000	1011	0111	1111	0100	0
1011	0001	0011	1100	0110	1000	0000	1011	0100	1001	1011	0010	0110	0111	1100	1010	1101	0100	0
1111	1101	1111	0111	0010	1110	1001	0100	1011	0010	0011	1100	0001	1010	0111	1111	1101	0000	0
1111	1101	1111	0111	0010	1110	1001	0100	1011	0010	0011	1100	0001	1010	0111	1111	1101	0000	0
0110	1000	0000	0101	1010	0001	1010	0101	0000	1000	1110	1001	0100	1011	1010	0101	1111	0000	0
0100	1110	1001	0100	1011	0010	0111	1111	1101	0001	0011	1100	0010	0111	1101	1000	0101	1011	0

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 va 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

1011	1000	0000	0101	10 00	0110	1100	0011	0001	1101	1111	0111	0010	1110	1001	0100	1011
1110	1001	1110	1011	10 10	0001	0011	1100	0110	0010	0111	1111	1101	1011	0100	1001	1110
0011	0101	1010	1000	01 00	1111	1101	0010	0111	1100	0110	0001	0011	0101	1010	1000	0000
0101	0101	1010	1000	00 00	1100	0110	0001	0011	1111	1101	0010	0111	1001	1110	1011	0100
0010	1110	1001	0100	00 00	1100	0110	0001	0011	1111	1101	0010	0111	1001	1110	1011	0100
1000	1000	0000	0101	10 11	1101	1111	0111	0010	0110	1100	0011	0001	1010	0101	0000	1000
1100	0001	0011	1100	10 10	0001	0011	1100	0110	0010	0111	1111	1101	1011	0100	1001	1110
(XOR) ∑=	**1111**	**0111**	**1000**	01 10	1000	0000	0101	1010	1011	0100	1001	1110	0010	0111	1111	1101
k' ning ikkinchi yarim bayti uchun nomzodlar				**00 00**	**0101**	**0010**	**1101**	**1010**	**1101**	**0101**	**1010**	**0010**	**1000**	**1111**	***0000***	***0111***

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															
	000 0	**000 1**	**001 0**	**001 1**	**010 0**	**010 1**	**011 0**	**011 1**	**100 0**	**100 1**	**101 0**	**101 1**	**110 0**	**110 1**	**111 0**	**111 1**
	$S^{-1}(k_i' \oplus L^1(T_j))$															
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	0010	0111	1111	0011	0001	1100	1101	1000	0000	1001	1010
1110	1011	0100	1001	1110	1100	0000	1000	1010	0101	0100	1111	0111	0110	0010	1101	1111
0011	0011	0001	0110	1100	0111	1001	1110	0111	0100	0101	1011	1000	0000	1100	0101	1010
0101	1111	1101	0010	0111	1101	1111	1010	1000	0101	0110	1010	1100	0001	1011	0000	1000
0010	1110	1001	0100	1011	1101	0101	1010	1000	0000	1001	1110	1011	0011	1111	0010	0111
1000	1100	0110	0001	1011	0011	0111	0010	1101	1010	1000	0000	1001	1110	1011	0100	1111
1100	0100	1011	1110	1001	0111	0000	1101	0111	1111	1010	1000	0101	0001	0110	1100	0000
(XOR) ∑=	0101	1000	0010	1111	0000											

k' ning birinchi yarim bayti uchun nomzodlar	0100 ва 1101

k' ning 2-qismini (yarim baytini) topish jarayoni *4.37-jadval*

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
.	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_1= 0001 0001
P_2= 0010 0001
P_3= 0011 0001
P_4= 0100 0001
P_5= 0101 0001
P_6= 0110 0001
P_7= 0111 0001
P_8= 1000 0001
P_9= 1001 0001
P_{10}= 1010 0001
P_{11}= 1011 0001
P_{12}= 1100 0001
P_{13}= 1101 0001
P_{14}= 1110 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.

Nazorat 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?
8. SKN1 shifrlash algoritmi uchun integral kriptoanaliz usulini qo'llash natijalari qanday?

V BOB. SIMMETRIK OQIMLI SHIFRLARNING KRIPTOANILIZI

5.1. Oqimli shifrlarga qaratilgan kriptotahlil usullari

Oqimli shifrlarni kriptoanaliz qilish usullari odatda to'liq tanlash (qo'pol kuch) hujumi, statik va analitik turlarga bo'linadi.

To'liq tanlash(qo'pol kuch) hujumi. Ushbu turdagi hujum usuli barcha bo'lishi mumkin bo'lgan variantlarni to'liq shakllantirish va ular orasidan mos kalitni qidirishga asoslanadi. To'liq qidiruvning murakkabligi masalaning barcha mumkin bo'lgan yechimlari soniga bog'liq (hususan, kalitlar yoki ochiq matnlar to'plamiga).

Ushbu hujum turini barcha turdagi oqimli shifrlash tizimlariga qo'llash mumkin. Shuning uchun shifrlash tizimlarini ishlab chiqishda algoritmning ushbu turdagi hujumga bardoshliligini ta'minlash zarur.

Statastik hujum. Statik hujum turi quyidagi ikki turga bo'linadi:

- *shifrlash gammalarining statistik xususiyatlarini kriptoanaliz qilish usuli* - kriptotizimdan chiqish biti biti ketma-ketligini o'rganishga qaratilgan;
- kriptoanalizator navbatdagi chiqish bitining qiymatini har xil statistik testlar yordamida yuqori ehtimollik bilan topishga harakat qilinadi.

Ketma-ketlik murakkabligi kriptoanaliz usuli: kriptoanalitik ketma-ketlikni generatsiyalash usulini, o'xshash qiymatlarni, sodda tarzda amalga oshiriladigan usulda topishga harakat qiladi. Yuqoridagi ikkita usul ham chiziqli murakkablik prinsipidan foydalaniladi. Keyingi tahlil usuli analitik hujum hisoblanadi.

Analitik hujum. Ushbu hujum kriptoanalitik generator tavsifini, ochiq va shifrimatnlarni biladi degan tahmin asasida amalga oshiriladi. Kriptoanalitikning vazifasi foydalanilgan kalitni aniqlash(Registrning dastlabki holatini).

Sinxron oqimlm shifrlash usullariga quyidagi agnalitik hujum usullari qo'llaniladi:

- korrelyatsion (o'zaro bog'livlilik)
- "vaqt-xotira" murosasi
- inversiya

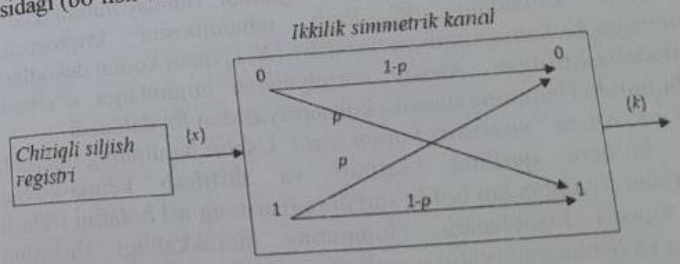
- "taxmin qilish va aniqlash"
- Kalitni yuilash va qayta boshlash
- XSL-hujumi

Korrelyatsion hujum. Bu oqimli shifrlarni buzishga qaratilgan eng keng tarqalgan hujumlardan biri hisoblanadi. Ma'lumki, agar kalit generatsiyasida chiziqli bo'lmagan funksiyalardan foydalanilgan bo'lsa, kriptotizimni buzish sezilarli darajada qiynchilik tug'diradi. Shuning uchun registrlarning dastlabki to'ldirilishini aniqlash uchun korrelatsion hujumlar shifrlash tizimining chiqish qiymatlari ketma-ketligi bilan chiqish registri ketma-ketligi orasidagi o'zaro bog'liqlikni tekshiradi.

Korrelatsion hujumlarning qo'yidagi kichik sinflari mavjud:

- Bazaviy korrelyatsion hujumlar
- Past vaznli imtiyozni tekshirishga asoslangan hujum usuli
- Xatoliklarni tuzatish kodlaridan foydalaniladigan hujum
- Texnik kaskadli kodlardan foydalanilgan hujum
- Chiziqli polinomlarni qayta tiklashga asoslangan hujum
- Tezkor korrelyatsion hujum

Bazaviy korrelyatsion hujumlar. Quyida bir xil uzunlikdagi ikkita ikkilik ketma-ketliklar orasidagi bog'liqlikni Xemming masofasi asosidagi (bo'lish va ochish) Zigentaler hujum usuli keltirilgan.



5.1-rasm. Bazaviy korrelyatsion hujum sxemasi

j-chiziqli siljish registrining ta'sirini ta'sirini aniqlash $\sum(\{x^{(j)}\}$ gamma shifri $\{g\}$ ga bog'liq holda) generatorning bir qismi ikkilik simmetrik kanal (ISK) sifatida modellashtirilgan.

1. $p_j = P(g=x^{(j)})$ korrelatsiya ehtimolini hisoblash ikkkinchi bosqich va f funksiya asosida amalga oshiriladi.

2. Boshlang'ich registr to'liq tanlash usuli yordamida to'ldiriladi. Ushbu qadamda gamma fragmenti $\{g\}$ va $x^{(j)}$ orasidagi bog'liqlik aniqlash, o'zaro bog'liqlilik funksiyasi $C_{x^{(j)},g}(d) = \frac{1}{n} * \sum_{i=1}^{n}(-1)^{a_i} *$

$* (-1)^{x_{i+d}^{[j]}}$ ni hisoblash va uni bir nechta T sonlari bilan taqqoslash orqali amalga oshiriladi.

Agar taqqoslash muvaffaqiyatli bo'lsa, faza to'g'ri deb aytiladi va $j+1$ registrni tekshirishga o'tiladi. Aks holda, faza yaroqsiz deb topildi va $d = d+1, d = 1,2,\ldots,2^{L_j}$ ga o'tiladi.

Past vaznli imtiyozni tekshirishga asoslangan hujum. Ushbu kichik hujum sinfiga Mayyer va Staffelbach tezkor korrelyatsion hujumi misol bo'la oladi. Bu filtr generatorlari uchun ham, birlashtiruvchi generatorlar uchun ham qo'llaniladi va ushbu turdagi barcha tezkor korrelyatsion hujumlar uchun asosiy hisoblanadi. Hujum g'oyasi chiziqli registrning teskari aloqa polinomiga tenglik tenglamalarini yechishga asoslangan.

Tezkor korrelyatsion hujum. Tezkor korrelyatsion hujumlar - bu hujumning hisoblash murakkabligidan sezilarli darajada kam bo'lgan hisoblash murakkabligiga ega bo'lgan hujumlar. Bunday hujum ikkilik nosimmetrik kanaldagi dekodlash muammosini kriptoanaliz muammosigacha kamaytiradi va tasodifiy (N, l) qator kodini dekodlash kabi modellashtirilgan. Asosiy korrelyatsion hujumlarga o'xshash ushbu hujumda Hamming masofa konsepsiyasidan foydalanadi.

"Vaqt-xotira" murosasi hujum usuli. Ushbu hujumning maqsadi ma'lum bo'lgan qurilma sxemasi va shifrlash ketma-ketligi fragmentidan foydalangan holda surish registrining asl holatini tiklash (kalitni topish) hisoblanadi. Hujumning murakkabligi shifrning kattaligiga va ushlangan oraliq uzunligiga bog'liq.

Hujum ikki bosqichdan iborat:

1. barcha turdagi "holat-chiqish" juftliklari yozilgan katta lug'at yaratish;

2. almashtirish registrining dastlabki to'ldirilishini taxmin qilish, chiqishni ishlab chiqarish, ushlangan chiqish ketma-ketligini ko'rish va hosil bo'lgan natijaga moslikni qidirish. Agar mos keladigan bo'lsa,

unda bu taxmin qilingan to'ldirish, ehtimol, boshlang'ich qiymat (kalit) hisoblanadi.

Ushbu turdagi hujumlarga Stiv Babbij va Biryukov-Shomir hujumlari misol bo'la oladi.

"Taxmin qilish va aniqlash" hujumi. Hujum kriptotahlilchi gamma shifri, teskari aloqa polinomini, elektron chiqindilar registr siljishlarining soni va filtr funksiyasini biladi degan taxminga asoslanadi.

Hujum 3 bosqichdan iborat:

1. Resistrning bir qancha qiymatlari taxminiy to'ldiriladi.

2. Kriptotahlilchiga ma'lum axborotlarni hisobga olgan holda registrning to'liq holatini aniqlash;

3. Agar registrning qiymati chiqish gamma shifriga teng bo'lsa unda birinchi bosqichdagi taxmin to'g'ri deb topilib ikkinchi bosqichga o'tish, aks holda 1 bosqichga qaytish.

5.2. Siljitish registrlariga asoslangan shifrlarning kriptoanalizi

Kompyuter tizimlarining rivojlanishi, elektron axborot almashuvining asosiy hujjat almashuviga aylanib kompyuterlarning lokal tarmoqqa yoki Internet tarmog'iga ulanishini taqozo qilmoqda. Tarmoqqa ulangan tashkilot va foydalanuvchilar ma'lumotlarining xavfsizligi shu tarmoqda uzatiluvchi axborotning xavfsizlik darajasiga bog'liqdir. Axborot xavfsizligini ta'minlash tarmoqda uzatilayotgan nafaqat hujjatli axborot almashinuvining oshib borishi bilan, balki multimedia, ya'ni video va ovozli axborot almashinuvining ham oshib borishi natijasida nisbatan tez ishlovchi kriptografik vositalarni talab etmoqda. Shu sababli lokal va global tarmoqda oqimli shifrlash algoritmlarini qo'llash dolzarb muammoga aylanib ulgurgan.

Oqimli shifrlar blokli algortimlardan farqli ravishda axborot oqimining har-bir elementi bo'yicha shifrlab axborotning kriptotizimda ushlanib qolishiga yo'l qo'ymaydi va asosiy yutug'i axborot kirish tezligiga yaqin yuqori tezlikda shifrlab uzatish hisoblanadi.

Shu holatda oqimli shifr axborotning miqdori, oqim razryadidan qat'iy nazar real vaqtda shifrlash hamda kechiktirilmagan holda uzatish imkonini beradi.

Oqimli shifrlash algoritmlarini tahlil qilib ko'rilsa bloklab shifrlash algoritmlaridan farqli ravishda shu paytgacha bu sohada kriptobardoshli sinxronlanuvchi yoki o'z-o'zidan sinxronlanuvchi oqimli shifrlash algoritmlarini yaratishning yagona usullari ishlab chiqilmagan. Ko'plab yo'nalishlar ishlab chiqilgan bo'lishiga qaramasdan ularning bir biri bilan umumiyligi yo'q.

Oqimli shifrlash tizimlarida psevdotasodifiy ketma-ketlikni ishlab chiquvchi generatorlar ushbu tizimning ajralmas qismi hisoblangan holda tizimning bardoshliligi ham to'liq holda ushbu generatorlarning ichki strukturasiga bog'liq. Oqimli shifrlarning haqiqiy bardoshliligi bir alfavitli o'rin almashtirish va bir martalik bloknot orqali shifrlash algoritmlari bardoshliligi oralig'ida yotadi. Bir martalik bloknot orqali shifrlash Shennon tomonidan kiritilgan bo'lib, amalda bir martalik bloknot bilan shifrlashni amalga oshirish uchun juda katta uzunlikdagi haqiqiy tasodifiy kalitlar ketma-ketligini generatsiya qilish, bloknot yoki fayl holatida yozib olish va uni kafolatlangan yopiq kanal orqali uzatish qiyinchiligini, shuningdek katta hajmga ega kalitlar to'plamining maxfiyligini saqlash masalasini yechishga olib keladi. Bu masalaning yechimi sifatida esa faqat yetarlicha katta uzunlikdagi tasodifiylik darajasi yuqori bo'lgan psevdotasodifiy ketma-ketlik hosil qiluvchi generatorlarni, ya'ni oqimli shifrlash algoritmlariga asoslangan kriptotizimlarini ko'rsatish mumkin. Bunday kriptotizimlarda kichik o'lchamli maxfiy kalitdan katta uzunlikdagi psevdotasodifiy gamma hosil qilinadi. Kichik o'lchamli maxfiy kalitni saqlash va assimetrik kriptotizim orqali uzatish qiyinchilik tug'dirmaydi.

Psevdotasodifiy kalit ketma-ketlikni ishlab chiquvchi generator hosil qilgan ketma-ketlik ko'rinishi haqiqiy tasodifiy ketma-ketlikka o'xshagani bilan ushbu ketma-ketlik aynan shunday holatda kalitni hosil qilgan holda yana qaytadan ishlab chiqilishi mumkin. Bu xususiyat oqimli shifrlarning amaliyotda samarali qo'llanilishini ta'minlab, oqimli shifrlar bardoshliligi darajasini bir martalik bloknot bilan shifrlash darajasigacha yetkazish imkonini beradi.

Telekommunikatsiya tarmoqlarining tez rivojlanishi, himoyalangan tranzaksiyalar, pochta aloqasi, internet saytlar, audio va video axborotlar almashinuvining ishonchli himoyasini amalga oshirish kriptografiyaga bo'lgan qiziqishning keskin oshishiga olib keldi. Shu

bilan birga tez ishlovchi va kriptobardoshli oqimli shifrlash algoritmlariga talabni oshirdi. Tez ishlovchi kriptografik vositalar asosan apparat va apparat-dasturiy vositalarda amalga oshirilishi mumkin. Kompyuter tarmoqlarining rivojlanishi o'z navbatida dasturiy kriptografik vositalarga bo'lgan talabni kuchaytirmoqda. Kompyuter tizimlarining asosidagi raqamli protsessorlarining 64 bitli platformaga o'tkazilishi dasturiy vositalarda shifrlash amalini bitlarda emas, balki bayt, 16, 32, 64 bitli so'zlarda samarali amalga oshirish imkoniyatlarni ochib berdi.

Oqimli shifrlash algoritmlari gammalashga asoslangan shifrlash bo'lib, ochiq matnning ketma-ket keluvchi har bir 1 bitini (1 baytini) generatordan chiqqan mos 1 bit (1 bayt) gamma kalitga XOR akslantirishi bilan qo'shish orqali shifrmatnga aylantiradi.

$$c_i = p_i \oplus k_i \tag{5.1}$$

Qabul qiluvchi olingan shifrmatnni (5.1) xuddi shu generatordan faqat axborot almashinuvchi abonentlargagina ma'lum bo'lgan maxfiy simmetrik kalitdan foydalanib hosil qilingan mos 1 bit (1 bayt) gammaga qaytadan XOR akslantirishi bilan qo'shish natijasida ochiq matnni (5.2) keltirib chiqaradi.

$$c_i \oplus k_i = p_i \oplus k_i \oplus k_i = p_i \tag{5.2}$$

Shu sababli oqimli shifrlarga asoslangan kriptotizimlarning bardoshliligi mana shu shifrlash algoritmida qo'llanilgan generatorning bardoshliligi bilan teng kuchlidir. Generatorning bardoshliligi esa hosil qilingan ketma-ketlikning takrorlanmas davri va tasodifiylik darajalari bilan baholanadi. Agar generator har seansda bir xil bo'lgan ketma-ketlikni bersa yoki takrorlanmas davri qisqa bo'lsa, bu orqali shifrlangan ikkita shifrmatnni XOR orqali qo'shib ikkita ochiq matnning XOR yig'indisiga $p_1 \oplus p_2$ ega bo'lish mumkin. Bu shifrmatnni ochish ko'p alfavitli shifrmatnni ochish qiyinchiligiga tenglashib qoladi, bu kriptohujumni osonlashtiradi. Agar ochiq matn qaysi tilda yozilganligi ma'lum bo'lsa, ochiq ma'lumotni tiklash barcha simvollarni to'liq ko'rib chiqish bilan teng kuchli.

$$p_1 \oplus k_1 = c_1, \qquad p_2 \oplus k_2 = c_2,$$
$$c_1 \oplus c_2 = p_1 \oplus k_1 \oplus p_2 \oplus k_2 = p_1 \oplus p_2 \qquad (5.3)$$

Oqimli shifrlar sinxron yoki o'z-o'zidan sinxronlanuvchi bo'lishi mumkin. Sinxron shifrlarda generatsiya qilingan gamma ketma-ketlik shifrlanuvchi ochiq matnga bog'liq emas. Bunday oqimli shifrlarda asosiy qiyinchilik sifatida jo'natuvchi va qabul qiluvchi o'rtasida ketma-ketliklarni mos ravishda aniq sinxronlashishni ko'rsatishimiz mumkin. Agar hosil qilingan shifrmatnni jo'natish paytida bir bit tushib qolsa yoki bir bit qo'shilib qolsa, buning natijasida qabul qilingan shifrmatnning ortiqcha qo'shilgan yoki tushirib qoldirilgan bitidan keyingi barcha ketma-ketlik bitlari noto'g'ri deshifrlanadi. Noto'g'ri deshifrlanish ma'lum bo'lib qolsa jo'natuvchi va qabul qiluvchi tomon qaytadan sinxronlashishga (moslashishga) majbur bo'ladi. Qayta sinxronlashish paytida noto'g'ri qabul qilingan ochiq matnni qaytadan uzatish boshqa gamma ketma-ketligi bilan amalga oshirilishi lozim, ya'ni tizimning bardoshliligini ta'minlash maqsadida bir marta ishlatilgan gamma ketma-ketligi qayta shifrlashda ishtirok etmasligi talab qilinadi. Sinxronlanuvchi oqimli shifrlarning yaxshi xususiyatlaridan biri hosil qilingan shifrmatnni uzatish va qabul qilish oralig'ida biror bit noto'g'ri qabul qilinsa, bu xatolik boshqa bitlarga ta'sir qilmasligidir. Sinxronlanuvchi oqimli shifrlash tizimlarida kanalda uzatilayotgan shifrmatnning alohida qismlarini olib qolish yoki qo'shimcha imitovstavka qo'shish imkonining yo'qligidir. Agar shunday bo'lsa qabul qiluvchi tomonidan xato darxol aniqlanib, qabul qiluvchi jo'natuvchi bilan qayta sinxronlashishni boshlaydi. Bu shifrlarning kamchiligi shundan iboratki, o'rtada turgan kriptoanalizchi o'ziga kerakli bo'lgan ma'lumot oqimning qaysi qismida bitlar joylashgan o'rnini bilib qolsa faqat shu qismini o'zgartirib ochiq matnning mazmunini o'zgartirishga erishishi mumkin. Kriptoanalizchi tomonidan kiritilgan bunday o'zgartirish qabul qiluvchi tomonidan aniqlanmasdan qoladi.

O'z-o'zidan sinxronlashuvchi oqimli shifrlash tizimlarida qo'llanilayotgan generatorning ichki holati qabul qilinayotgan shifrmatnga bog'liq bo'ladi. Agar shifrmatnning bir biti xato qabul qilingan bo'lsa, shu qabul qilingan bitdan keyingi ochiq matn noto'g'ri deshifrlanadi. Jo'natuvchi har seansda ochiq matn oldiga n bitli

tasodifiy qiymatni qo'shib jo'natganligi sababli bu oqimli shifrlash tizimi o'z-o'zidan sinxronlashuvchi deb ataladi. Qabul qiluvchi tomon shifrmatn boshida turgan n bitli tasodifiy qiymatni deshifrlaydi, bu matn tushunarsiz bo'lgani bilan davomida keluvchi ochiq matnni qabul qilish uchun sinxronlashishga erishadi.

Barcha oqimli shifrlash algoritmlari bir tomonlama hisoblanuvchi juda ham uzun psevdotasodifiy ketma-ketliklarni keltirib chiqaradi. Mana shu hosil qilingan ketma-ketlikning ichi bitini (baytini) hosil qilish yo'li faqat bitta bo'lib, u ham bo'lsa i -bit(bayt)gacha bo'lgan barcha bit(bayt)larni generatsiya qilish kerak bo'ladi. Oqimli shifrlarda i - bit(bayt)ni hosil qilish uchun shu i -bit(bayt)gacha bo'lgan bit(bayt) larning barchasini generatsiya qilish shart emas, balki i -bitni bilgan holda shu bit(bayt)ni oson generatsiya qilish mumkin. Oqimli shifrlarning bu xossasidan vinchester klasterlarini shifrlashda ishlatish mumkin. Shifrlash jarayonida nolinchi klasterdan boshlab oxirigacha barcha klasterlar ketma-ket shifrlab chiqiladi. Deshifrlashda esa har bir klasterning tartib raqamini va bitta klasterning hajmini (bitlarda) bilgan holda ixtiyoriy klasterni alohida-alohida deshifrlab ochiq ma'lumotni hosil qilish, qayta ishlash, vinchesterga yozish paytida qayta shifrlab yozish mumkin bo'ladi.

Oqimli shifrlash tizimlarida qo'llaniladigan generatorlarning yana bir asosiy xarakteristikasi ushbu generatorlar hosil qilgan ketma-ketlikning tasodifiylik darajasidir. Hosil qilingan ketma-ketliklar bloklarining tasodifiylik darajasi ma'lum bir kriteriyalar orqali baholanadi. Tasodifiylik darajasi yuqori bo'lgan psevdotasodifiy sonlar ketma-ketligini ishlab chiqaruvchi generatorlar zamonaviy kriptotizimlarning ajralmas qismi hisoblanadi. Tasodifiy ketma-ketliklar kriptografiyada qo'llanilish maqsadlarini quyida ko'rsatib o'tishimiz mumkin:

- simmetrik kriptotizimlar uchun tasodifiylik darajasi yuqori bo'lgan seans kalitlari va boshqa kalitlarni generatsiya qilish;
- asimmetrik kriptotizimlarda qo'llaniladigan katta uzunlikka ega matematik kattaliklar uchun tasodifiy boshlang'ich qiymatlar generatsiyasi, masalan katta tub sonlar generatsiyasi uchun;

• blokli algoritmlarning boshlang'ich tasodifiy qiymat talab qiluvchi SVS, OFB va boshqa rejimlari uchun boshlang'ich tasodifiylik darajasi yuqori bo'lgan vektorlar hosil qilib berish;

• elektron raqamli imzo tizimlari uchun kerak bo'lgan katta uzunlikka ega parametrlar uchun dastlabki tasodifiy qiymatlar generatsiyasi;

• bitta protokol orqali bir xil ma'lumotlarni har-xil jo'natish uchun talab qilinadigan kerakli uzunlikdagi tasodifiy qiymatlarni hosil qilib berish, masalan SSL va SET protokollarida.

Ixtiyoriy ehtimollik taqsimoti qonuniyati bilan tasodifiy ketma-ketlik hosil qilish muammosi oxir-oqibatda tekis taqsimlangan ketma-ketlik generatsiyasi muammosiga keladi. Tekis taqsimlangan ketma-ketliklar uchun ixtiyoriy tN, tasodifiy qiymat $x_t \cdot A$ ketma-ketlik to'plamidagi elementning diskret tekis-taqsimlangan extimolligi $P\{x_t, A\} = 1/N$ ga tengdir. Agar ushbu A ketma-ketlik to'plamidagi har bir elementining hisoblangan ehtimolliklarining kvadratik farqlari $[0,05; 0,95]$ oraliqda yotsa bu ketma-ketlikni tasodifiy ketma-ketlik deb olish mumkin bo'ladi.

Tekis taqsimlangan ketma-ketliklarning xossalaridan biri bu ikkita ketma-ketlik $A(a_i)$- tekis taqsimlangan tasodifiy va $V(v_i)$ tekis taqsimlangan va tasodifiy bo'lmagan ketma-ketliklar berilgan bo'lsa u holda $S(s_i) = A(a_i) \oplus V(v_i)$ natijaviy ketma-ketlik tekis taqsimlangan tasodifiy ketma-ketlik bo'ladi. Bu xossadan algoritmlarni kombinatsiyalashda qo'llash maqsadga muvofiq bo'ladi.

Tekis taqsimlangan tasodifiy ketma-ketliklar haqiqiy tasodifiy ketma-ketliklarga va psevdotasodifiy ketma-ketliklarga bo'linadi.

Tekis taqsimlangan tasodifiy ketma-ketlikni 2 xil yo'l bilan ishlab chiqish mumkin:

- fizik generatorlar orqali;
- dasturiy generatorlar orqali.

Bu birinchi usul: fizik generatorlar orqali ishlab chiqilgan haqiqiy tasodifiy ketma-ketlik bo'lib bu ketma-ketlik bir martagina ishlab chiqilib uni keyinchalik biror bir qonuniyat bilan xuddi shunday ishlab chiqish mumkin emas. Shu sababli fizik generatorlarni gamma kalitlarini hosil qilish shifrlash uchun uchun qo'llash mumkin emas.

Ikkinchi usul: dasturiy generatorlar orqali ishlab chiqilgan psevdotasodifiy ketma-ketlik bo'lib - bu tekis taqsimlangan ketma-ketlikni boshlang'ich kalit qiymatini bilgan holda xuddi shunday yetarlicha uzunlikda qaytadan ishlab chiqilishi mumkin.

Tasodifiy ketma-ketlik ishlab chiquvchi generatorlar tabiiy hamda tasodifiy fizik hodisalarga asoslangan bo'ladi. Tasodifiy ketma-ketlikni hosil qilishning bunday metodlari maxsus apparatura va uskunalarni talab qiladi. Lekin bunday fizik xodisalarni kompyuterda ham olish mumkin. Masalan PGP tizimida haqiqiy tasodifiy ketma-ketliklar klaviatura bosilish vaqtini 32 bitli formatda hisoblash, bosilgan simvolning 8 bitli qiymati, ketma-ket bosilgan klaviatura tugmalari oralig'idagi vaqt miqdori, operatsion xotiraga murojaat vaqti va boshqa parametrlar ustida matematik amallar bajarish orqali hosil qilinadi. Kompyuterning videokartasi shovqini asosida va operatsion tizim murojaat qilgan tasodifiy operativ xotira yoki vinchester xotirasi adreslarini ikkilik tizimga o'tkazish va ular orasida XOR akslantirishini bajarish orqali ham haqiqiy tasodifiy ketma-ketlikni hosil qilish mumkin.

Yuqorida ko'rsatib o'tilgan amaliy masalalarni yechishda haqiqiy tasodifiy ketma-ketliklar ishlab chiquvchi tasodifiy fizik hodisalarga asoslangan generatorlarni ishlatish juda ko'p hollarda qiyinchiliklar keltirib chiqaradi. Chunki, smart kartalar, avtonom tizimlar va boshqalarda tasodifiy ketma-ketlik hosil qiluvchi generator uchun hech qanday tasodifiy fizik hodisa manbai mavjud emas, mavjud bo'lganlari esa tasodifiylik va bardoshlilik talablariga umuman javob bermaydi. Masalan, SSL protokolida to'xtovsiz tasodifiy ketma-ketliklar, Kerberos protokoli qo'llanishida tarmoq serveri har soatda minglab sessiya kalitlarini ishlab chiqishi lozim, shu sababli hattoki zamonaviy kompyuterlardagi tasodifiy hodisalarni hisobga olgan holda ishlaydigan fizik generatorlar orqali chekli vaqt mobaynida yetarlicha miqdorda haqiqiy takrorlanmas va tasodifiylik darajasi yuqori bo'lgan ketma-ketliklar ishlab chiqish murakkab holat hisoblanadi. Shu hollarda yetarlicha katta davr uzunligiga ega va tasodifiylik darajasi yuqori bo'lgan ketma-ketliklar hosil qiluvchi dasturiy psevdotasodifiy ketma-ketliklar generatorini ishlatish maqsadga muvofiqdir.

Oqimli shifrlash tizimlarida shifrlash bilan birga deshifrlash tez bo'lishi uchun faqat psevdotasodifiy hamda, tekis taqsimlangan

tasodifiy ketma-ketliklar hosil qiluvchi dasturiy generatorlar qo'llanadi. Shu paytgacha mavjud bo'lgan tekis taqsimlangan ketma-ketlik ishlab chiqish generatorlar va ular asosidagi oqimli shifrlash tizimlari ma'lum bir yondashuvlar asosida yaratilgan.

Hozirgi paytdgacha mavjud bo'lgan psevdotasodifiy ketma-ketliklar ishlab chiquvchi dasturiy generatorlarga asoslangan algoritmlarni yaratish yo'nalishlarini klassifikatsiyalashda uch xil asosiy yondashuvni ko'rsatishimiz mumkin.

1. Tizimli-nazariy yondashuv yo'nalishidagi psevdotasodifiy ketma-ketliklar generatorlari asosida yaratilgan algoritmlar.

2. Murakkablikka asoslangan nazariy yondashuv yo'nalishidagi psevdotasodifiy ketma-ketlik generatorlari asosida yaratilgan algoritmlar.

3. Kombinatsiyalash yo'nalishidagi psevdotasodifiy ketma-ketlik generatorlari asosida yaratilgan algoritmlar.

Tizimli-nazariy yondashuv asosida qurilgan oqimli shifrlash algoritmning kriptobardoshliligi fundamental matematik kriteriyalar va qonuniyatlari hisobga olingan holda shu paytgacha murakkab va noma'lum bo'lgan, hamda yechish yo'li yo'q deb hisoblangan muammoning qiyinchiligiga tenglashtiriladi.

5.3. RC4 shifrining kriptoanalizi

RC4 oqimli shifrlash algoritmi bo'lib, u SSL(Secure Sockets Layer) protokoli va WEP (simsiz tarmoqlarda xavfsizlikni ta'minlashda) keng foydalaniladi. RC4 oqimli shifrlash algoritmi Ron Rivest tomonidan 1987 yilda yaratilgan va shuning uchun RC4(Rivest Cipher 4) deb nomlangan.

RC4 psevdotasodifiy bitlar ketma-ketligini hosil qiladi va quyidagi ikki qismdan iborat bo'lgan maxfiy oraliq holatidan foydalaniladi:

- barcha mumkin bo'lgan 256 baytning joylashishdagi o'rni(*S* ni topish);
- ikkita 8 – bitli indekslar (*i* va *j* larni topish).

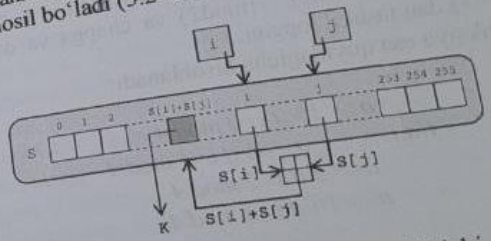
Baytlarning kelish tartibi kalit uzunligi bilan amalga oshiriladi, odatda 40-256 bit oralig'ida bo'lib, kalit jadvali(key-scheduling) algoritmi orqali hosil qilinadi. Bu jarayon tugagandan so'ng

psevdotasodifiy sonlar generatori algoritmi yordamida bitlar ketma-ketligi hosil qilinadi.

Kalit jadvali algoritmi quyidagicha:

```
for i from 0 to 255
S[i]:=i
endfor
j:=0
for i from 0 to 255
j := (j + S[i] + key[i mod keylength]) mod 256
swap values of S[i] and S[j]
endfor
```

Psevdotasodifiy sonlar generatori algoritmi orqali hosil bo'lgan ketma-ketlik tanlangan $S(i)$ va $S(j)$ o'zgaruvchilarni *mod*256 bo'yicha qo'shishdan hosil bo'ladi (5.2- rasm).



5.2-rasm. RC4 generatori almashtirishi

Psevdotasodifiy sonlar generatori algoritmi quyidagicha:

```
i := 0
j := 0
while GeneratingOutput:
 i := (i + 1) mod 256
 j := (j + S[i]) mod 256
 swap values of S[i] and S[j]
 k := inputByte XOR S[(S[i] + S[j]) mod 256]
 output K
```

endwhile

Algoritmda *i* o'zgaruvchini qiymati ortishi bilan hosil bo'lgan baytlar soni ham ortib boradi.

Bu yerda almashtirish funksiyasi *swap* quyidagi ko'rinishga ega:

```
byte temp = array[ind1];
array[ind1] = array[ind2];
array[ind2] = temp;
```

Ushbu generator kriptobardoshli sanalib, xususiyati kiruvchi kalit tasodifiylik darajasi bilan belgilanadi. Hozirda ushbu algoritmning bir nechta variantlari mavjud bo'lib (RC4A, VMPC, RC4+), ularda dastlabkilarida mavjud kamchiliklar bartaraf etilgan.

ISAAC. Ushbu PTSKK(Psevdotasodifiy sonlar ketma-ketligi) generatori 1966 yilda Robert Jenkins tomonidan yaratilgan bo'lib, RC4 algoritmiga o'xshashdir. Kiruvchi parametr sifatida 32 bit o'lchamdagi so'zlardan iborat bo'lgan 256 uzunlikdagi massiv olinadi. Chiqishning har bir bosqichida xuddi shu o'lchamdagi massiv hosil bo'ladi. Ushbu PTSKK generatorida ^(XOR), +(mod2) va chapga va o'nga surish amallari(<<, >>) dan tashkil topgan.

f(a,i) funksiya esa quyidagicha hisoblanadi:

$$f(a,i)=\begin{cases} a<<13 \text{ if } i=0 \bmod 4 \\ a>>6 \text{ if } i=1 \bmod 4 \\ a<<2 \text{ if } i=2 \bmod 4 \\ a>>16 \text{ if } i=3 \bmod 4 \end{cases}$$

bu yerda i {0,…..,255} oraliqqa tegishli son.

Ushbu generatorning algoritm kiruvchi parametrlar a, b, c va s holat massivi, 256 o'lchamga ega bo'lgan 32 bitli so'zlardan tashkil topgan.

Chiqish r massiv, 256 o'lchamli 32 bitli so'zdan iborat bo'ladi.

1: $c \leftarrow c + 1$
2: $b \leftarrow b + c$
3: for $i = 0, \ldots, 255$ do
4: $x \leftarrow s_i$
5: $a \leftarrow f(a, i) + s_{i+128 \bmod 256}$
6: $s_i \leftarrow a + b + s_{x>>2 \bmod 256}$

7: $r_i \leftarrow x + s_{x>>10 \bmod 256}$
8: $b \leftarrow r_i$
9: end for
10: return r

Ushbu generator bardoshli generator sanalib, undagi mavjud kamchiliklar *ISAAC+* generator algoritmida tuzatilgan. Ushbu generatorda bir necha marta nazariy hujumlar amalga oshirilgan, ammo amaliy tomondan hujumga uchramagan.

5.4. ORYX shifrining kriptoanalizi

ORYX oqimli shifrlash algoritmi Amerikada uyali aloqa tarmoqlari orqali uzatiladigan ma'lumotlarni shifrlash uchun ishlatilgan. A5 algoritmida bo'lgani kabi, ushbu kriptosxemaning muallifi noma'lum va uning tavsifi Internet tarmog'ida fuqarolarning ma'lumot olish erkinligi uchun anonim shaxs tomonidan nashr etilgan.

Kriptoalgoritm to'rt komponentga asoslangan: uchta 32-bitli LFSR, A, B va K sifatida belgilanadi. 0 dan 255 gacha bo'lgan qiymatlar uchun ma'lum L almashtirishni o'z ichiga olgan bitta S-box. Kalit uchta registrni dastlabki to'ldirishdir, ya'ni jami 96 bit. Kalitni ochishning ancha murakkab algoritmi mavjud bo'lib, u kalit bo'shlig'ini to'liq qidirish orqali kalitni qidirishda osongina tekshiriladigan o'lchamga qisqartiradi. Barcha hisob-kitoblarga ko'ra, bu kriptoalgoritmning eksport versiyasini zaiflashtirish uchun ataylab qilingan. Biroq, kalitni ochish algoritmining yaxshiroq versiyasi bilan 96 ta teng ehtimolli kalit bitlari etarlicha kuchli kriptosxemasini ta'minlaydi deb taxmin qilingan.

ORYX ochiq matn baytlariga XOR amali bilan hisoblangan baytlarning psevdo-tasodifiy ketma-ketligini yaratish orqali ma'lumotlarni shifrlaydi. Har bir gamma bayt quyidagi tarzda hosil qilinadi:

1. LFSR K bir marta o'zgartiriladi;
2. LFSR A registrning K bit qiymatiga qarab ikki xil teskari polinomlardan biri yordamida bir marta siljiydi.
3. LFSR B ro'yxatdan o'tish K boshqa bitning qiymatiga qarab bir yoki ikki marta siljiydi.

4. A, B va K registrlarining yuqori baytlari bir-biri bilan birlashtirilib bayt hosil qiladi

gamma shifrlash quyidagicha:

$$gamma = High8(K) \oplus L[High8(A)] \oplus L[High8(B)],$$

bu erda $High8$ - registrning yuqori 8 bitini olish operatsiyasi, L esa $Sbox$ almashtirish qo'llanilishi.

ORYX algoritmining kriptoanalizi 1997 yil may oyida Devid Vagner (Kaliforniya universitetining aspiranti, Berkli, bir qator muvaffaqiyatli kriptoanalitik ishlari bilan tanilgan), Bryus Shnayer (Amaliy kriptografiya muallifi va Counterpane Systems kripto konsalting kompaniyasi prezidenti) va Jon Kelsi (Counterpane Systems kompaniyasining kriptonalist) Internetda ORYX kripto sxemalarining jiddiy zaif tomonlarini ko'rsatuvchi maqola chop etishdi. Xususan, ular muvaffaqiyatli bo'lish uchun 24 bayt ma'lum ochiq matn va 2^{16} marta (boshlang'ich holatning sinovlari) talab qilinadigan hujumni taqdim etdilar. Ushbu usul kalitni ochish algoritmining turidan qat'i nazar, kalitning dastlabki holatini ochib beradi.

Hujum "bo'lish va ochish" texnikasiga asoslanadi, bu erda boshlang'ich axborotning nisbatan kichik qismini taxmin qilish va taxminning to'g'riligini tekshirish orqali generator bosqichma-bosqich buziladi. Faraz qilaylik, A, B va K registrlarning yuqori 8 bitlari ma'lum bo'lsin. Unda har bir chiqish bayti uchun K va A ularda bitta noma'lum bit siljishi, B ning esa bir yoki ikkita shunday noma'lum bitlari borligidan foydalanishi mumkin. Ushbu kuzatish parametrlarning barcha mumkin bo'lgan qiymatlarini sinab ko'rish imkonini beradi. Jami 24 ta mumkin bo'lgan chiqishlar mavjud. Agar 8 ta muhim bit taxmini to'g'ri bo'lsa, keyingi gamma bayt taxmin qilingan 24 baytdan biri bo'lishi kerak. Agar taxmin noto'g'ri bo'lsa, u taqriban 29/32 holatda aniqlanadi. Bundan tashqari, agar taxmin to'g'ri bo'lsa, bu odatda K, A va B dagi yangi qiymatlarning yagona mumkin bo'lgan to'plamini beradi, bu esa tegishli registrlar haqidagi ma'lumotlarni oshiradi.

Hujumning chuqur tavsifiga to'xtalmasdan, shuni ta'kidlash mumkinki, uning shakli induksiya bilan dalilga o'xshaydi. Barcha uchta registrning 8 ta eng muhim biti olinishi bilanoq, qolgan barcha bitlar

tiklanadi. To'g'ridan-to'g'ri A va B ning yuqori 8 bitlari haqidagi taxmin K registrining muhim 8 bitlari haqida gapirayotganini to'g'ridan-to'g'ri ko'rish mumkin. Umuman olganda, bu usul shifrlash diapazonining taxminan 24 bayti mavjud bo'lganda imkon beradi. Vagner, Shnayer va Kelsi o'z tadqiqotlarida, ORYX kriptotizimi kriptografik hamjamiyat tomonidan tegishli har tomonlama o'rganilmasdan keng ommoga e'lon qilingan. Amalga oshirilgan tadqiqotlar usbu shifrning zaiflikka ega ekanligini ko'rsatdi degan fikrlarni bildirgan.

5.5. PKZIP shifrining kriptoanalizi

Ushbu algoritmda uchta 32-bitli o'zgaruvchilardan foydalaniladi: $K0 = 305419896$; $K1 = 591751049$; $K2 = 878082192$.

$K2$ dan olingan 8 bitli $K3$ kaliti ishlatiladi.

Algoritm (standart C yozuvida) quyidagicha:

```
Ci=Pi^K3;
K0=src32 (K0,Pi);
K1=K1+ (K0 va 0x000000ff);
K1= K1*134775813 + 1;
K2 = src32 (K2, K1 >> 24);
K3 = ((K2|2)*((K2 | 2)^1))>>8.
```

$CRC32$ funktsiyasi o'zining oldingi qiymat baytini oladi, ularni XOR amali yordamida qo'shadi va $0xcdb88320$ tomonidan aniqlangan CRC polinomi yordamida keyingi qiymatni hisoblaydi.

Amalda, 256 elementli jadvalni muddatidan oldin hisoblash mumkin va bu $CRC32$ hisobida quyidagiga teng:

$$crc32(a,b) = (a << 8)^{\wedge} jadval\,[(a\&\ 0xff)\ xor\ b].$$

To'g'ri matn oqimini shifrlash uchun kalitlarni yangilash uchun avval shifrlash algoritmidagi kalit baytlari aylantiriladi. Qabul qilingan shifrmatn bu bosqichda e'tiborga olinmaydi. Keyin ochiq matn bayti shifrlanadi. To'g'ri matndan oldin 12 ta tasodifiy bayt mavjud, ammo bu muhim emas.

Ushbu algoritmning xavfsizligi unchalik katta emas. Hujum uchun 40 dan 2000 baytgacha ma'lum ochiq matn kerak bo'ladi. Agar siqilgan faylda standart sarlavhalar ishlatilsa, hujum yanada osonlashadi.

5.6. Psevdotasodifiy sonlar generatorini baholash usullari

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:

$(w,\ n,\ m,\ r) = (32, 624, 397, 31)$;
$a = 9908B0DF_{16}$;
$(u,\ d) = (11, FFFFFFFF_{16})$;
$(s, b) = (7, 9D2C5680_{16})$;
$(t, c) = (15, EFC60000_{16})$;
$l = 18$.

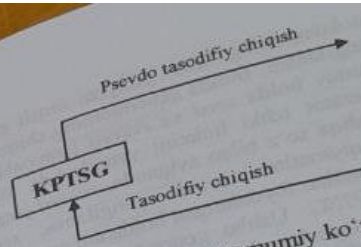
Bu yerda: w- so'z uzunligi (bitda), n – takrorlanish darajasi, m – foydalaniluvchi o'rta so'z, r – bir so'zning ikkiga bo'linish nuqtasi, a – twist matritsasi uchun koeffisent, b, c – almashtirish bit maskalari, s, t – almashtirishdashi siljitish bitlari, u, d, l – qo'shimcha siljitish va maska parametrlari. 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 }
```

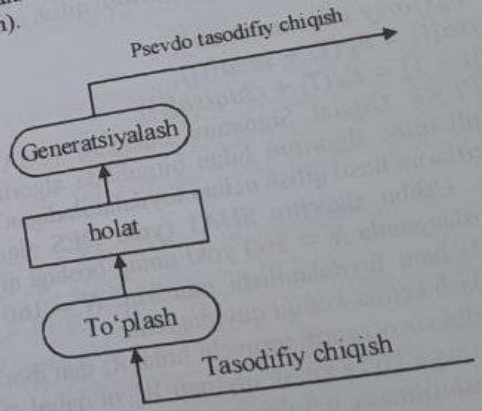
Ushbu generatorda almashtirish funksiyasi sifatida bir tomonlama funksiyadan foydalanilmaganiligi sababli, xavfsiz emas deb qaraladi. Ushbu generatorning keyingi versiyalarida tezkorlikni oshirishga harakat qilingan (TinyMT).

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. $T_i = E_K(joriy\ vaqt\ metkasi)$;

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:

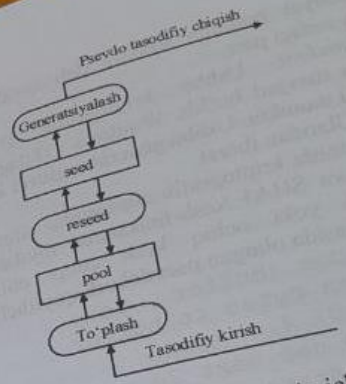
1. KPTSG uzluksiz o'zgarib turuvchi holat X_i dan iborat.

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.

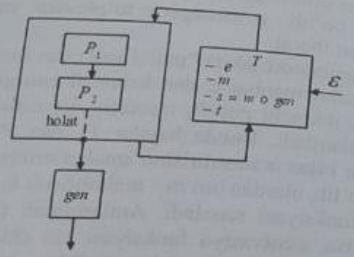
/dev/random generatori ikkita "pul" (pool) dan iborat. Birlamchi pul $\mathcal{P}_1$ tashqi hodisalar manbai $\mathcal{E}$ dan keluvchi entropiyani to'plash uchun foydalanilsa, ikkinchi pul $\mathcal{P}_2$ tasodifiy qiymatlarni generasiya qilish uchun foydalaniladi. Bunda baytlar $\mathcal{P}_1$ dan $\mathcal{P}_2$ ga ko'chirib o'tkaziladi. "Pul"lar bilan aralashtirishni amalga oshirish uchun ikkita funksiya mavjud bo'lib, ulardan biri m – aralashtirish funksiyasi pulga – 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.

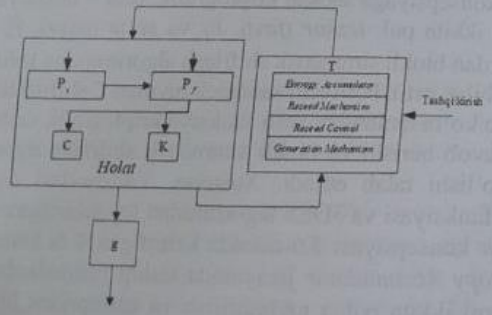
Yarrow konsepsiyasi 5.6-rasmda keltirilgan 4 ta komponentdan iborat. *Entropy Accumulator* jarayonida tashqi manbalardan kiruvchi ma'lumotlarni ikkita pulga joylashtirish va entropiyani hisoblashdan iborat. *Reseed Mechanism* jarayonida holat talabdagi kabi bo'lsa pullardan yangi kalit hosil qilinadi. *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.



5.6-rasm. /dev/randomning umumiy strukturasi

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.

5.7. Tasodifiylikka tekshirish testlari

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
4.	Alfred Menezes, et. al./CRC Press, Inc.	Handbook of Applied Cryptography	
5.	Pierre L'Ecuyer, Richard Simard/ Université 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 Template Matchings	Kesishmagan shablonlarni qanchalik ko'p payd bo'lishini
8.	Overlapping Template Matchings	Birlarning *m* bitli yugirishlarni paydo bo'lishi
9.	Universal Statistical	Siqilishni (biror qoniniyatga asoslanishini)
10.	Random Excursions	Tasodifiy yurishda yagona holatga o'tishlar son 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'ishi

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)
	Chastota (Frequency) testi	100
	Bloklar uchun chastota (Frequency Test within a Block) testi	100
	Yugurishlar (Runs) testi	100
	Blok ichidagi eng uzun yugurish (Longest Run of Ones in a Block) testi	128
	Birlik matrisa rangini hisoblash (Binary Matrix Rank) testi	38912
	Diskret Furye almashtirishlari (Discrete Fourier Transform) testi	1000
	Davriy bo'lmagan qismlar (Non-overlapping Template Matching) testi	10^6
	Davriy bo'lgan qismlar (Overlapping Template Matching) testi	10^6
	Maurerning «Universal statistik» (Maurer's «Universal Statistical») testi	387840
	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) testi	100

№	Statistik test	Minimal kirish qiymat uzunligi (bit)
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 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.

Nazorat savollari

1. Siljitish registorlariga asoslangan shifrlarning kriptoanalizi natijalari
2. RC4 shifrining kriptoanalizi natijalari
3. ORYX shifrining kriptoanalizi natijalari
4. PKZIP shifrining kriptoanalizi natijalari
5. Psevdotasodifiy sonlar generatorini baholash usullari
6. Kriptografik psevdotasodifiy sonlar generatori

7. Tasodifiylikka tekshirish testlarining qanday turlari mavjud?
8. Tasodifiy ketma-ketliklar entropiyasini o'lchash usullari
9. To'liq tanlash hujumi nimaga asoslanadi
10. Statistik tahlil hujumini tushuntiring
11. Analitik hujumlarga qaysi hujum turlari kiradi
12. Korrelatsion hujumlarda qaysi parametrlar muhim hisoblanadi
13. "Vaqt-xotira" usulini tushuntiring
14. "Taxmin qilish va aniqlash" hujum turini izohlang

VI BOB. XESH FUNKSIYALARNING KRIPTOANALIZI

6.1. 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_i va shifrogrammalar $w = F(z_i, x)$ 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_{i1} kalitni olib, u shifrmatn ochiladi va natija $v = F(z_{i1}, u)$ ni MB bilan taqqoslanadi. Agar v biror w bilan teng chiqsa, kalit z_{ii} 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

$$0((p\#\{z\}) \text{ bo'ladi.}$$

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:

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

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:

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

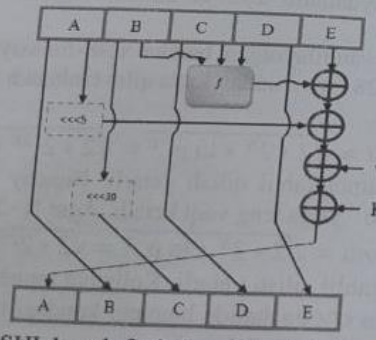
ta ochiq matnni tahlil qilish yetarli. Kolliziya topish uchun $3*10^{54}$ yil kerak bo'ladi. Bu o'z navbatida bugungi kundagi hisoblash texnikasi imkoniyat darajasidan chiqib ketadi.

6.2. SHA-1 xesh funksiya algoritmiga differensial kriptotahlil usulining qo'llanilishi

Xesh funksiya algoritmlarini tahlil qilishdan asosiy maqsad shundan iboratki, mumkin bo'lgan barcha variantlarni tahlil qilish (total perebor) usulini qo'llab kolliziya topish uchun sarflanadigan vaqtg

qaraganda ancha qisqa vaqt ichida kolliziya topish hisoblanadi. Bunday holatda vazifa shunday $(M^{(0)} \dots M^{(15)}) = (W^{(0)} \dots W^{(15)})$ va $(M'^{(0)} \dots M'^{(15)}) = (W'^{(0)} \dots W'^{(15)})$ ikkita turli xil ma'lumotni topish kerakki, natijada ulardan hisoblangan xesh funksiya qiymati bir xil bo'lishi zarur.

Buning uchun SHA-0 xesh funksiya algoritmining soddalashtirilgan holatlarida qanday o'zgarishlar bo'lishi kuzatiladi. Bu bir tomondan xesh funksiya algoritmining tuzilishi, boshqa tomondan esa funksiyaning kriptografik hususiyatlarini o'rganish imkonini beradi. SHA algoritmlari oilasiga mansub xesh funksiya algoritmlarida asosan ikkita chiziqsiz amal mavjud bo'lib, bu – f funksiya va $(a+b) mod\ 2^{32}$ bo'yicha qo'shish amalidir. Dastlab aynan ana shu ikkita chiziqsiz amalni, $(a+b) mod\ 2^{32}$ bo'yicha qo'shish amalini XOR amaliga, f funksiyani esa chiziqli $f(x,y,z) = x \oplus y \oplus z$ funksiyaga almashtirilgan holati hisoblangan SHI-1 xesh funksiya algoritmiga differensial kriptotahlil usulini qo'llash jarayoni bilan tanishib chiqamiz.



6.1-rasm. SHI-1 xesh funksiya algoritmi sxemasi

Algoritmda foydalanilgan f funksiya va W` parametrlarning qiymatlari quyidagicha aniqlanadi:

$$f(b,c,d) = b \oplus c \oplus d$$

$$W_t = \begin{cases} M_t, & t = 0,\dots,15, \\ (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}), & t = 16,\dots,79. \end{cases} \quad (6.1)$$

Xeshlash jarayonida foydalaniladigan dastlabki W ning o'n oltita bloki ($W^{(0)} \dots W^{(15)}$) ni mavjud deb hisoblaymiz va $W^{(t)}$ blokdagi ixtiyoriy bitta bitning o'zgarishini keyingi raunddagi parametrlarga(o'zgaruvchilarga) qay tarzda ta'sir etishi ko'rib chiqiladi. Quyida $W^{(t)}$ ning ikkinchi bitining o'zgarishi ko'rib chiqiladi, ya'ni $W_1^{(t)}$ ni o'zgartirib uni o'zidan keyingi beshta raunddagi akslantirish jarayonlari kuzatiladi (6.1-jadval).

6.1-jadval.

Ikkinchi bit o'zgarishining keyingi raund qiymatlariga ta'siri

№ raund	Akslantirishlar	O'zgaruvchi bitlar	Izoh
i+1	$a^{(i+1)} = W^{(i)} \oplus (a^{(i)} <<<5) \oplus b^{(i)} \oplus c^{(i)} \oplus d^{(i)} \oplus e^{(i)} \oplus K^{(i)}$	$a_1^{(i+1)}$	$W_1^{(t)}$ ning o'zgarishi mos holda $a_1^{(i+1)}$ ni o'zgarishiga olib keladi
	$b^{(i+1)} = a^{(i)}$	-	O'zgarish yo'q
	$c^{(i+1)} = (b^{(i)} <<<30)$	-	
	$d^{(i+1)} = c^{(i)}$	-	
	$e^{(i+1)} = d^{(i)}$	-	
i+2	$a^{(i+2)} = W^{(i+1)} \oplus (a^{(i+1)} <<<5) \oplus b^{(i+1)} \oplus c^{(i+1)} \oplus d^{(i+1)} \oplus e^{(i+1)} \oplus K^{(i+1)}$	$a_6^{(i+2)}$	$a_1^{(i+1)}$ ni chapga siklik 5 bitga surgandan keyin o'zgargan 2-bit 7-bitni o'zgartiradi. Ya'ni $a_6^{(i+2)}$
	$b^{(i+2)} = a^{(i+1)}$	$b_1^{(i+2)}$	$b_1^{(i+2)}$ esa oldingi raunddagi $a_1^{(i+1)}$ ning o'zgarganligi sababli o'zgaradi
	$c^{(i+2)} = (b^{(i+1)} <<<30)$	-	
	$d^{(i+2)} = c^{(i+1)}$	-	

№ raund	Akslantirishlar	O'zgaruvchi bitlar	Izoh
	$e^{(i+2)} = d^{(i+1)}$	-	O'zgarish yo'q
$i+3$	$a^{(i+3)} = W^{(i+3)} \oplus (a^{(i+2)} <<<5) \oplus b^{(i+2)} \oplus c^{(i+2)} \oplus d^{(i+2)} \oplus e^{(i+2)} \oplus K^{(i+2)}$	$a_1^{(i+3)}$ $a_{11}^{(i+3)}$	$a_6^{(i+2)}$ ni chapga siklik 5 surgandan keyin bitga o'zgargan 6-bit 12-bitni o'zgartiradi $a_{11}^{(i+3)}$. Bundan tashqari $b_1^{(i+2)}$ ning o'zgarishi $a_1^{(i+3)}$ o'zgarishiga olib keladi
	$b^{(i+3)} = a^{(i+2)}$	$b_6^{(i+3)}$	$b_6^{(i+3)}$ ham oldingi raunddagi $a_6^{(i+2)}$ ning o'zgarishi kabi o'garadi
	$c^{(i+3)} = (b^{(i+2)} <<<30)$	$c_{31}^{(i+3)}$	$b_1^{(i+2)}$ ni chapga siklik 30 surgandan keyin bitga o'zgargan 32-bit $c_{31}^{(i+3)}$ bitni o'zgartiradi
	$d^{(i+3)} = c^{(i+2)}$	-	O'zgarish yo'q
	$e^{(i+3)} = d^{(i+2)}$	-	
$i+4$	$a^{(i+4)} = W^{(i+3)} \oplus (a^{(i+3)} <<<5) \oplus b^{(i+3)} \oplus c^{(i+3)} \oplus d^{(i+3)} \oplus e^{(i+3)} \oplus K^{(i+3)}$	$a_{16}^{(i+4)}$ $a_{31}^{(i+4)}$	$a_1^{(i+3)}$ va $a_{11}^{(i+3)}$ larni chapga siklik 5 bitga surish 7 va 17-bitlarni o'zgarishiga olib keladi. $b_6^{(i+3)}$ esa 7-bitni yana o'zgartiradi. Aniqrog'i $a_6^{(i+4)}$ ni dastlabki holatiga qaytaradi. $c_{31}^{(i+3)}$ ning o'zgarishi $a_{31}^{(i+4)}$ ni o'zgartiradi.
	$b^{(i+4)} = a^{(i+3)}$	$b_1^{(i+4)}$ $b_{11}^{(i+4)}$	$a_1^{(i+3)}$ va $a_{11}^{(i+3)}$ larning o'zgarishi $b_1^{(i+3)}$ va $b_{11}^{(i+3)}$ o'zgartiradi.
	$c^{(i+4)} = (b^{(i+3)} <<<30)$	$c_4^{(i+4)}$	$b_6^{(i+3)}$ ni chapga 30 bit siklik surish $c_4^{(i+4)}$ ni o'zgarishiga olib keladi
	$d^{(i+4)} = c^{(i+3)}$	$d_{31}^{(i+4)}$	$c_{31}^{(i+3)}$ ning o'zgarishi $d_{31}^{(i+4)}$ ni o'zgartiradi.
	$e^{(i+4)} = d^{(i+3)}$	-	O'zgarish yo'q
$i+5$	$a^{(i+5)} = W^{(i+4)} \oplus (a^{(i+4)} <<<5) \oplus b^{(i+4)} \oplus c^{(i+4)} \oplus d^{(i+4)} \oplus e^{(i+4)} \oplus K^{(i+4)}$	$a_1^{(i+5)}$ $a_{11}^{(i+5)}$ $a_{21}^{(i+5)}$ $a_{31}^{(i+5)}$	$a_{16}^{(i+4)}$ va $a_{31}^{(i+4)}$ larni chapga siklik 5 bitga surish 22 va 5-bitlarni o'zgarishiga olib keladi. $c_4^{(i+4)}$ ning o'zgarishi 5-bitni qaytadan o'zgartiradi. Natijada 5-bit o'zgarishsiz qoladi. $b_1^{(i+4)}$ va $b_{11}^{(i+4)}$ larning o'zgarishi $a_1^{(i+5)}$ va $a_{11}^{(i+5)}$ larni o'zgarishiga olib keladi. $d_{31}^{(i+4)}$ esa $a_{31}^{(i+5)}$ ni o'zgarishiga olib keladi
	$b^{(i+5)} = a^{(i+4)}$	$b_{16}^{(i+5)}$ $b_{31}^{(i+5)}$	$a_{16}^{(i+4)}$ va $a_{31}^{(i+4)}$ lar $b_{16}^{(i+5)}$ va $b_{31}^{(i+5)}$ larni o'zgartiradi.
	$c^{(i+5)} = (b^{(i+4)} <<<30)$	$c_9^{(i+5)}$ $c_{31}^{(i+5)}$	$b_1^{(i+4)}$ va $b_{11}^{(i+4)}$ larni 30 bit chapga siklik surilishidan hosil bo'lgan qiymat $c_9^{(i+5)}$ va $c_{31}^{(i+5)}$ larni o'zgartiradi.
	$d^{(i+5)} = c^{(i+4)}$	$d_4^{(i+5)}$	$c_4^{(i+4)}$ esa $d_4^{(i+5)}$ ni o'zgartiradi.

№ raund	Akslantirishlar	O'zgaruvchi bitlar	Izoh
	$e^{(i+5)} = d^{(i+4)}$	$e_{31}^{(i+5)}$	$d_{31}^{(i+4)}$ esa $e_{31}^{(i+5)}$ ni o'zgartiradi.

Ushbu jadvaldan ko'rinib turibdiki, har bir raunddagi o'zgarish keyingi raunddagi parametrlarning o'zgarishiga olib kelmoqda. Shuning uchun ushbu o'zgarishlarni oldini olish maqsadida W ning 5 ta ($W_6^{(i+1)}$, $W_1^{(i+2)}$, $W_{31}^{(i+3)}$, $W_{31}^{(i+4)}$, $W_{31}^{(i+5)}$) bloklaridagi qiymatlarni mos ravishda teskarisiga o'zgartiriladi(*0* bo'lsa *1* ga va aksincha). Kiritilgan har bir o'zgaruvchi o'z navbatida ba'zi qiymatlarni o'zgartirib beradi. Masalan $W_6^{(i+1)}$ ning o'zgarishi $a_6^{(i+1)}$ o'zgarishsiz qolishiga olib keladi (6.1-jadval). Bu esa o'z navbatida aynan ushbu o'zgaruvchi bilan bog'liq barcha 6.1-jadvalda ko'rsatilgan o'zgarishlarni oldini oladi. 6.2-jadvalda yuqorida ko'rsatilgan 5 ta to'g'irlovchi o'zgaruvchilarning boshqa parametrlarning o'zgarishiga qanday ta'sir etishi keltirilgan.

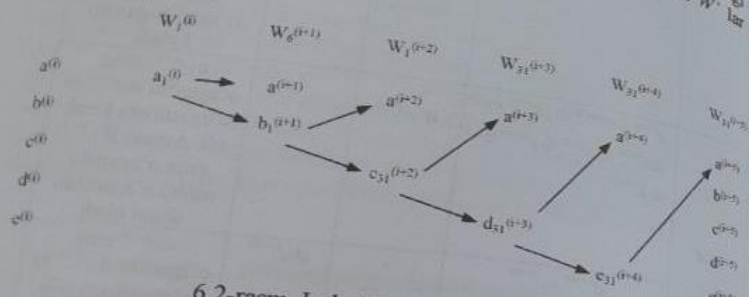
6.2-jadval.

Bitlarni to'g'irlanish jadvali

№ raund	Akslantirishlar	To'g'irlovchi bitlar	O'zgaruvchi bitlar	Izoh
i+1	$a^{(i+1)} = W^{(i)} \oplus (a^{(i)} <<<5) \oplus b^{(i)} \oplus c^{(i)} \oplus d^{(i)} \oplus e^{(i)} \oplus K^{(i)}$	-	$a_1^{(i+1)}$	$W_1^{(i)}$ ning o'zgarishi $a_1^{(i+1)}$ ni o'zgartiradi
i+2	$a^{(i+2)} = W^{(i+1)} \oplus (a^{(i+1)} <<<5) \oplus b^{(i+1)} \oplus c^{(i+1)} \oplus d^{(i+1)} \oplus e^{(i+1)} \oplus K^{(i+1)}$	$W_6^{(i+1)}$	-	$W_6^{(i+1)}$ ning o'zgartirilishi $a_6^{(i+2)}$ ni o'zgarishsiz qolishiga olib keladi
	$b^{(i+2)} = a^{(i+1)}$	-	$b_1^{(i+2)}$	$b_1^{(i+2)}$ oldingi raunddagi $a_1^{(i+1)}$ ning o'zgarishi sababli o'zgaradi
i+3	$a^{(i+3)} = W^{(i+2)} \oplus (a^{(i+2)} <<<5) \oplus b^{(i+2)} \oplus c^{(i+2)} \oplus d^{(i+2)} \oplus e^{(i+2)} \oplus K^{(i+2)}$	$W_1^{(i+2)}$	-	$b_1^{(i+2)}$ ning o'zgarishi $a_1^{(i+3)}$ ni o'zgartirishi kerak edi. Ammo $W_1^{(i+2)}$

№ raund	Akslantirishlar	To'g'irlovchi bitlar	O'zgaruvchi bitlar	Izoh
				ning o'zgarishi ushbu o'zgarishni oldini oladi.
	$c^{(i+3)} = (b^{(i+2)} <<<30)$	-	$c_{31}^{(i+3)}$	$b_1^{(i+2)}$ ning o'zgarishi va uning chapga 30 bit siklik surish natijasi $c_{31}^{(i+3)}$ ning o'zgarishiga olib keladi.
i+4	$a^{(i+4)} = W^{(i+3)} \oplus (a^{(i+3)} <<<5) \oplus b^{(i+3)} \oplus c^{(i+3)} \oplus d^{(i+3)} \oplus e^{(i+3)} W_{31}^{(i+3)} \oplus K^{(i+3)}$	-	-	$c_{31}^{(i+3)}$ ning o'zgarishi $a_{31}^{(i-4)}$ ni o'zgartirishi kerak edi. Ammo $W_{31}^{(i+3)}$ ning o'zgarishi ushbu o'zgarishni oldini oladi.
	$d^{(i+4)} = c^{(i+3)}$	-	$d_{31}^{(i+4)}$	$c_{31}^{(i+3)}$ ning o'zgarishi $d_{31}^{(i-4)}$ ni o'zgarishiga olib keladi.
i+5	$a^{(i+5)} = W^{(i+4)} \oplus (a^{(i+4)} <<<5) \oplus b^{(i+4)} \oplus c^{(i+4)} \oplus d^{(i+4)} \oplus e^{(i+4)} W_{31}^{(i+4)} \oplus K^{(i+4)}$	-	-	$d_{31}^{(i+4)}$ ning o'zgarishi $a_{31}^{(i-5)}$ ni o'zgartirishi kerak edi. Ammo $W_{31}^{(i+4)}$ ning o'zgarishi ushbu o'zgarishni oldini oladi.
	$e^{(i+5)} = d^{(i+4)}$	-	$e_{31}^{(i+5)}$	$d_{31}^{(i+4)}$ ning o'zgarishi $e_{31}^{(i+5)}$ ni o'zgarishiga olib keladi.
i+6	$a^{(i+6)} = W^{(i+5)} \oplus (a^{(i+5)} <<<5) \oplus b^{(i+5)} \oplus c^{(i+5)} \oplus d^{(i+5)} \oplus e^{(i+5)} W_{31}^{(i+5)} \oplus K^{(i+5)}$	-	-	$e_{31}^{(i+5)}$ ning o'zgarishi $a_{31}^{(i-6)}$ ni o'zgartirishi kerak edi. Ammo $W_{31}^{(i+5)}$ ning o'zgarishi ushbu o'zgarishni oldini oladi.

6.1 va 6.2- jadvallardan ko'rinib turibdiki, kiritilgan ($W_1^{(i+2)}$, $W_{31}^{(i+3)}$, $W_{31}^{(i+4)}$, $W_{31}^{(i+5)}$) to'g'irlovchi o'zgartirishlar ($a^{(i)}$, $b^{(i)}$, $c^{(i)}$, $d^{(i)}$, $e^{(i)}$) qiymatlarni ($a^{(i+6)}$, $b^{(i+6)}$, $c^{(i+6)}$, $d^{(i+6)}$, $e^{(i+6)}$) qiymatlarga akslanishida hosil bo'lgan qiymat W ni hisoblashdagi ($a^{(i+6)}$, $b^{(i+6)}$, $c^{(i+6)}$, $d^{(i+6)}$, $e^{(i+6)}$) qiymatlari bilan bir xil bo'ladi. Ya'ni ($i+6$) dan keyingi barcha raundlarda bajariladigan barcha amallar ikkala W va W' lar uchun bir xilda davom etadi.



6.2-rasm. Lokal kolliziya topish sxemasi

Bu esa lokal kolliziya borligidan dalolat beradi(6.2-rasm). Ushbu holatda W hamda W' larni $i = 16$ dan boshlab 6.1-ifoda asosida hisoblanadi. Shuni ham eslatib o'tish joizki, o'zgartirishlarni boshlash ($i < 75$) bo'lganda amalga oshirish mumkin. Sababi kiritilgan o'zgartirishni bartaraf etish maqsadida keyingi beshta raunddagi o'zgaruvchilar uchun maxsus to'g'irlovchi o'zgaruvchilarni kiritish zarur. Umumiy holda bunday kolliziyani topish uchun 80 bitdan iborat $m0$ deb nomlangan vektorni qurish talab etiladi. Ushbu vektor yuqorida keltirilgan kolliziya topish jarayonini matematik modelini tuzishga yordam beradi.

Aytaylik shunday ($m0^{(0)}$, …, $m0^{(79)}$) vektor mavjud bo'lsin. Quyida W ma'lumotni yangi W' ma'lumotga akslantiruvchi qandaydir maskani topish jarayoni keltirilgan.

Jarayonni amalga oshirish uchun 80 ta 32 bitdan iborat bo'lgan L maskadan foydalaniladi, ya'ni $L = (L^{(0)}, \ldots, L^{(79)})$. Har bir $L^{(i)}$ ni hisoblash uchun esa qo'shimcha oltita to'g'irlovchi $L0$, $L1$, $L2$, $L3$, $L4$,

$L5$ maskalar kiritiladi. Chunki kiritilgan oltita maska ($W_1^{(i)}$, $W_6^{(i+1)}$, $W_1^{(i+2)}$, $W_{31}^{(i+3)}$, $W_{31}^{(i+4)}$, $W_{31}^{(i+5)}$) to'g'irlashlarni aks ettirish vositasini bajarishga yordam beradi. Dastlabki $L0$ maskaga yana ($i = -5$ dan $i = -1$) beshta nol blok kiritiladi va qolgan bloklari quyidagi tartibda to'ldiriladi.

$$L0^{(i)} = 0, \quad -5 \le i \le -1;$$
$$L0_k^{(i)} = 0, \quad 0 \le i \le 79 \text{ va } k \ne 1;$$
$$L0_1^{(i)} = m0^{(i)}, \quad 0 \le i \le 79;$$

Ikkinchi to'g'irlovchi $L1$ maskaga esa ($i = -4$ dan $i = -1$) to'rtta 0 blok kiritiladi va qolgan bloklar $L0$ maska qiymatlarini 5 bit chapga siklik surishdan hosil bo'lgan qiymatlaridan olinadi. Bu qo'shimcha ravishda kiritilgan $W_6^{(i+1)}$ ni ifodalaydi. Ushbu holatda to'g'irlanuvchi bit raqami $k = 6$ bo'ladi.

$$L1^{(i)} = L0^{(i-1)} <<< 5, \quad -4 \le i \le 79; \tag{6.2}$$

Uchinchi $L2$ maskaga uchta 0 blok kiritiladi va qolgan bloklari $L0$ maskadan olinadi. Bu qo'shimcha ravishda kiritilgan $W_1^{(i+2)}$ ni ifodalaydi. O'z navbatida ushbu holatda to'g'irlanuvchi bit raqami $k = 1$ bo'ladi.

$$L2^{(i)} = L0^{(i-1)}, \quad -3 \le i \le 79; \tag{6.3}$$

Shunday tarzda $L3$, $L4$, $L5$ maskalarga ham mos ravishda ikkita, bitta, nolta *nol* bloklar kiritiladi. Qolgan qiymatlari esa yuqoridagidek $L0$ maskani 30 *bit* chapga siklik surish natijasida hosil qilinadi. Bu qo'shimcha ravishda kiritilgan $W_{31}^{(i+3)}$, $W_{31}^{(i+4)}$, $W_{31}^{(i+5)}$ larni ifodalaydi. Ushbu holatda to'g'irlanuvchi bit raqami barchasida $k = 31$ bo'ladi.

$$L3^{(i)} = L0^{(i-3)} <<< 30, \quad -2 \le i \le 79; \tag{6.4}$$
$$L4^{(i)} = L0^{(i-4)} <<< 30, \quad -1 \le i \le 79; \tag{6.5}$$
$$L5^{(i)} = L0^{(i-5)} <<< 30, \quad 0 \le i \le 79; \tag{6.6}$$

Natijaviy L maska yuqoridagi oltita qo'shimcha maskalarni *modul* 2 bo'yicha qo'shish natijasida hosil qilinadi.

$$L^{(i)} = L0^{(i)} \oplus L1^{(i)} \oplus L2^{(i)} \oplus L3^{(i)} \oplus L4^{(i)} \oplus L5^{(i)}, \quad 0 \le i \le 79; \tag{6.7}$$

L maskani topish jarayonini yanada tushunarli bo'lishi uchun *m0* maskaning dastlabki $m0^{(0)}$ qiymati *1* ga qolganlari esa *0* ga teng bo'lganda uning birinchi beshta blokini ko'rib chiqiladi(6.3-jadval). 6.3-jadvalda tartiblash $i = -5$ dan boshlangan. Birinchi blokning $i = 0$ bo'lgungacha to'g'irlovchi *L0, L1, L2, L3, L4, L5* maskalarni *0* bilan to'ldirib chiqiladi. $L0^{(0)}$ qiymatini esa mos holda $m0^{(0)}$ ning qiymati, ya'ni *1* ga teng deb olinadi. Qolgan barcha bloklariga esa *0* o'rnatiladi. *L0, L1, L2, L3, L4, L5* to'g'irlovchi maskalar (6.2) - (6.6) ifodalarga binoan hisoblanadi. *L* maska esa 6.7-ifoda yordamida aniqlanadi.

6.3-jadval.

To'g'irlovchi L maskani qurish

i	*-5*	*-4*	*-3*	*-2*	*-1*	*0*	*1*	*2*	*3*	*4*	*5*
L0	0	0	0	0	0	$L0_1^{(0)}$	0	0	0	0	0
L1	-	0	0	0	0	0	$L1_6^{(1)}$	0	0	0	0
L2	-	-	0	0	0	0	0	$L2_1^{(2)}$	0	0	0
L3	-	-	-	0	0	0	0	0	$L3_{31}^{(3)}$	0	0
L4	-	-	-	-	0	0	0	0	0	$L4_{31}^{(4)}$	0
L5	-	-	-	-	-	0	0	0	0	0	$L5_{31}^{(5)}$
L	-	-	-	-	-	$L_1^{(0)}$	$L_6^{(1)}$	$L_1^{(2)}$	$L_{31}^{(3)}$	$L_{31}^{(4)}$	$L_{31}^{(5)}$

m0 vektorni tanlashda shuni ham eslatib o'tish kerakki, $i = 16$ dan boshlab $W^{(i)}$ ni hisoblash 6.1-ifoda asosida amalga oshiriladi.

Shuning uchun *L0* maskaning $i = 11$ (chunki $i = -5$ dan boshlangan) dan keyingi qiymatlari (2.1.8) ifoda asosida hisoblanadi.

$$L0^{(i)} = L0^{(i-3)} \oplus L0^{(i-8)} \oplus L0^{(i-14)} \oplus L0^{(i-16)}, \quad 11 \le i \le 79; \tag{6.8}$$

(2.1.1) ifodadagi barcha akslantirishlar to'laligicha chiziqli hisoblanadi. Ushbu akslantirishlar natijasini 80 razryadli 32 ta blok $V = (V^{(0)}, \ldots, V^{(32)})$ ko'rinishida ifodalash mumkin. Ya'ni har bir $V^{(i)}$ blok 80 bitdan iborat.

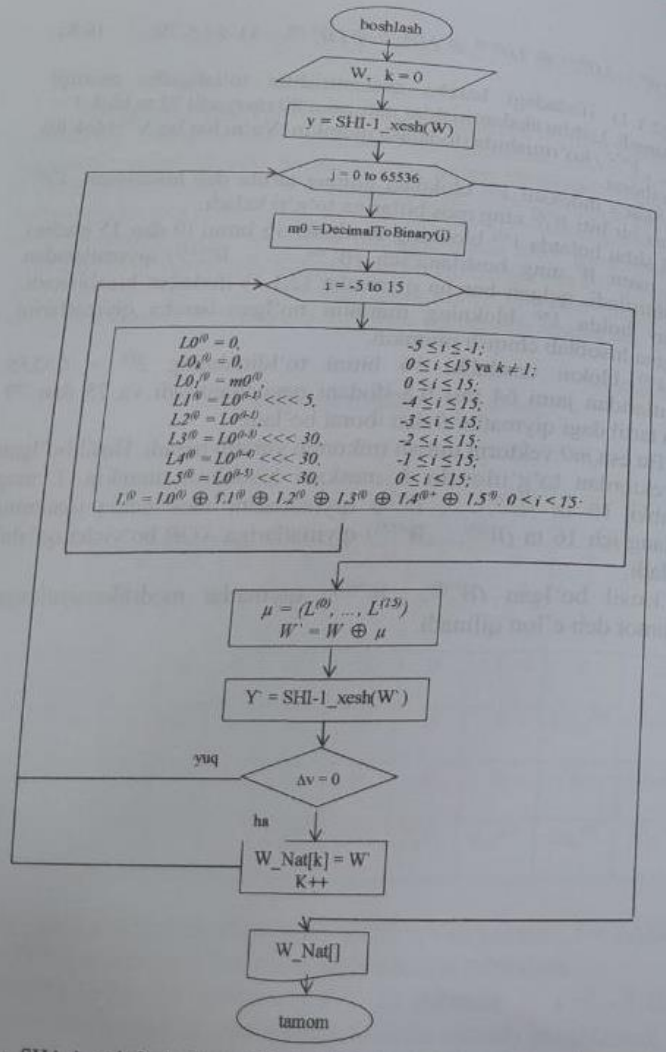
Agar *j* indeksni $V^{(i)}$ blokdagi bitning tartibi deb hisoblasak, $V_j^{(i)}$ ning har bir biti $W_i^{(j)}$ ning mos bitlariga to'g'ri keladi.

Ushbu holatda $V^{(i)}$ blokning dastlabki 16 bitini (0 dan 15 gacha) ochiq matn *W* ning boshlang'ich $(W^{\vee(0)}, \ldots, W^{\vee(15)})$ qiymatlaridan o'zlashtiriladi, qolgan barcha qiymatlar (2.1.1) ifodadan hisoblanadi. Bunday holda $V^{(i)}$ blokning mumkin bo'lgan barcha qiymatlarini osongina hisoblab chiqish mumkin.

$V^{(i)}$ blokni dastlabki 16 bitini to'ldirishning $2^{16} = 65536$ variantlaridan jami 64 tasi 6.8-ifodani qanoatlantiradi va 75 dan 79 gacha tartibdagi qiymatlar *0* dan iborat bo'ladi.

Bu esa *m0* vektorni qurish imkonini yaratib beradi. Hosil bo'lgan *m0* vektordan to'g'irlovchi *L* maskani hisoblash mumkin. *L* ning dastlabki 16 ta $(L^{(0)}, \ldots, L^{(15)})$ qiymatlarini mos ochiq matnning boshlang'ich 16 ta $(W^{(0)}, \ldots, W^{(15)})$ qiymatlariga *XOR* bo'yicha qo'shib chiqiladi.

Hosil bo'lgan $(W^{\vee(0)}, \ldots, W^{\vee(15)})$ qiymatlar modifikatsiyalangan ma'lumot deb e'lon qilinadi.



6.3-rasm. SHA-1 xesh funksiyaga differensial kriptotahlil usulini qo'llashning blok-sxemasi

Agar $\mu=(L^{(0)},\ldots,L^{(15)})$ ya'ni kiruvchi ayirma deb hisoblasak, $W`=W\oplus\mu$ ko'rinishda ifodalash mumkin. Bu ifodadan olingan $W`$ va W qiymatlar SHI-1 xesh funksiya algoritmida ikkita bir xil xesh qiymatga ega bo'luvchi ochiq matnlar ekanligini anglatadi. Yuqorida faqatgina $W_1^{(i)}$ bitning o'zgarishi ko'rib chiqildi. Ushbu o'zgarishni $W^{(i)}$ ning ixtiyoriy biti uchun amalga oshirish mumkin. Ammo $W_1^{(i)}$ - bitni o'zgartirish boshqalariga qaraganda yaxshiroq natija olinadi.

6.3. MD4 algoritmining kriptoanalizi

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:

$$For\ j = 0,1,2\ and\ i = 0,1,2,3$$
$$a = \phi_j(a,b,c,d,w_{j,4i},,s_{j,4i})$$

$$d = \phi_j(d,a,b,c,w_{j,4i+1},,s_{j,4i+1})$$
$$c = \phi_j(c,d,a,b,w_{j,4i+2},,s_{j,4i+2})$$
$$b = \phi_j(b,c,d,a,w_{j,4i+3},,s_{j,4i+3})$$

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
	a_1	m_0	3			a_1
1	a_1	m_0	3			
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
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	a_6	m_9	9			c_6
24	b_6	m_{13}	13			b_6
25	a_7	m_4	3	$2^{28}+2^{31}$	2^{28}	a_7
26	b_9	m_{12}	15	-2^{16}		$b_9[-32]$
27	a_{10}	m_7	3	$2^{28}+2^{31}$	2^{31}	$a_{10}[-32]$
28	d_{10}	m_{10}	9			d_{10}
29	c_{10}	m_6	11			c_{10}
30	b_{10}	m_{14}	15			b_{10}
31	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 $f(\neg b_{2,14}, \neg d_{2,14}) = 1$. 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	$a_{3,13} = 1, a_{3,14} = 1$ $a_{3,15} = 1, a_{3,17} = 0, a_{3,19} = 0, a_{3,20} = 0, b_{3,20} = 0, a_{3,21} = 0, a_{3,22} = b_{2,23} a_{3,22} = 1, a_{3,26} = b_{2,26}$
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	$c_{3,17} = 1$, $c_{3,20} = 0$, $c_{3,21} = 0$, $c_{3,22} = 0$, $c_{3,23} = 0$, $c_{3,26} = 0$, $c_{3,30} = 1$, $c_{3,32} = d_{3,32}$
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}	$a_{10,32} = 1$

Nazorat 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.

VII BOB. OCHIQ KALITLI KRIPTOTIZIMLARNING KRIPTOANALIZI

7.1. Diskret logarifmlash muammosining murakkabligiga asoslangan ochiq kalitli kriptotizimlarning kriptoanalizi

Shunday x- butun son topilsinki:

$$a^x \equiv b(mod r) \tag{7.1}$$

tenglik o'rinli bo'lsin. Bu yerda p –tub son va 7.1-tenglamaning yechimi $x = log_a b$ - ni quyidagi formula orqali topish mumkin:

$$log_a b \equiv \sum_{j=1}^{p-2} (1 - a^j)^{-1} b^j \ (mod\ p-1).$$

Biroq bu formula bilan yechimni topish masalasi bevosita «mumkin bo'lgan barcha holatlarni ko'rib chiqish» kabi usulga o'xshash bo'lgani uchun ham amalda bu formula qo'llanilmaydi. Quyida keltiriladigan algoritm esa hisoblashlar sonini qisqartirib yechimni topishning samarali usulini beradi.

Diskret logarifmlash algoritmi:

1-Qadam. Quyidagi son hisoblansin

$N = [p^{1/2}] + 1$

2-Qadam. Quyidagi son hisoblansin

$S \equiv a^N (mod\ p)$

3- Qadam. $u, 1 \le u \le H$ sonli qiymatlari uchun $S^u\ (mod\ p)$ jadval tuziladi va bu qiymatlar tartiblab chiqiladi.

4 –Qadam. Keyingi jadval esa $ba^v\ (mod\ p), 0 \le v \le H$ qiymatlar uchun tuzilib tartibladi.

5- Qadam. Birinchi va ikkinchi jadvalda teng chiqqan u va v elementlar olinadi.

6- Qadam. Javob sifatida

$x \equiv N * u - v (mod\ p-1)$

qiymat olinadi.

Misol. Quyidagi $3^x \equiv 15\ (mod\ 17)$ ifodadan x – topilsin.

Yechim: Bevosita tekshirib ko'rish mumkinki, $x = 6$ bu tenglikni qanoatlantiradi . Haqiqatan $3^6 = 729; 729 = 42 * 17 + 15$.

Shuni ta'kidlash kerakki bu masalada faqat butun yechimlarni topish kerak. Shuning uchun ham (7.1) ifodadan butun x-ni topish masalasi murakkab hisoblanadi.

Bu misolni yechish jarayoni yuqoridagi algoritm orqali quyidagicha amalga oshiriladi:

1-qadam. $N = \left[p^{\frac{1}{2}}\right] + 1, N = 5.$

2-qadam. $S \equiv a^N (mod\ p)\ S = 3^5 (mod\ 17) = 5.$

3-qadam. $5^u (mod\ 17), 1 \le u \le 5$ jadval qiymatlarini hisoblaymiz:

$u = 1,5 (mod\ 17) = 5$

$u = 2,25 (mod 17) = 8$

$u = 3,125 (mod\ 17) = 6$

$u = 4,625 (mod 17) = 13$

$u = 5,3125 (mod 17) = 6$

Bu qiymatlar tartiblansa: 5,6,8,13 .

4-qadam. $15 * 3^v (mod\ 17), 0 \le v \le 5$ jadval qiymatlarini hisoblaymiz:

$v = 1,45 (mod\ 17) = 1$

$v = 2,15 * 9 (mod\ 17) = 16$

$v = 3,15 * 27 (mod\ 17) = 14$

$v = 4,15 * 81 (mod 17) = 8$

$v = 5,15 * 243 (mod\ 17) = 7$

Bu qiymatlar tartiblansa: 7,8,11,14,16.

5- qadam. Ikkita jadval natijalari ustma-ust tushgan u, v – elementlar tanlab olinadi.

Ya'ni, $u = 2, v = 4.$

6- qadam. Javob:

$$x \equiv N * u - v\ (mod\ p-1)$$

ya'ni $x \equiv 5 * 2 - 4 (mod\ 16) = 6 (mod\ 16), x = 6.$

7.2. Faktorlash muammosining murakkabligiga asoslangan ochiq kalitli kriptotizimlarning kriptoanalizi

Faktorlash muammosining yuzaga kelishi antik davrlarga, Eratosfen yashagan davrlarga, taxminan, eramizgacha 284-202 yillarga to'g'ri keladi. Muammoning undan keyingi tarixi Fibbanochi (taxminan 1180-1250 yy.), Ferma (1601-1665 yy.), Eyler (1707-1783 yy), Lejandr (1752-1833 yy.), Gauss (1777-1855 yy.) kabi ulug' matematiklar nomi bilan bog'langan.

Faktorlash muammosini hal etishda n modulni faktorlash masalasini yechishda birinchi navbatda xayolga keladigan usul, bu $\sqrt{n}$ dan oshmaydigan tub sonlarni tanlab ularga bo'lib ko'rishdir. Boshqa tanlash usuli Fermaga tegishli bo'lib, n ni kvadratlar ayirmasi ko'rinishida ifodalashga asoslangan:

$$n = a^2 - b^2 = (a + b)(a - b).$$

Ferma eng katta umumiy bo'luvchi - $EKUB(n, a - b)$ ni, ya'ni n ning natural bo'luvchisini topishga harakat qilishni hamda bunga imkon beruvchi usulni ham taklif etgan. Agar n ning ko'paytuvchilari bir-biridan katta farq qilmasa, bu usul oddiy tanlash usuliga nisbatan tez yechim beradi va uning murakkabligi $O(\sqrt{n})$ ko'rinishida ifodalanadi, ammo hozirgi kunda kriptografik tizimlarda amalda foydalaniladigan hollar uchun ahamiyatga ega emas. Lejandr mazkur yondashuvda

$a^2 \equiv b^2 \ (mod\ n)$ ga ega bo'lish lozimligiga e'tibor qaratgan. Ammo, keltirilgan taqqoslama har qanday n uchun yetarli emasligini ham ko'rsatgan va ko'zlangan maqsadga erishish uchun uzluksiz kasrlardan foydalanish yo'lini taklif etgan.

Kompyuterlar asrida dastlabki 1970 yillarda taklif etilgan faktorlash algoritmlaridan biri *(p-1)* Pollard algoritmi bo'lgan. Undan so'ng *(p+1)* Vilyams algoritmi va EEChlardan foydalanishga asoslangan Lenstra algoritmi ishlab chiqildi. Keyinchalik *(p-1)* Pollard algoritmi *(p+1)* Pollard algoritmi sifatida, Pollardning *p*- usuli nomlari ostida takomillashtirildi. Pollardning *p*- usulining murakkabligi $I_p = \sqrt{\pi q}/4$ amal bilan belgilanadi. Hozirgi kunga kelib, faktorlash

muammosining eng tezkor usullari bo'lib, chiziqli g'alvir, kvadratik g'alvir, sonli maydon g'alviri, umumlashgan sonli maydon g'alviri usullari tan olingan.

Hozirgi kunda eng samarali kriptotahlil algoritmlarining murakkabligi eksponensial emas, balki subeksponensial murakkablikka ega.

Algoritm eksponensial murakkablikka ega deyiladi, agarda uning murakkabligi qiymatining tartibi $O(t^{f(n)})$ bo'lsa.

Algoritm polinomial murakkablikka ega deyiladi, agarda uning murakkabligi qiymatining tartibi $O(n^m)$ bo'lsa. Subeksponensial murakkablikka ega bo'lgan algoritm murakkabligi qiymatining tartibi $O(n^m)$ va $O(t^{f(n)})$ orasida bo'ladi.

Quyida faktorizatsiyalash muammosini bartaraf etish imkoniyatiga ega bo'lgan ba'zi algoritmlar haqida ma'lumot beriladi.

Sonni tub ko'paytuvchilarga ajratish

Quyidagi teorema tub ko'paytuvchilarga ajratish algoritmini ifodalaydi hamda berilgan sonning tub ekanligini aniqlash imkonini beradi.

Teorema. Aytaylik, $n > 1$ toq son. Bu son murakkab son bo'ladi faqat va faqat $\exists p, q \in z$ 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 $\exists p, q \in z$ sonlar topish kerakki,

$n = p^2 - q^2$; $p^2 = n + q^2$ yoki $q^2 = n + p^2$ bajarilsin.

Agar $p^2 = n + q^2$, $q = 1,2,3 \ldots \ldots$ qiymatlar uchun $n + q^2$-son biror sonning to'la kvadratidan iborat bo'lmasa, u holda $q = (n - 1)/2$ qiymat uchun $n + q^2$ -ni tekshirib ko'riladi va biror sonning kvadratidan iborat bo'lsa, u holda n – tub son bo'ladi.

Misol. $n = 527$ soni tub yoki tub emasligi aniqlansin.

q	$n + q^2$
1	527+1=528
2	527+4=531
3	527+9=536

4	527+16=543
5	627+25=552
6	527+36=563
7	527+49=576=24^2

Demak, $q = 7$ uchun $n + q^2 = 24^2$ to'liq kvadratidan iborat. Bu esa tub ko'paytuvchilarga yoyilmasi bor degani, ya'ni

$527=24^2-7^2=(24-7)*(24+7)=17*31$.

Natija. Umuman olganda

$q = 1,2,3 \ldots \ldots (n-1)/2 = (527-1)/2 = 263$

qiymatgacha yetib borishi har doim ham shart emas ekan.

Yuqorida bayon etilgan usulni quyidagi ikkinchi tenglama ko'rinishda ham olish mumkin edi, yani $q^2 = p^2 - n$, $r = m, m+1, ..$

bu yerda m, soni sifatida quyidagi $m^2 \geq n$ shartni kanoatlantiruvchi eng kichik butun sonni olamiz. Shu tartibda $(p^2 - n)$ –soni, $r = m, m+1, ..$ qiymatlar uchun hisoblaymiz, toki $(p^2 - n)$ – son qandaydir sonning to'liq kvadrati bo'lmaguncha . Agar $p = (n+1)/2$ qiymatgacha $(p^2 - n)$ –son biror sonning to'liq kvadratidan iborat bo'lmasa, u holda n – tub son bo'ladi.

Shuni alohida takidlash joizki, bunday holda tekshirish yuqorigi holdagi tekshirishimizdan kamroq miqdordagi (sondagi) hisoblashlarni talab etadi.

Dikson usuli

Faraz qilinsinki, n sonini faktorlash lozim bo'lsin. Agar Lejandr e'tibor qaratgan $x^2 \equiv y^2 (mod\ n)$ taqqoslamani, ya'ni n ga karrali bo'lgan, x va y $k \neq 0$ uchun $x^2 - y^2 = kn$, unda $(x-y)(x+y) = kn$ bo'ladi. Agar kichik ehtimollik bilan $x - y = k$ va $x + y = n$ hosil qilinsa, kamida ½ ehtimollik bilan n ni faktorlash mumkin bo'ladi. Agar $EKUB(n, x-y)$ va $EKUB(n, x+y)$ bo'lsa, unda bular n ning fosh etilgan faktorlari bo'ladi.

Masalan, $100=9\ (mod\ 91)$, unda $10^2=3^2 (mod\ 91)$, $(10-3)(10+3) = 7*13 = 0\ (mod\ 91)$, demak, $7*13=91$.

Umumiy holda faktorlar $EKUB(n, x-y)$ va $EKUB(n, x+y)$ larni hisoblash orqali topiladi. $EKUB$ dan foydalanish zarurligini ko'rish uchun faraz qilinsinki, $x = 34, y = 8$, bular $34^2 = 8^2 (mod 91)$ taqqoslamani qanoatlantiradi, chunki $34^2\ (mod\ 91) = 64$ dir. Bu misolda $x+y=42$, binobarin, $EKUB(91,26) = 13$, $EKUB(91,42) = 7$. $x-y=26$ va $24^2 = 49 (mod 527)$ $(24+7)*(24-7) = k*527 = 17*31$.

Misol. $EKUB\ O(log\ a)^2$ dan kichik murakkablikka ega bo'lgan Yevklid algoritmi asosida oson hisoblanadi, ammo $x^2 \equiv y^2\ (mod\ n)$ taqqoslamani qanoatlantiruvchi o'zgaruvchilar juftini topish murakkab masaladir. Bu masalani yechishni osonlashtirish uchun taqqoslamani qanoatlantirish shartlarini biroz o'zgartirish kifoya.

Masalan, $41^2 = 32\ (mod\ 1649)$ va $43^2 = 200\ (mod\ 1649)$ bo'lsin, bu yerda 32 ham, 200 ham kvadratik chegirma emas.

Biroq, ikkala tenglamadan kutilgan taqqoslama $(41*43)^2 = 80^2\ (mod\ 1649)$ beruvchi $41^2 43^2 = 32*200 = 6400\ (mod\ 1649)$ topiladi.

Bu masalani yechish uchun foydalaniladigan subeksponensial murakkablikka ega bo'lgan algoritmlarda silliqlik xususiyatiga ega bo'lgan sonlardan foydalaniladi. Algoritmlar murakkabligi bu xususiyatdan foydalanishga bo'lgan yondashuv bilan farqlanadi.

Faktorlash masalasini yechishda ikki bosqichda hisoblashlar amalga oshiriladi:

- birinchi, tayyorlanish bosqichida biror chegara V tanlanadi va faktor bazasi hamda bu baza asosida tenglamalar sistemasi shakllantiriladi. Faktor bazasi deganda $2 \leq p_i \leq L^n$ shartini qanoatlantiruvchi k ta tub son p_i tushuniladi, bu yerda $L = e^{\sqrt{logn}loglogn}$ va bazaning $m^2 (mod\ n)$ sinfida eng kichik nomanfiy chegirmasi $Q(m)$ bilan belgilanadi;

- ikkinchi bosqichda tenglamalar sistemasining yechimi topiladi.

Odatda boshlang'ich hisoblashlar bir marta amalga oshiriladi, so'ngra faktorlar topiladi. Shunday qilib, faktorlash tenglamalar sistemasini yechishga o'tiladi.

Algoritmning birinchi bosqichini amalga oshirishda, faktor bazasini shakllantirishda $1 < m_i < n$ shartini qanoatlantiruvchi $m_1 \ldots m_{k+1}$ sonlar tasodifiy tarzda izlanadi va $Q(m_i) = p_i^{\alpha l,1} \ldots p_k^{\alpha l,k}$ $(i = 1, k+1)$ ko'rinishdagi sonlar shakllantiriladi. Bu yerda $m_i^2 = Q(m_i)(mod n)$ *silliq* sonlar (B-silliqlik munosabati bilan

bog'langan sonlar)dir, chunki ular uncha katta bo'lmagan tub sonlarning ko'paytmasi sifatida ifodalanadi.

$Q(m_i)$ ko'rsatkichlari vektorini $v_i\vec{}=(\alpha_{i,1}\dots\alpha_{i,k})\in Z^k$ bilan belgilanadi, bu yerda Z^k – k uzunlikka ega bo'lgan vektor fazosi.

k o'lchamli Bul fazosi $Z^k{}_2$ da $x_1v_1\vec{}+\dots+x_tv_t\vec{}\equiv 0\vec{}\ (mod\ 2)$ ko'rinishdagi tenglamalar sistemasini yechib, $x_1\dots x_{k+1}\in\{0,1\}$ topiladi, bu yerda $x_1\dots x_{k+1}$ vektori nolga teng vektordan farqli. Bunday yechim mavjud, chunki tenglamalar soni noma'lumlar sonidan kichik.

Hisoblangan qiymatlar $x\dots x_{k+1}$ uchun, quyidagi taqqoslama o'rinlidir:

$$(m_1{}^{x1}***m_1{}^{xk+1})^2\equiv p_1{}^{c1}***p_k{}^{ck}\ (mod\ n),$$

bu yerda $c_j=\sum^{k+1}_{i=1}x_i\alpha_{i,1}$, $c_k=\sum^{k+1}_{i=1}x_i\alpha_{i,k}$,

$X=m_1{}^{x1}***m_1{}^{xk+1}$, $Y=\prod^{k}_{j=1}p_j{}^{ck/2}$, c_k - x_i ta'rifga ko'ra butun son.

Natijada $X^2\equiv Y^2(mod\ n)$ taqqoslamasiga ega bo'linadi. So'ngra $1<EKUB\ (X\pm Y,n)<n$ tekshiriladi, shart bajarilsa faktorlar topilgan bo'ladi, aks holda algoritm boshiga qaytiladi va toki qoniqarli yechim topilmaguncha, boshqa m_i lar bilan yuqoridagi amallar bajariladi.

Pollard usuli

Aytaylik , n –juft bo'lmagan murakkab son, bo'luvchisi katta bo'lmagan. P – orqali n –sonning eng kichik tub bo'luvchisini belgilasak. Pollard usulining mohiyati shu bo'luvchini topishdan iborat.

Algoritm bajarilish ketma-ketligi quyidagidan iborat:

1. Aytaylik,

$$z=[n^{1/4}]+1, y=z^2>n^{1/2}$$

2. n va u' sonlarining eng kichik umumiy karralisini topamiz:

$$EKUK(n,u')=n*u'/EKUB(n,u').$$

3. Malumki u' soni berilgan n sonining eng kichik tub bo'luvchisi –ga bo'linadi, chunki $R\le\sqrt{n}<y$.

4. U holda berilgan sonning eng kichik tub bo'luvchisi P -ekanligi javob qilib beriladi.

Misol. Quyidagi sonni Pollard usulidan foydalanib ko'paytuvchilarga ajratilsin. $n = 527$

Yechish. Bevosita Ferma usulidan foydalanib ko'rsatish mumkinki:

$$527 = 24^2 - 7^2 = 17*31.$$

Maqsad shu sonni tub ko'paytuvchilarga yoyilmasini Pollard usuli yordamida amalga oshirishdan iborat. Har bir qadamni ketma-ket bajarib chiqamiz.

$z=\left[n^{\frac{1}{4}}\right]+1=\left[527^{\frac{1}{4}}\right]+1=4+1=5, y=z^2>n^{1/2}=25.$

EKUB(527, 25!) =17,

EKUK (527, 25!) = 527*25!/ 17 = 31*25!

Demak, 25! Sonining bo'linuvchisi 17 bor. U holda

R = 17 , javob esa 527 = 17*b, b = 31, yani 527 = 17*31.

Pollardning p usuli

Pollardning p usuli 1975 yilda Dj. Pollard tomonidan topilgan bo'lib, $F_8=2^{256}+1$ Ferma sonining tub ko'paytuvchilari aniqlanilgan.

Aytaylik, $n\in N$ bizdan shu sonni tub ko'paytuvchilarga ajratish masalasi so'ralayotgan bo'lsin. Bu usulning mohiyati quyidagidan iborat:

1)$f(x)$ – ko'phad darajasi ikki yoki undan katta bo'lgan, masalan $f(x)=x^2+1$ deb olinadi.

2) Tasodifiy $x_0\in Z$ tanlanadi.

3) Qandaydir fiksirlangan (malum bo'lgan) j,k –nomerlar uchun quyidagi shartlarning bajarishligi tekshiriladi:

$$1<EKUB(x_j-x_k;n)<n$$

toki, n –sonining tub ko'paytuvchilari topilmaguncha.

Bu yerda, agar j–soni

$$2^h\le j<2^{h+1}, h\in N$$

bo‘lsa, u holda $k = 2^n - 1$ ko‘rinishda olish maqsadga muvofiq.

Misol. n =728 soni tub ko‘paytuvchilari topilsin.

Yechish. Tasodifiy $x_0 \in Z$ –son sifatida

$$x_0 = 2, f(x) = x^2 + 1$$

deb olinsa, u holda

$$x_i = f(x_{i-1}) \ (mod\ n);\ i = 0,1,2$$

ya‘ni $x_0 = 2, x_1 = 5, x_2 = 26, x_3 = 677, \ldots$

$$EKUB\ (x_1 - x_0\ ;\ n) = EKUB\ (3; 728) = 1$$

Bu esa 3-shart intervaliga tegishli emas. Shuning uchun boshqa i – qiymatlar uchun hisoblashlarni davom ettirish kerak.

$$EKUB\ (x_2 - x_1; n) = EKUB(21; 728) = 7;$$

Ya‘ni 3-shart intervaliga tushdi. Demak, 729:7=104. U holda bitta tub ko‘paytuvchisi 7 ekan. Keyingi hisoblashlarni $n = 104$ uchun bajarish yetarli.

$EKUB\ (x_1 - x_0\ ;\ n) = EKUB\ (3;\ 104) = 1$, bu hol bajarilmaydi;

$EKUB\ (x_2 - x_1\ ;\ n) = EKUB\ (21;\ 104) = 1$; bu hol ham bajarilmadi;

$EKUB\ (x_3 - x_2;\ n) = EKUB\ (651;\ 104) = 1$; bu ham bajarilmadi;

$EKUB\ (x_4 - x_3\ ;\ n) = EKUB\ (457653;\ 104) = 1$; bu ham bajarilmadi;

Demak, boshqa j, k –nomerlar uchun tekshirish kerak:

$$j = 2, k = 0;$$

U holda

$$EKUB\ (x_2 - x_0;\ n) = EKUB\ (24;\ 104) = 8$$

va 1< 8 < 104 shart bajarildi.

Natijada 104:8=13 bo‘lib, bevosita tekshirish mumkinki 13 soni tub son, javob esa 728 = 7*8*13= $7*2^3*13$.

Faktorlash muammosiga asoslangan kriptobardoshliligi tanlanadigan tub sonlarning kattaligiga bog‘liq bo‘lgan shifrlash algoritmlaridan biri RSA hisoblanadi.

Quyida ushbu shifrlash algoritmining bayoni, faktorizatsiya muammosi va undan kriptoanalizchining foydalanish imkoniyati ko‘rsatib o‘tilgan. Shuningdek faktorizatsiya muammosining yechilishi

hujumchiga maxfiy ma’lumotdan xabardor bo‘lish imkoniyatini berishi ifodalanadi.

Jo‘natuvchi	Kriptoanalizchi	Qabul qiluvchi
6-qadam. Ochiq matn <GAZ> X(i) =< 4,1,9 > 7-qadam. X(i) ketma-ketligi ochiq kalit {7,33} yordamida shifrlanadi: $S = M^e modn$ Y(1)=(4^7)(mod 33)=16384(mod 33)=16 Y(2)=(1^7)(mod 33)=1(mod 33)=1 Y(1)=(9^7)(mod33)=4782969(mod 33)=15	(e,n) tutib oladi S shifrmatnni ham tutib oladi $M = C^d modn$ $(d \cdot 7) \cdot (\mathrm{mod}) f(p,q) = 1$ $f(p,q) = (p-1)^*$ $(q-1)$ Faktorizatsiya muammosi $n = p * q = 33$ $= 11 * 3$ $n = p^* q = 33 = 11^*3$ $f(p,q) = (p-1)^*$ $(q-1) = (11-1)^*(3-1) = 20$ $(d \cdot 7) \cdot (\mathrm{mod}20) = 1$ d=3 $M = C^d modn$ $= 16^3 mod33 = 4$	1-qadam. 2^{100} dan katta p=3 va q=11 sonlar tanlab olinadi. 2-qadam. $n = p^* q = 3 \cdot 11 = 33$ hisoblanadi. 3-qadam. Eyler funksiyasi aniqlanadi. $f(p,q) = (p-1)^*$ $(q-1 =)(3-1) \cdot (11-1) = 20$ 4-qadam $f()$ bilan o‘zaro tub son sifatida e=7 soni tanlab olinadi. 5-qadam $(d \cdot 7) \cdot (\mathrm{mod}20) = 1$ shartini qanoatlantiruvchi d soni tanlanadi. (f*1+1)/e= haqiqiy son 20*1+1/7=3 **d=3** Shifrlangan so‘z Y(i)=<16,1,15> Shifrlangan so‘zni dshifrlash qilish maxfiy kalit {3,33} yordamida bajariladi: $M = C^d modn$ Y(1)=(16^3)(mod 33)=4096(mod 33)=4 Y(1)=(1^3)(mod 33)=1(mod 33)=1 Y(1)=(15^3)(mod 33)=3375(mod 33)=9 Dastlabki son ketma-ketligi rasshifrovka qilingan X(i)=<4,1,9> ko‘rinishida dastlabki matn <GAZ> bilan almashtiriladi.

Faktorlash muammosi asos qilib olingan RSA algoritmining mualliflaridan biri Ronald Rayvest 1977 yilda 125 razryadli sonni faktorlash uchun 40 kvadratillion yil kerak bo'ladi deb "bashorat" qilgan edi. Ammo, 1994 yildayoq 129 o'nli xonali son faktorlandi.

7.3. Elliptik egri chiziq gruppasida diskret logarifmlash masalasining murakkabligiga asoslangan tizimlarning kriptoanaliz usullari

Elliptik egri chiziq (EECH)da nuqtalarni qo'shish amali aniqlangan. E() EECH nuqtalar to'plami nuqtalarni qo'shish amaliga nisbatan chekli kommutativ (Abel) gruppasini hosil qiladi.

Ta'rif. $(\{O,(x,y)\in E(K)\};\ "+")$ juftligi ko'rinishidagi algebraik strukturani EECH nuqtalari gruppasi deb ataladi.

EEChga asoslangan ko'pchilik kriptografik algoritmlarning bardoshliligi EECHda diskret logarifmlash masalasini yechish murakkabligi (ECDLP) bilan belgilanadi.

Bugungi kunda ECDLP masalasini yechishning eng yaxshi algoritmi, EECHda nuqtalarni $\sqrt{\pi n/2}$ tartibli qo'shishni talab etuvchi Pollardning ρ-usulidir.

EECH nuqtalari tartibi ERI bardoshliligini belgilab beruvchi muhim parametrlaridan biridir. $F(q)$ chekli maydonda EECH tartibi $\#E(F(q))$ deb belgilanuvchi $Ye(F(q))$ nuqtalar soniga aytiladi. Modomiki Veyyershtrass tenglamasi barcha $x\in F(q)$ uchun ikkidan ortiq yechimga ega emas ekan, $\#E(F(q))\in[1,2q+1]$ bo'ladi. Tartib qiymati intervali chegarasi mashhur Xasse teoremasiga muvofiq quyidagicha aniqlanadi:

$$q+1-2\sqrt{q}\le\#E(F(q))\le q+1+2\sqrt{q}.$$

Kriptografik algoritmlarga bo'ladigan barcha ma'lum hujumlarga qarshilik qilish uchun kriptotizim parametrlari quyidagi shartlarni qanoatlantirishi shart:

- q tartib katta tub songa teng yoki 2 ning katta darajasi shaklida bo'lishi;
- EECH nuqtalari soni $\#E(K)=nh$, bu yerda tub son $n>2^{160}, h\le 8, \#E(K)\neq q$;
- n barcha $1\le k\le B$ uchun q^k-1 ga bo'linmasligi shart.

Odatda amaliyotda ANSI X9.62-1998 da tavsiya qilinganidek $B\ge 20$. tanlanadi. GOST R 34.10-2001 da B son $B\ge 31$ tengsizlikni qanoatlantiradi. Germaniya Federativ Respublikasi standartida B uchun quyi chegara qilib $B\ge 10^4$ tanlangan.

A.V. Kobets fikricha bu xatolikni, EECH x koordinatasining qarama-qarshi nuqtasi bilan tengligi $G_x == -G_x$ keltirib chiqaradi va quyidagi aynanlikka olib keladi:

$$r_1=[k]G==r_1=[(q-1)k]G==r.$$

Agar kriptoanalizchiga har xil hujjatlarning e va e_2 xesh-qiymatlari uchun ERIni hisoblash (tanlab olish) zarur bo'lsa, u holda ikkala tenglamaning tengligidan s komponenta uchun, u asosida har xil hujjat uchun bir xil ERIni shakllantiruvchi shaxsiy kalit d ni aniqlashning o'zi yetarlidir. Lekin bu xatolikni tuzatish murakkab emas. Masalan, shaxsiy kalit daliliy generatsiyasini yetarli darajada ta'minlash yetarlidir.

Turli xildagi hujumlarga bardoshli, maxsus ishlab chiqilgan ERIni shakllantirish va tekshirish algoritmi sxemalari katta qiziqish uyg'otadi. Bunday algoritmlar guruhiga EEChda ERI xalqaro standarti darajasidagi Germaniya va Koreya milliy algoritmlarini kiritishimiz mumkin.

ERI algoritmi ma'lum turdagi hujumlarga yetarli darajada bardoshlilikka ega bo'lmog'i lozim. Har qanday hujum aniq maqsadga yetish uchun yo'naltiriladi. Shuni hisobga olgan holda EEChdagi ERI sxemalariga bo'lgan xavflarni xatarliligi oshib borish tartibida quyidagi turlarga ajratish mumkin:

- buzg'unchi kriptoanalizchining qo'lga kiritganidan farqlanadigan, ba'zi ma'nosiz ma'lumotlar uchun ERI hosil qilishiga olib keluvchi ekzistensial soxtalashtirish;
- oldindan tanlangan ma'lumot uchun ERIni yaratishga olib keluvchi selektiv soxtalashtirish;
- foydalanilayotganiga funksional ekvivalent bo'luvchi samarali ERI algoritmini yaratish bilan tugallanuvchi universal soxtalashtirish;
- ochiq kalitga mos ERI egasining shaxsiy kalitidan farqli bo'lishi mumkin bo'lgan maxfiy kalitni hisoblab topuvchi to'li ochish.

Hujumlardan eng kuchlisiga asoslangan eng kuchsiz tahdid

bardoshlisi ERI algoritmlarining eng ishonchli sxemasi hisoblanadi, ya'ni imzolangan ma'lumotlarni tanlab olishli hujumga asoslangan ekzistensial soxtalashtirishga.

Tizimli parametrlar Polig-Xellman, SHenksning "kichkina va katta qadamlar" $\rho-$Pollard murakkab logarifmi, indeksni hisoblab topishga va shu kabi boshqa hujumlarga bardoshlilikni ta'minlashi lozim.

Polig-Xellman algoritmi asosida bazaviy (generator) nuqtalar tartibini aniqlash uchun faktorlash masalasi yotadi. Algoritm faktorlash natijasida har bir modul bo'yicha olingan diskret logarifm yechimi evaziga kalitni topish murakkabligini pasaytiradi. Kalitni topishda qoldiqni topish haqidagi xitoya teoremasidan foydalaniladi.

"Kichkina va katta qadamlar" algoritmi tezkorlik va xotiradan foydalanish o'rtasidagi o'zaro moslikni ta'minlaydi.

EEChda diskret logarifmlash masalasini yechishnig ma'lum usullaridan eng mashhuri Pollardning $\rho-$ va $\lambda-$ usullaridir. EECH nuqtalarini qo'shish bilan aniqlanuvchi Pollardning $\rho-$usuli murakkabligini quyidagi ifoda orqali baholash mumkin:

$$lp = \sqrt{\pi q}/2,$$

bu yerda q - EECH bazaviy nuqtalari tartibi.

Pollard ρ-usuli tezligi $\sqrt{2}$ martaga oshirish mumkin. U holda usul murakkabligi $lp = \sqrt{\pi q}/4$ bilan baholanadi.

Pollard ρ-usulining afzallik tomonlaridan biri kriptoanaliz jarayonini mustaqil bir nechta parallel jarayonlarga ajratishdir. Bu holda har bir jarayonni amalga oshirish murakkabligi $l_p = \sqrt{\pi q/2r^2}$ va $l_p = \sqrt{\pi q/4r^2}$bilan baholanadi.

Pollard $\lambda-$usuli murakkabligi $l_\lambda = 2\sqrt{q}$ bilan va parallellashda $l_\lambda = 2r^{-1}\sqrt{q}$ bilan baholanadi.

Pollardning ikkala usulining qiyosiy tahlili Pollard λ-usuli Pollard ρ-usuliga nisbatan murakkabroqligini ko'rsatadi.

2004 yilda Pollard parallellangan algoritmi asosida "buzilgan" EECH kalitining eng katta uzunligi 109 bitni tashkil etdi.

7.1-jadvalda EEChda diskret logarifmlash masalasini yechishning hisoblash murakkabligini baholari keltirilgan.

EEChda diskret logarifmlash masalasini Pollard $\rho-$usulidan

foydalanib yechish murakkabligiga taalluqli keltirilgan ma'lumotlar shuni ko'rsatadiki, ERI algoritmlarida bazaviy nuqtasi $q \geq 2^{256}$ tartibli EECH qo'llanishi EECH bazasidagi ERI zarur bardoshliligining kelajakdagi istiqbolini ta'minlaydi. Bu GOST R 34.10-2001 ning 10 yil davomida muvaffaqiyatli ekspluatatsiyasi va kalitni ochish murakkabligi $3 * 10^{38}$ arifmetik amaldan iboratligi bilan ham asoslanadi.

7.1-jadval

ERIni buzish murakkabligi

Bazaviy nuqta G tartibi (uzunlik bitlarda)	Gruppadagi amallar soni
128	$1{,}63480*10^{19}$
192	$7{,}02141*10^{28}$
256	$3{,}01567*10^{38}$
320	$1{,}29522*10^{48}$
352	$8{,}48836*10^{52}$
384	$5{,}56293*10^{57}$
416	$3{,}64572*10^{62}$
448	$2{,}38926*10^{67}$
480	$1{,}56583*10^{72}$
512	$1{,}02618*10^{77}$
1024	$1{,}18824*10^{154}$

Keyingi paragrafda RSA kriptotizimi protokolining zaif tomonlaridan foydalanishga asoslangan hujum yo'nalishlari bayon etilgan.

7.4. 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;

b) imzolash paytida tasodifiy vektor qo'shish lozim yoki xeshlash funksiyasidan foydalanish lozim.

Nazorat 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. Elliptik egri chiziq gruppasida diskret logarifmlash muammosining murakkabligiga asoslangan tizimlarni eng tezkor kriptoanalizlash usullari yo'qligining asosiy sababi nimada?
7. EECH gruppasida diskret logarifmlash muammosini yechishning samarali hisoblangan qaysi kriptoanaliz usullarini bilasiz? Ularni amalga oshirish uchun zaruriy amallar soni qanday ifodalanadi?
8. Xizmat li sxemada ishlatilgan RSA algoritmi yordamida qo'yilgan imzoga hujum qanday uyushtiriladi va hujumdan qanday himoyalanish mumkin?
9. Tanlangan shifrmatn bo'yicha RSA algoritmidan foydalanib qo'yilgan imzoga hujum qanday uyushtiriladi?

FOYDALANILAYOTGAN ADABIYOTLAR

1. Столлинг В. Криптография и защита сетей. Принципы и практика. Изд.:Лори Вильямс, 2001.
2. [«Oshkora kalitli kriptotizimlarni kriptoanalizlash uchun qurol-vositalar ishlab chiqish va ularni tadqiq etish» mavzusi bo'yicha bajarilgan ilmiy-tadqiqot ishining 1-8-bosqich hisobotlari. – O'zAAA FTMTM, Toshkent, 2002.]
3. Зашита информатсии. Малий тематический випуск ТИИЭР. – Москва, 1988. – т.76, №5.
4. Diffie, W., Hellman, M.E. New directions in cryptography // IEEE Transactionson Information Theory, vol. IT-22, 1976. – Rr. 644-654.
5. ElGamal T., A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Transactions on Information Theory, 1985, vol. IT-31. – Rp. 469-472.
6. Молдовян А.А., Молдовян Н.А. Введениэ в криптосистеми с откритим ключом. Санкт – Петербург «БХВ-Петербург» 2005.
7. «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.
8. Арипов М.М., Пудовченко Ю.Е. Основы криптологии.- Ташкент: 2004. – 136 с.
9. Баричев С.Г., Серов Р.Е. Основы современной криптографии. Учебное пособие. – Москва: Лори Горячая Линия - Телеком, 2002. – 152 с.
10. Алексеев А. Криптография и криптоанализ: вековая проблема человечества. http://www.nvkz.kuzbass.net/hard-soft/soft/other/kripto-analiz.html.
11. «Oshkora kalitli kriptotizimlarni kriptoanalizlash uchun qurol-vositalar ishlab chiqish va ularni tadqiq etish» mavzusi bo'yicha bajarilgan ilmiy-tadqiqot ishining 1-8-bosqich hisobotlari. – O'zAAA FTMTM, Toshkent, 2002.
12. Бияшев Р.Г., Горковенко Е.В., Нысаанбаева С.Е. Алгоритмы шифрования сообщений и формирования электронной

цифровой подписи с заданной криптостойкостью информации // Институт проблем информатики и управления МОН РК, г. Алма-Ата.
13. O'z DSt 1109:2006 «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Atamalar va ta'riflar».
14. Защита информации. Малый тематический выпуск ТИИЭР. – Москва, 1988. – т.76, №5.
15. Diffie, W., Hellman, M.E. New directions in cryptography // IEEE Transactionson Information Theory, vol. IT-22, 1976. – Pp. 644-654.
16. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 - 816 с.
17. Венбо Мао. Современная криптография. Теория и практика. – Москва - Санкт-Петербург - Киев: Лори Вильямс, 2005.
18. Нильс Фергюсон, Брюс Шнайер. Практическая криптография –Москва: "Диалектика", 2004.
19. ElGamal T. On computing logarithm over finite fields // Advances in cryptology—CRYPTO'85 (Santa Barbara, Calif., 1985). (Lect. Notes in Comput. Sci.; V. 218). – Pp. 396-402.
20. ElGamal T., A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Transactions on Information Theory, 1985, vol. IT-31. – Pp. 469-472.
21. Столлингс В. Криптография и защита сетей. Принципы и практика. Изд.:Лори Вильямс, 2001.
22. Молдовян А.А., Молдовян Н.А. Введение в криптосистемы с открытым ключом. Санкт – Петербург «БХВ-Петербург» 2005.
23. O'z DSt 1106:2009 «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Xeshlash funksiyasi».
24. ГОСТ Р 34.11-94. Государственный Стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования.
25. Akbarov D.YE. Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanishlari. Toshkent. "O'zbekiston markasi ", 2009. – 432 b.

26. Шеннон К. Теория и связи в секретных системах. Работы по теории информации и кибернетике. – М.: Иностранная лит. 1963. – 243 б.

27. Авдошин С.М., Савельева А.А. «Криптоанализ: вчера, сегодня, завтра», Государственный университет – Высшая Школа Экономики. Москва – 2007.

28. Авдошин С.М., Савельева А.А. «Криптоанализ: современное состояние и перспективы развития», Государственный университет – Высшая Школа Экономики.

29. Жуков А.Е. «Криптоанализ по побочным каналам (Side Channel Attacks)», Пособие по курсу «Криптографические методы защиты информации» Москва – 2004.

30. Савельева А.А. «Исследование эффективности алгоритмов дискретного логарифмирования, использующих факторную базу», Государственный университет – Высшая Школа Экономики Москва – 2007.

31. Joux, Antoine. Algorithmic cryptanalysis / Antoine Joux. p. cm. -- (Chapman & Hall/CRC cryptography and network security) Includes bibliographical references and index, 2009.

32. Voorhoeve M. Factorization algorithms of exponential order // Computational methods in number theory. V. 1 / H.W. Lenstra and R. Tijdeman, editors. Amsterdam, 1982. P. 79—88.

33. Лунин А.В., Сальников А.А. Перспективы развития и использования асимметричных алгоритмов в криптографии. http: //www.ssl.stu.neva.ru.

34. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М., МЦНМО, 2003. – 328 с.

35. Кузнецов М.И., Бурланков Д.Е., Чирков А.Ю., Яковлев В.А. Компьютерная алгебра: Учебник. // Нижегородский Государственный Университет им. Н.И. Лобачевского, 2002. опубликовано: http://www.itlab.unn.ru/archive/docs/coaBook.pdf.

36. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc. 2004.

37. Соловьев Ю.П. Рациональные точки на эллиптических кривых //Соросовский образовательный журнал, №10, 1997.

38. Коробейников А.Г., Гатчин Ю.А. Математические основы криптологии. Учебное пособие. Санкт-Петербург-2004.

39. Алгоритмические основы эллиптической криптографии / Болотов А.А., Гашков С.Б., Фролов А.В., Часовских А.А. – Москва МЭИ, 2000.

40. Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы / Болотов А.А., Гашков С.Б., Фролов А.В., Часовских А.А. – Москва МЭИ, 2006.

41. Коблиц Н. Введение в эллиптические кривые и модулярные формы // Пер с англ. – Москва: Мир, 1988.

42. Коблиц Н. Курс теории чисел и криптографии. – М. Научное изд-во ТВП, 2001г. – 261 с.

43. Кобец А.М. Подмена подписанного документа в новом американском стандарте ЭЦП ECDSA// http: www.bugtrag/ru.

44. ANSI X9.62-1998: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).

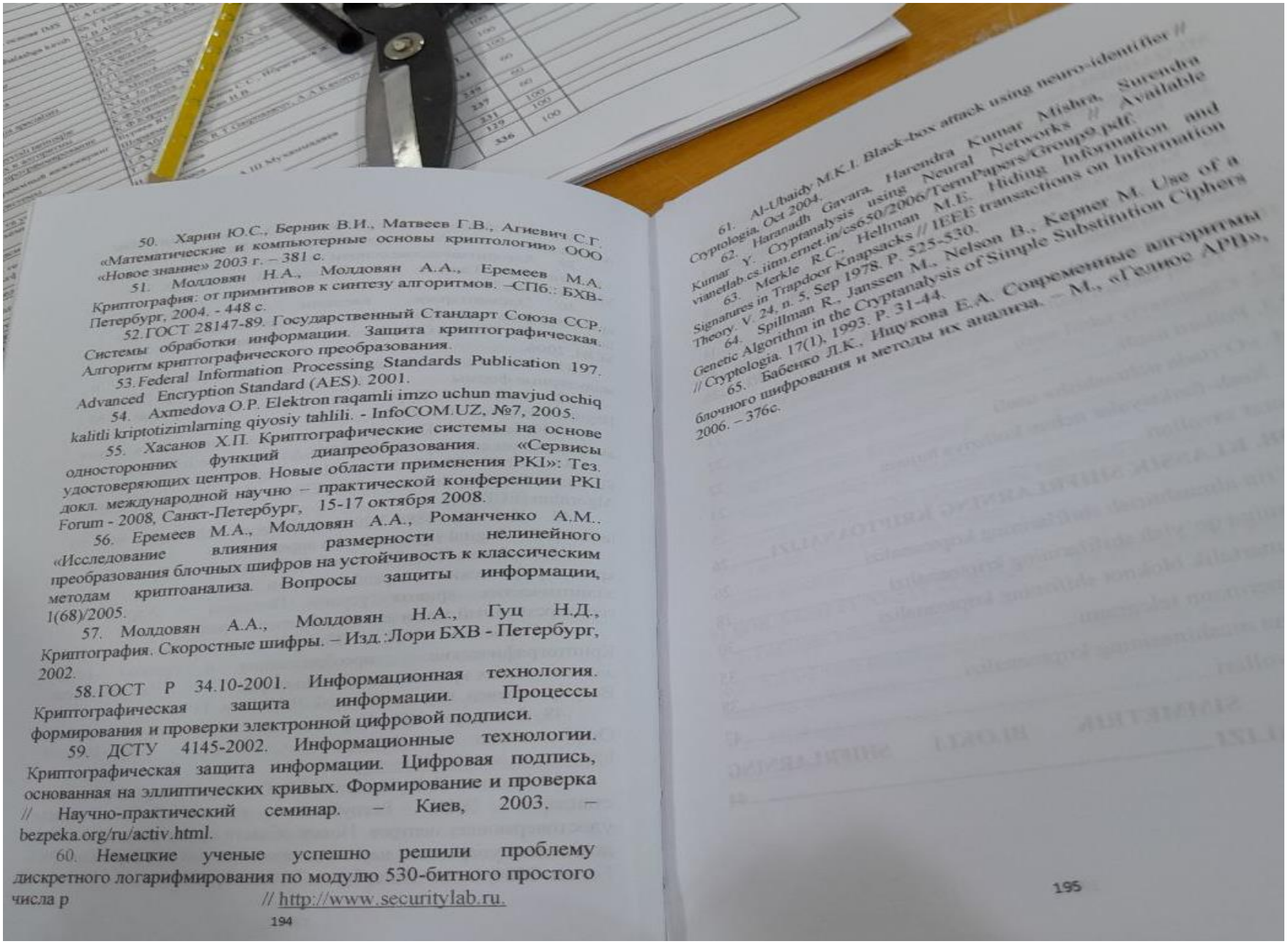
45. ISO/IEC 14888-3:2006. Information technology – Security techniques – Digital signatures with appendix.

46. Горбенко И.Д., Збитнев С.И., Поляков А.А. Криптоанализ криптографических преобразований в группах точек эллиптических кривых усулом Полларда // Харьковский государственный технический университет радиотехники.

47. Горбенко И.Д., Збитнев С.И., Поляков А.А. Криптографические преобразования в группах точек эллиптических кривых методом Полларда // Радиотехника: Всеукр. межвед. научно-техн. сб. 2001. Вып. 119.

48. Стандарт ЦП Украины на эллиптической кривой. Опубликовано: domarev , On: Nov-19-2004 http://www.security.ukrnet.net.

49. Хасанов П.Ф., Хасанов Х.П. Стойкость Государственного стандарта ЭЦП Республики Узбекистан //«Сервисы удостоверяющих центров. Новые области применения PKI»: Тез. докл. международной научно – практической конференции PKI Forum- 2006, Санкт-Петербург, 7-10 ноября 2006.



50. Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.Г. «Математические и компьютерные основы криптологии» ООО «Новое знание» 2003 г. – 381 с.

51. Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов. –СПб.: БХВ-Петербург, 2004. - 448 с.

52. ГОСТ 28147-89. Государственный Стандарт Союза ССР. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

53. Federal Information Processing Standards Publication 197. Advanced Encryption Standard (AES). 2001.

54. Axmedova O.P. Elektron raqamli imzo uchun mavjud ochiq kalitli kriptotizimlarning qiyosiy tahlili. - InfoCOM.UZ, №7, 2005.

55. Хасанов Х.П. Криптографические системы на основе односторонних функций диапреобразования. «Сервисы удостоверяющих центров. Новые области применения PKI»: Тез. докл. международной научно – практической конференции PKI Forum - 2008, Санкт-Петербург, 15-17 октября 2008.

56. Еремеев М.А., Молдовян А.А., Романченко А.М., «Исследование влияния размерности нелинейного преобразования блочных шифров на устойчивость к классическим методам криптоанализа. Вопросы защиты информации, 1(68)/2005.

57. Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Криптография. Скоростные шифры. – Изд.:Лори БХВ - Петербург, 2002.

58. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

59. ДСТУ 4145-2002. Информационные технологии. Криптографическая защита информации. Цифровая подпись, основанная на эллиптических кривых. Формирование и проверка // Научно-практический семинар. – Киев, 2003. – bezpeka.org/ru/activ.html.

60. Немецкие ученые успешно решили проблему дискретного логарифмирования по модулю 530-битного простого числа p // http://www.securitylab.ru.

61. Al-Ubaidy M.K.I. Black-box attack using neuro-identifier // Cryptologia, Oct 2004.

62. Kumar Y. Haranadh Gavara, Harendra Kumar Mishra, Surendra Kumar Y. Cryptanalysis using Neural Networks // Available vlanetlab.cs.iitm.ernet.in/cse650/2006/TermPapers/Group9.pdf.

63. Merkle R.C., Hellman M.E. Hiding Information and Signatures in Trapdoor Knapsacks // IEEE transactions on Information Theory. V. 24, n. 5, Sep 1978. P. 525-530.

64. Spillman R., Janssen M., Nelson B., Kepner M. Use of a Genetic Algorithm in the Cryptanalysis of Simple Substitution Ciphers // Cryptologia. 17(1), 1993. P. 31-44.

65. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. – М., «Гелиос АРВ», 2006. – 376с.

MUNDARIJA

AXMEDOVA O.P., XUDOYKULOV Z.T.,
ALLANOV O.M., BOYQUZIYEV I.M.

KRIPTOANALIZ

O‘quv qo‘llanma

Toshkent - “METODIST NASHRIYOTI” - 2024

Muharrir: Bakirov Nurmuhammad

Texnik muharrir: Tashatov Farrux
Musahhih: Xolmurodova Zahro
Dizayner: Ochilova Zarnigor

Bosishga 20.05.2024.da ruxsat etildi.
Bichimi 60x90. “Times New Roman” garniturasi.
Ofset bosma usulida bosildi.
Shartli bosma tabog‘i 13. Nashr bosma tabog‘i 12,5.
Adadi 300 nusxa.

“METODIST NASHRIYOTI” MCHJ matbaa bo‘limida chop etildi.
Manzil: Toshkent shahri, Shota Rustaveli 2-vagon tor ko‘chasi, 1-uy.

+99893 552-11-21

ISBN 978-9910-03-218-9