

G.U. JO'RAYEV

KRIPTOTAHLIL USULLARI

*O'zbekiston Respublikasi Oliy va o'rta maxsus ta'lim vazirligi
70610301 – «Kriptografiya va kriptoanaliz» hamda 70610302 –
«Axborot xavfsizligi» magistratura mutaxassisliklari uchun
o'quv qo'llanma sifatida tavsiya etgan*

TOSHKENT

2022

O'quv qo'llanma.

Kriptotahlil usullari. G.U. Jo'rayev

Mazkur o'quv qo'llanmasida hozirgi kunda simmetrik blokli shifrlarning kriptobardoshligini tadqiq qilish uchun keng qo'llaniladigan kriptotahlil usullari – differensial, chiziqli, chiziqli-differensial kriptotahlil usullari hamda slaydli hujumga asoslangan kriptotahlil usuli bayon qilingan. Shuningdek, ochiq kalitli RSA kriptotizimiga hujumlar tashkil qilish va ushbu hujumlardan himoyalanish bo'yicha ma'lumotlar keltirilgan.

O'quv qo'llanmasi oliy o'quv yurtlarining 70610301 – «Kriptografiya va kriptoanaliz» hamda 70610302 – «Axborot xavfsizligi» magistratura mutaxassisliklari talabalari hamda axborot xavfsizligi bo'yicha mutaxassislarga mo'ljallangan.

Taqrizchilar:

texnika fanlari doktori, professor Muxamediyeva D.T.

fizika-matematika fanlari doktori, professor Kasimov N.X.

M U N D A R I J A

Kirish	7
1-Bob. Dastlabki ma'lumotlar va ta'riflar	10
§1.1. Kriptografiyaning asosiy vazifasi va tushunchalari	10
§1.2. Kriptotahlil	12
§1.3. Kriptotahlil usullari haqida qisqacha ma'lumot	13
§1.4. Kriptotizimga hujum	16
§1.5. Kriptotahlilchi ega bo'lgan ma'lumotlarga ko'ra kriptotahlil turlari	18
§1.6. Bardoshlilik va shifrni buzish	22
Nazorat savollari	24
2-Bob. Kriptotahlil jarayonida qo'llaniladigan shifrlarning tavfsifi	27
§2.1. DES shifri	27
§2.2. S-DES-1 shifri	34
§2.3. S-DES-2 shifri	41
§2.4. GOST 28147-89 shifri	44
Nazorat savollari	47
3-Bob. Feystel tarmog'iga asoslangan blokli shifrlarning differensial kriptotahlili	50
§3.1. Differensial kriptotahlil usulining asosiy g'oyasi	50
§3.2. Differensial kriptotahlilni S-DES-2 shifriga qo'llanishi	53
§3.3. R-raunddan iborat bo'lgan blokli shifrlar uchun differensial kriptotahlilning umumiyligi	63
§3.4. DES shifrlash algoritmining bitta raundi differensial kriptotahlili	65
§3.5. DES shifrlash algoritmining uchta raundi differensial kriptotahlili	72
§3.6. DES shifrlash algoritmining to'liq raundi differensial kriptotahlili	75
§3.7. GOST 28147-89 shifrlash algoritmi raund akslatirishlarining tahlili	79
§3.8. GOST 28147-89 shifrlash algoritmining differensial tahlili	84
Nazorat savollari	91
4-Bob. SP tarmog'iga asoslangan blokli shifrning differensial kriptotahlili	93
§4.1. SP tarmog'iga asoslangan shifrning tavsifi	93
§4.2. SP tarmog'i asosidagi shifr akslatirishlarining tahlili	96
§4.3. SP tarmog'i asosidagi shifr uchun differensial xarakteristikalarini qurish	99
§4.4. Kalit bitlarini ajratish	102
§4.5. Differensial hujumning murakkabligi	105
Nazorat savollari	106
5-Bob. Blokli shifrlarning chiziqli kriptotahlili	108
§5.1. Chiziqli tahlil usulining asosiy g'oyasi	108
§5.2. Kalit bitlarini topish uchun chiziqli tahlilda qo'llaniladigan algoritmlar	110
§5.3. «Oddiylikdan murakkablikga» tamoyilini chiziqli tahlilda qo'llanilishi	113
§5.4. DES shifrlash algoritmi uchun chiziqli munosabatlar qurish	114
§5.5. DES shifrlash algoritmi chiziqli kriptotahlili	121
§5.6. SP tarmog'iga asoslangan shifrning chiziqli kriptotahlili va kalit bitlarini aniqlash	126
Nazorat savollari	133
6-bob. Chiziqli-differensial kriptotahlil usuli	135
§6.1. Chiziqli-differensial kriptotahlilni qurishning asosiy prinsiplari	135
§6.2. DES shifrlash algoritmiga chiziqli-differensial kriptotahlilni qo'llanilishi	141
Nazorat savollari	146

7-bob. Slaydli hujumga asoslangan kriptotahvil usuli	147
§7.1. Slaydli hujumga asoslangan kriptotahhlilning asosiy g'oyasi. Odatdag'i slaydli hujum	147
§7.2. Odatdag'i slaydli hujumni S-DES-1 shifrlash algoritmiga qo'llanilishi	151
§7.3. Yaxshilangan slaydli hujumning asosiy g'oyasi	156
§7.4. To'rt raundli o'z-o'ziga o'xhash shifrlash algoritmiga slaydli hujumni qo'llash Nazorat savollari	160
	162
8-bob. Ochiq kalitli RSA kriptotizimiga hujumlar tashkillashtirish	163
§8.1. RSA kriptotizimining xavfsizligi va uni buzish	163
§8.2. RSA kriptotizimiga hujumlar tashkil qilish	166
§8.3. RSA kriptotizimiga Viner hujumi	168
§8.4. Bir necha foydalanuvchilarga bir xil xabarni jo'natishga asoslangan hujum	171
§8.5. Ochiq kalit kichik bo'lganda bir-biriga bog'langan xabarlarga asoslangan hujum	173
§8.6. Eng katta umumiy bo'lувчи (EKUB)ni hisoblash orqali buzish usuli	176
Nazorat savollari	179
9-bob. RSA raqamli imzoga hujumlar tashkil qilish	181
§9.1. Notarius sxemasi bo'yicha RSA raqamli imzosiga hujum uyushtirish	181
§9.2. Tanlangan shifrmattin bo'yicha RSA raqamli imzosiga hujum uyushtirish	182
§9.3. RSA kriptotizimi va raqamli imzosi xavfsizligini ta'minlash uchun taklif qilingan tavsiyalar	183
Nazorat savollari	184
Foydalilanigan adabiyotlar ro'yxati	186

СОДЕРЖАНИЕ

Введение	7
1-Глава. Передварительные сведения и определения	10
§1.1. Основные функции и понятия криптографии	10
§1.2. Криptoанализ	12
§1.3. Краткая сведения о методах криptoанализа	13
§1.4. Атака на криптосистему	16
§1.5. Виды криptoанализа по имеющейся у криptoаналитика информации	18
§1.6. Стойкость и взлом шифра	22
Контрольные вопросы	24
2-Глава. Описание шифров, используемых в криptoанализе	27
§2.1. Шифр DES	27
§2.2. Шифр S-DES-1	34
§2.3. Шифр S-DES-2	41
§2.4. Шифр ГОСТ 28147-89	44
Контрольные вопросы	47
3-Глава. Дифференциальный криptoанализ блочных шифров, основанных на базе сети Фейстеля	50
§3.1. Основная идея метода дифференциального криptoанализа	50
§3.2. Применение дифференциального криptoанализа к шифру S-DES-2	53
§3.3. Общая схема дифференциального криptoанализа блочных шифров, состоящих из R-раундов	63
§3.4. Дифференциальный криptoанализ одного раунда алгоритма шифрования DES	65
§3.5. Дифференциальный криptoанализ трех раундов алгоритма шифрования DES	72
§3.6. Дифференциальный криptoанализ полного раунда алгоритма шифрования DES	75
§3.7. Анализ раундовых криптографических преобразований алгоритма шифрования ГОСТ 28147-89	79
§3.8. Дифференциальный криptoанализ алгоритма шифрования ГОСТ 28147-89	84
Контрольные вопросы	91
4-Глава. Дифференциальный криptoанализ блочных шифров, основанных на базе SP сеть	93
§4.1. Описание шифра, основанного на базе SP сеть	93
§4.2. Анализ преобразований шифра, основанного на базе SP сеть	96
§4.3. Построение дифференциальных характеристик для шифра, основанного на базе SP сеть	99
§4.4. Извлечение битов ключа	102
§4.5. Сложность дифференциальной атаки	105
Контрольные вопросы	106
5-Глава. Линейный криptoанализ блочных шифров	108
§5.1. Основная идея метода линейного анализа	108
§5.2. Алгоритмы, используемые в линейном анализе для поиска ключевых бит ...	110
§5.3. Применение принципа «от простого к сложному» в линейном анализе	113
§5.4. Построение линейных зависимостей для алгоритма шифрования DES	114
§5.5. Линейный анализ алгоритма шифрования DES	121
§5.6. Линейный криptoанализ ключей шифра, основанного на базе SP сеть и выявление битов ключа	126
Контрольные вопросы	133

6-Глава. Линейно-дифференциальный метод криptoанализа	135
§6.1. Основные принципы построения линейно-дифференциального криptoанализа	135
§6.2. Применение линейно-дифференциального криptoанализа к алгоритму шифрования DES	141
Контрольные вопросы	146
7-Глава. Метод криptoанализа, основанный на слайдовой атаке	147
§7.1. Основная идея криptoанализа, основанная на слайдовой атаке. Обычная слайдовая атака	147
§7.2. Применение обычной слайдовой атаки к алгоритму шифрования S-DES-1	151
§7.3. Основная идея улучшенной слайдовой атаки	156
§7.4. Применение методов слайдовой атаки к алгоритмам шифрования с четырехраундовым самоподобием	160
Контрольные вопросы	162
8-Глава. Организация атак на криптосистему RSA с открытым ключом ...	163
§8.1. Безопасность криптосистемы RSA и ее взлом	163
§8.2. Организация атак на криптосистему RSA	166
§8.3. Атака Винера на криптосистему RSA	168
§8.4. Атака, основанная на отправке одного и того же сообщения нескольким пользователям	171
§8.5. Атака на основе взаимосвязанных сообщений при небольшом размере открытого ключа	173
§8.6. Метод взлома путем вычисления наибольшего общего делителя (НОД)	176
Контрольные вопросы	179
9-Глава. Организация атак на цифровой подпись RSA	181
§9.1. Организация атак на цифровую подпись RSA по схеме нотариуса	181
§9.2. Организация атак на цифровую подпись RSA по выбранным шифр текстом	182
§9.3. Рекомендации по безопасности криптосистемы и цифровой подписи RSA	183
Контрольные вопросы	184
Список использованной литературы	186

KIRISH

Ma'lumki, kriptografik tizimlardan foydalanishda asosiy xavfsizlik tahdidlari quyidagilardan iborat bo'ladi:

1. Raqib tomonidan shifrlangan ma'lumotlarni ushlab qolish va ishlatilgan kalitni bilmasdan ulardan himoyalangan ma'lumotlarni olish – shifrni buzish.
2. Raqib tomonidan shifrlangan ma'lumotlarni ushlab qolish va maxfiy agentlar, joususlik va h.k. yordamida olingan kalitlar yordamida ulardan himoyalangan ma'lumotlarni olish.
3. Bir abonentdan ikkinchisiga ma'lumotni uzatishda qasddan (raqib tomonidan) yoki bilmasdan (aloqa kanallaridagi buzilishlar tufayli) shifrlangan ma'lumotning bir qismi yoki hammasini boshqa ma'lumot bilan almashtirish.
4. Abonentlardan biri shifrlangan ma'lumotning bir qismini yoki hammasini qasddan almashtirish va uni boshqa abonent yuborgan haqiqiy ma'lumot sifatida ta'kidlashi.
5. Abonentlardan birining shifrlangan ma'lumotni yuborganlik faktini rad qilishi.
6. Bir abonentdan ikkinchisiga uzatishda shifrlangan ma'lumotni qasddan yoki bilmasdan yo'q qilinishi.
7. Raqibning soxta shifrlangan ma'lumotlarni qonuniy abonentlar nomidan yuborishi.
8. Kalitlarni qasddan yoki bilmasdan yo'q qilish yoki almashtirish.

Bu yerda keltirilgan birinchi ikkita tahdidlarni amalga oshirish va oldini olish shifrlarni kriptotahlili fani doirasida ko'rib chiqiladi [1,2]. Qolgan 3–8 tahdidlarni bartaraf qilish mualliflik huquqining yaxlitligi va haqiqiyligini ta'minlaydigan kriptografik protokollarning kriptotahlili doirasida o'r ganiladi [3,4].

Kriptotahlil yunoncha kryptós (yashirin) va analyein (tahlil qilish) so'zlaridan olingan bo'lib, shifrlash kalitini bilmasdan shifr matnni dastlabki matnga o'girish usullari bilan shug'ullanuvchi fan hisoblanadi. Shuningdek, kriptotahlil kriptografik algoritm va protokollarni zaifligini aniqlash usullarini ham qamrab oladi. Norasmiy

tarzda kriptotahlil deyilganda shifrni buzish ham tushuniladi. Kriptotahlil bilan shug'ullanuvchi mutaxassislarini kriptoanalitiklar deb nomlashadi.

Kriptografik algoritmlarni amaliyatga muvaffaqiyatli qo'llash uchun mutaxassis turli tahdid modellariga nisbatan algoritmlarning bardoshlilik darajalarini aniq tushunishi kerak. O'z navbatida algoritmlarning kriptografik bardoshliligini baholashning eng muhim usuli bu kriptotahlildir.

Kriptotahlilning vazifasi shifrning buzilish ehtimolini aniqlash va shu tariqa uning ma'lum bir sohaga qo'llanilishini baholashdan iborat [1].

So'ngi o'ttiz yilda kriptologiyada ochiq ilmiy ishlar soni keskin oshdi. Kriptotahlil tadqiqotlarning eng faol rivojlanayotgan yo'nalishlaridan biriga aylandi. Kriptoanalitik uchun qiziq bo'lgan matematik usullarning safi kengaydi. Hisoblash texnikasining rivojlanishi ilgari amalga oshmaydigan hujumlarning mumkin bo'lgan turlarini yaratdi.

Simmetrik blokli shifrlarni kriptotahilini qilishda eng katta yutuqlarga XX asrning oxirida erishildi, bu esa differensial va chiziqli kriptotahlil usullarining paydo bo'lishi bilan bog'liq. Agar simmetrik blokli shifrlar kriptotahlilning mana shu usullariga nisbatan bardoshli bo'lsa, u holda axborotlarni ishonchli himoyasini ta'minlash uchun ushbu shifrlardan foydalanish mumkinligi tadqiqotchilar tomonidan asoslab berildi [5,6].

Hozirgi kunda foydalanilayotgan ochiq kalitli kriptografik tizimlarning deyarli barchasi katta natural sonni faktorlash yoki tub sonni moduli bo'yicha diskret lografmlash masalalariga asoslangan [7,8]. Chunki, ayni vaqtda ushbu masalalarni yechish matematik jihatdan murakkab yoki imkonsizligi mutaxassislar tomonidan e'tirof etilgan. Shu bois, ochiq kalitli kriptografik tizimlarning bardoshliklari ushbu masalalarning hisoblash nuqtai nazaridan murakkabliklari orqali ta'minlanadi [9,10]. Asimetrik kriptotizimlarni kriptotahlil qilish uchun "o'rtada uchrashuv" usuli kabi universal usullardan foydalanish mumkin. Yoki assimetrik shifrni bardoshligini ta'minlashda qo'llanilgan matematik muammoni hal qilish lozim bo'ladi.

Yangi kriptografik algoritm yoki protokollarning paydo bo'lishi ularni buzish yoki sindirishni yangi usullarini ishlab chiqishni talab qiladi. O'z navbatida har bir yangi kriptotahlil usulining paydo bo'lishi natijasi mavjud shifrlarning xavfsizlikgini baholashni qayta ko'rib chiqish hamda yanada xavfsizroq shifrlarni yaratishni taqoza etadi [11]. Bu masalalarni ijobiy hal qilishda «Kriptotahlil usullari» fanining o'rni beqiyos darajada mihimdir.

Ushbu o'quv qo'llanmasini tayyorlashda rus va inliz tilidagi o'quv adabiyotlaridan hamda Internet tarmog'idagi mavjud manbalardan keng foydalanidi.

1-BOB. DASTLABKI MA'LUMOTLAR VA TA'RIFLAR

Ushbu bobda kriptotahlilda foydalaniladigan bir qator tushunchalarning ta'rifi keltiriladi va ularning mohiyati ochib beriladi. Bu esa o'quvchiga keyingi boblarda keltirilgan mavzularni tushunishda yordam beradi.

§1.1. Kriptografiyaning asosiy vazifasi va tushunchalari

Kriptografiyada shifr va kriptografik tizim tushunchalaridan keng foydalaniladi. Shu sababli ushbu tushunchalarning mohiyatini bilish va ularning bir-biridan keskin farqlash maqsadga muvofiq [12].

Shifr bu uzatiladigan ma'lumotlarning maxfiyligini ta'minlash uchun mo'ljallangan bo'lib, qandaydir maxfiy parametrlarga (kalitlarga) bog'liq bo'lgan teaskarilanuvchi almashtirishlar tizimidir. Shifrlar diplomatik vakillarning o'z hukumatlari bilan maxfiy yozishmalar, qurolli kuchlarda maxfiy hujjatlar matnini texnik aloqa vositalarida uzatish uchun qo'llaniladi. Shifr odatiy belgilar (raqamlar, harflar yoki ma'lum belgilarning an'anaviy alifbosi) ning kombinatsiyasi yoki oddiy raqamlar va harflarni almashtirish algoritmi bo'lishi mumkin. Xabarni shifr yordamida sir tutish jarayoni *shifrlash deyiladi*. Shifrlarni yaratish va ulardan foydalanish haqidagi fan *kriptografiya deb ataladi*.

Shifrlashni kodlash bilan aralashtirib yubormaslik kerak. Odatda, *kodlash deyilganda* axborotdan to'g'ridan-to'g'ri foydalanish hamda axborotni saqlash, uzatish yoki avtomatik qayta ishslashda qulay bo'lishi uchun axborotni boshqa shaklga *o'tkazish tushuniladi*. Qisqa ma'noda, ma'lumotni kodlash deganda, ma'lumotni kod, ya'ni sodda ko'rinishda ifodalash tushuniladi. Kodlashda kalitdan foydalanilmaydi. Hozirgi vaqtda kodlash axborotga ruxsatsiz kirish yoki undan foydalanishdan himoya qilish uchun amalda qo'llanilmaydi.

Shuningdek, shifr bilan kriptografik tizim (yoki qisqacha kriptotizim) ni ham farqlash lozim. *Kriptografik tizim* bu shifrning almashtirish yoki akslantirishlar

oilasi va kalitlar to'plami (ya'ni, shifrlash algoritmi, kalitlar) dan tashkil topadi. Algoritmning o'zi kriptotizim emas. Shifrlash algoritmi kalitlarni taqsimlash va boshqarish sxemalari bilan to'dirilsagina, u tizimga aylanadi. Kriptografik tizimlar uzatilayotgan xabarlarni nafaqat maxfiyligini, balki ularning butunlilgi, foydalanuvchining autentligi (haqiqiyligi) ni ta'minlaydi.

Kriptografiyaning asosiy vazifasi axborotni kriptografik himoyalash tizimini ishlab chiqishdan iborat. Kriptografik tizim (yoki oddiy qilib aytganda kriptotizim) lar bu axborot xavfsizligini kriptografik usullar bilan ta'minlash tizimlaridir. Shifrlash, identifikasiyalash, imitohimoyalash, ERI kabi tizimlar kriptotizimlarning qismiy tizimlari bo'lshi mumkin [13]. Shu bois, kriptotizimlarning turlari quyidagicha bo'lshi mumkin:

- Shifrlash tizimi (konfidensiallikni ta'minlash uchun);
- Imitohimoyalash tizimi (butunlikni ta'minlash uchun);
- Identifikasiyalash tizimi (autentifikasiyalash uchun);
- ERI tizimi (mualliflikni rad qilishni oldini olish uchun);
- Kalitlar tizimi (boshqa kriptotizimlarni ishslashini ta'minlash uchun).

Shifrlash tizimi axborot bilan tanishish huquqiga ega bo'lмаган shaxslardan axborotni himoyalash uchun mo'ljallangan. Axborotni shifrlash yo'li bilan uning himoyasi ta'minlanadi. Shifrlash tizimi tushunchasi shifr, kalit tizimlari va axborotlarni kodlashtirish (ko'rinishini o'zgartirish) tushunchalaridan tarkib topadi.

Imitohimoyalash tizimi axborotni ruxsat etilmagan o'zgartirish yoki unga yolg'on axborotlarni tiqishtirishdan himoyalashga mo'ljallangan. Bunda himoyalash xabarni mazmunini autentifikasiyalash orqali ta'minlanadi. Imitohimoyalash tizimi tushunchasi imitohimoyalovchi kodlashtirish algoritmi, qabul qilingan axborotni asl (haqiqiy) ligi haqida qaror qabul qilish algoritmi hamda kalitli tizimni nazarda tutadi.

Identifikasiyalash tizimi axborot almashinuvida ishtirok etuvchi tomonlarni autentifikasiyalashga mo'ljallangan. Identifikasiyalash tizimi identifikasiyalash protokoli va kalit tizimidan tashkil topadi.

Elektron raqamli imzo tizimi sub'ektlarni oldin qilgan harakatlaridan tonishini oldini olishga mo'ljallangan. Bunda rad qilishdan himoyalanish axborot manbaini yoki xabarni autentifikasiyalash orqali ta'minlanadi. ERI tizimi tushunchasi raqamli imzo sxemasi va kalitli tizimi (ochiq kalitlar infratuzilmasi) dan iborat bo'ladi.

Kalit tizimi kriptografik tizimlardan foydalanish tartibini aniqlaydi. Ushbu tizim kalitlar to'plamidan hamda kalitlarni taqsimlash va boshqarishdan tashkil topadi.

§1.2. Kriptotahlil

Kriptotahlil atamasi XX asrning yigirmanchi yillarida taniqli amerikalik kriptograf Uilyam Fridman tomonidan kiritilgan [14].

Kriptografik bardoshlilik haqida asoslanadigan baholar olish maqsadida kriptografik tizimni tadqiq qilish *kriptografik tahlil* (yoki oddiy qilib *kriptotahlil*) deyiladi.

Kriptotahlil natijalari quyidagilar tomonidan ishlataladi:

- Kriptotizimni ishlab chiquvchisi va qonuniy foydalanuvchisi tomonidan ehtimolli raqib yoki buzg'unchi hujumidan axborotni himoyalash tizimi samaradorligini baholash uchun;
- Raqib yoki buzg'unchi tomonidan kriptotizimga hujum tayyorlash va uni amalga oshirish uchun.

Kriptografik tizim (kriptoprotokol) ning raqib yoki buzg'unchi tomonidan maxfiy kalitni yoki ochiq matnni qo'lga kiritish maqsadida qilingan hujumiga nisbatan qarshi turishini xarakterlovchi xossasi *kriptografik tizim (kriptoprotokol) ning kriptografik bardoshligi (kriptobardoshligi)* deyiladi.

Kriptotizimning bardoshliligi kriptotahlil o'tkazish jarayonida, ushu kriptotizim bardoshliligining asoslangan bahosi olingandan so'ng baholanadi.

Kriptotizimni kriptotahlili quyidagilardan tashkil topadi:

- Kriptotahlil usuli;

- Kriptotizimga hujum;
- Kriptotahlil farazlari.

Kriptotizimning bardoshligini tadqiq qilishga yo'naltirilgan, bir yoki bir necha matematik, texnik yoki boshqa g'oyalar bilan birlashtirilgan usullar birikmasi *kriptotahlil usuli deyiladi*.

Agar biror bir kriptografik algoritmga nisbatan to'liq saralash usuli samarasiz bo'lsa va uni kriptotahlil qilishning boshqa nisbatan tez usullari mavjud bo'lmasa, u holda ushbu *kriptografik algoritm kriptografik bardoshli deyiladi*. To'liq saralash usuliga nisbatan samarali bo'lган ixtiyoriy kriptotahlil usuli, hattoki uni amalda qo'llash mushkul bo'lsa-da shifrning kriptografik bardoshliligini pasaytiradi.

Kriptotahlil usulining xarakteristikasi mehnat sarfi va ishonchlikdan iborat bo'ladi.

Hozirgi kundagi kriptotahlil usullari quyidagilardan iborat:

- ✓ Kalitlarni to'liq saralash usuli;
- ✓ Kalitlarni ketma-ket saralash usuli (sequential key search);
- ✓ O'rtada uchrashuv usuli;
- ✓ Ekvivalent kalitlar usuli;
- ✓ Differensial (ayirmali) usul;
- ✓ Chiziqli usul;
- ✓ Algebraik tahlil usuli.
- ✓ Statistik usul;
- ✓ Chastotaviy tahlil usul.

§1.3. Kriptotahlil usullari haqida qisqacha ma'lumot

Kalitlarni to'liq saralash usuli qandaydir mezon bo'yicha kalitlarni yolg'on variantlarini chiqarib tashlash natijasida qolgan, bo'lishi mumkin bo'lган barcha kalitlarni saralashga asoslangan.

Kalitlarni ketma-ket saralash usulida kalitlar ketma-ket saralanib, kalitlar to'plamida qandaydir tartiblash, masalan, kalitlarni paydo bo'lish ehtimolligini hisobga olgan holda ayrim kalitlar chiqarib tashlanadi.

«*O'rtada uchrashuv» usuli.* Ushbu usulda kalit ikki qismga bo'linadi: birinchi bosqichda kalitning bitta qismi ustida hisoblashlar olib boriladi. Hisoblash natijalari xotiraga yoziladi. Ikkinci bosqichda xotiraga ketma-ket murojaat qilish orqali kalit aniqlanadi.

Shifrlash jarayoni E_1 va E_2 funksiyalarni ketma-ket qo'llash natijasida hosil qilingan bo'lsin:

$$C = E(P, K) = E_2(E_1(P, K_1), K_2).$$

Bu yerda K – uzunliklari mos holda m_1 va m_2 bo'lgan K_1 va K_2 qismiy kalitlarning konkatenasiyasidan tashkil topgan bo'lsin,

Faraz qilaylik, kriptotahlilchiga (P, C) ochiq matn-shifr matn juftligi ma'lum bo'lsin. U holda «*o'rtada uchrashuv» usuli* quyidagicha qo'llaniladi:

1. K_1 qismiy kalitning barcha bo'lishi mumkin bo'lgan variantlari bilan P ochiq matnni E_1 funksiya yordamida shifrlanadi. Shifrlash natijalari $U_1, U_2, \dots, U_{2^{m_1}}$ massivlarda saqlanadi.

2. K_2 qismiy kalitning barcha bo'lishi mumkin bo'lgan variantlari bilan C shifr matnni dastlabki matnga o'girib, E_2 funksiyani teskarisi aniqlanadi. Natijalar $V_1, V_2, \dots, V_{2^{m_2}}$ massivlarda saqlanadi.

3. U va V massivlar tahlil qilinadi. Agar C shifr matnni K_2 qismiy kalit bilan dastlabki matnga o'girishning qandaydir V_j natijasi P ochiq matnni K_1 qismiy kalit bilan shifrlashdan hosil bo'lgan U_i oraliq shifr matn bilan bir xil bo'lsa, qismiy kalitlarning $K=(K_1, K_2)$ juftligi aniqlanadi. Ushbu holda K kalit bilan «*o'rtada uchrashuv»* sodir bo'ldi deb hisoblanadi.

4. (P, C) ochiq matn-shifr matnlarning bir necha juftliklari (ikki, uch) uchun 1-3 qadamlar takrorlanadi. Bunda bo'lishi mumkin bo'lgan kalitlar to'plami qisqaradi. Odatda takrorlashlar soni juda kichik bo'ladi.

Shuni ham qayd etish lozimki, ushbu holda to'liq saralash usulining murakkabligi $2^{m_1+m_2}$ bo'lgani hoda «o'rtada uchrashuv» usulining murakkabligi $a \cdot 2^{m_1} + b \cdot 2^{m_2}$ bilan aniqlanadi, bu erda a, b - qandaydir o'zgarmaslar. $m_1 = m_2$ bo'lganda «o'rtada uchrashuv» usuli anchagina samarali bo'ladi. Aynan «o'rtada uchrashuv» usulining oddiyligi bois, kriptografiyada turli kalitlar bilan bir xil shifrlash algoritmi yordamida ochiq matnga ikki karrali shifrlash qo'llanilmaydi. Chunki, ularning tahlili oddiy, ya'ni bir martalik shifrlashdan unchalik farq qilmaydi. Shu sababli, Double DES algoritmidan shifrlash jarayonida foydalanilmaydi, amalda DES yoki uchlangan DES algoritmlaridan foydalaniladi.

Ekvivalent kalitlar usuli kalitlarni ekvivalent kalitlar sinfiga birlashtirish va har bir sinfdagi bittadan kalitni sinashga asoslangan.

Chastotaviy tahlil usuli esa ochiq va shifr matnlarni chastotaviy xarakteristikalarini o'rganishga asoslanadi.

Statistik usullar matematik statistikaga asoslanadi.

Differensial tahlil usuli bir xil ayirmaga ega bo'lgan ochiq matn juftliklaridan hosil bo'lgan shifrmattn juftliklari ayirmalari qiyatlarining notekis taqsimlanishidan foydalanishga asoslanadi. Ushbu usulni xesh funksiyalarni tahlili uchun ham qo'llash mumkin.

Chiziqli tahlil usuli kalit bitlarini aniqlash uchun ochiq matn va unga mos keluvchi shifr matn hamda shifrlash kalitining alohida bitlari o'rtaсидаги chiziqli munosabatdan foydalaniladi.

Slaydli hujum usuli. Raundlar sonining oshishi bilan algoritmning bardoshligini tahlil qilishda statistik hujumlarga asoslangan chiziqli va differensial tahlil kabi kriptotahlil usullarining qo'llanilishi murakkablashadi. Slaydli hujum usuli shifrlash algoritmi raundlari soniga bog'liq bo'lмаган kriptotahlil usulidir. Slaydli hujum shifrlashning har bir raundida bitta qismiy kalitga bog'liq bo'lgan kriptografik F-funksiyasidan foydalanishga asoslangan.

Algebraik tahlil usuli. Ushbu usulning asosiy mohiyati tadqiq qilinayotgan shifr akslantirishlarini murakkab bul tenglamalar sistemasi ko'rinishida ifodalashdan iborat. Bunda ochiq matn va unga mos keluvchi shifr matn hamda

shifrlash kalitining bitlari o'zaro bog'lanadi. Ochiq matn hamda kriptoanalitikka noma'lum kalit bilan hosil qilingan shifr matnning bir necha juftliklaridan foydalanib, kalit bitlariga nisbatan algebraik chiziqsizlik darajalari nisbatan past bo'lgan tenglamalar sistemasi tuziladi. Ushbu tenglamalar sistemasini yechish orqali kalit bitlarini aniqlash mumkin bo'ladi.

Kriptotahlilning har bir yangi usuli shifrlashning kriptografik algoritmlariga yangi talablarni paydo bo'lishiga turtki bo'ladi. Masalan, shifrmatndagi belgilarning taqsimlanishiga ko'ra kalit haqida faraz qabul qilishga asoslangan *chastotaviy tahlil usuli* shifrmatnlarda belgilarning tekis taqsimlanishi bo'yicha talabni paydo bo'lishiga sababchi bo'ldi.

§1.4. Kriptotizimga hujum

Raqib yoki buzg'unchning ma'lum bir kriptotahlil usuli asosida konkret kriptotizimni xavfsizlik darajasini pasaytirishga yo'naltirilgan harakati *kriptotizimga hujum deyiladi* [11].

Kriptotahlilni amalga oshirishda qabul qilinadigan shartlar va taxminlar majmuasi kriptotahlilning *farazi deyiladi*. Ayrim farazlar asosida kriptotizimga hujum bajariladi (modellashtiriladi). Ushbu farazlar quyidagi ma'lumotlar asosida qabul qilinadi:

- raqib (buzg'unchi) ning modeli, ya'ni uning maqsadi, imkoniyatlari va unda mavjud bo'lgan dastlabki ma'lumotlar;
- kriptotizimni amalga oshirish va qo'llash bilan bog'liq bo'lgan xususiyatlari.

Gollandiyalik kriptograf Ogyust Kerkgofts 1883 yilda «Harbiy kriptografiya» nomli kitobida harbiy shifrlarni loyihalashning oltita tamoyilini bayon qilgan [14]. Kerkgoftsning kriptotizimni ishlab chiqish yoki yaratish bo'yicha tamoyili kriptografik algoritm barcha foydalanuvchilar uchun ochiq bo'lgani holda faqatgina shifrlash kaliti maxfiy bo'lishidan iborat.

Klod Shennon 1949 yilda «Maxfiy tizimlarda aloqa nazariyası» mavzusidagi maqolasida «raqib maxfiy tizimni biladi» farazi asosida kriptotizimni loyihalash lozimligini ta'kidlab o'tgan [13].

Hozirgi kunda simmetrik blokli shifrlarga nisbatan hujumning quyidagi asosiy hujum turlari mavjud [11]:

- to'liq saralash usuliga asoslangan;
- ekvivalent kalitlarga asoslangan;
- differensial tahlilga asoslangan;
- chiziqli tahlilga asoslangan;
- slaydli va boshqalar.

Kriptotahlil usullarini ayrim belgi yoki alomatlarga ko'ra bir necha turlarga bo'lish mumkin.

Matematik usullardan foydalanish jihatiga ko'ra kriptotahlil turlari quyidagicha:

- statistik usullar (masalan, differensial va chiziqli tahlil usullari);
- analitik usullar (masalan, algebraik tahlil usuli).

Kriptotahlil usulining qo'llanish xarakteriga ko'ra universal yoki universal bo'limgan turlarga ajratish mumkin. Universal, ya'ni ko'pgina shifrlarga qo'llash mumkin kriptotahlil usullari quyidagilardan iborat:

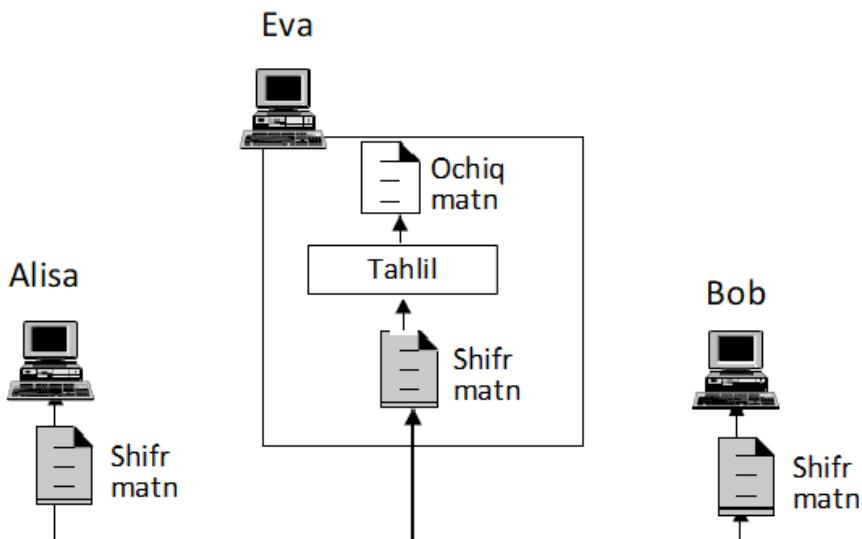
- to'liq saralash usuli;
- lug'at yordamida tahlil;
- «tug'ilgan kun» paradoksidan foydalanish;
- «o'rtada uchrashuv» usuli;
- «bo'lib tashla va boshqar» usuli.

Kriptotahlilchida mavjud axborotlarga ko'ra kriptotahlil usullari quyidagi turlarga bo'lish mumkin:

1. faqat shifr matn ma'lum bo'lishiga asoslangan kriptotahlil;
2. ochiq matn ma'lum bo'lishiga asoslangan kriptotahlil;
3. tanlangan ochiq matnga asoslangan kriptotahlil;

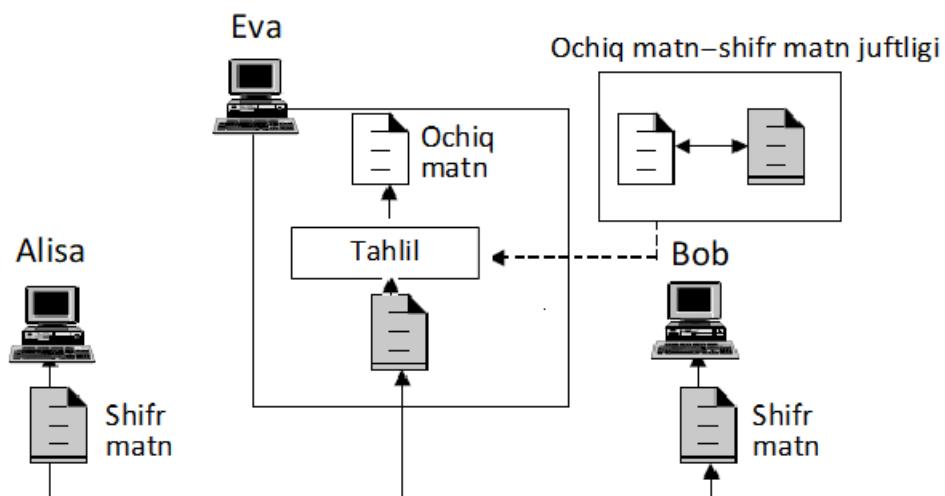
4. tanlangan shifr matnga asoslangan kriptotahlil.

§1.5. Kriptotahlilchi ega bo’lgan ma’lumotlarga ko’ra kriptotahlil turlari



1.1-rasm. Shifr matn asosidagi hujum.

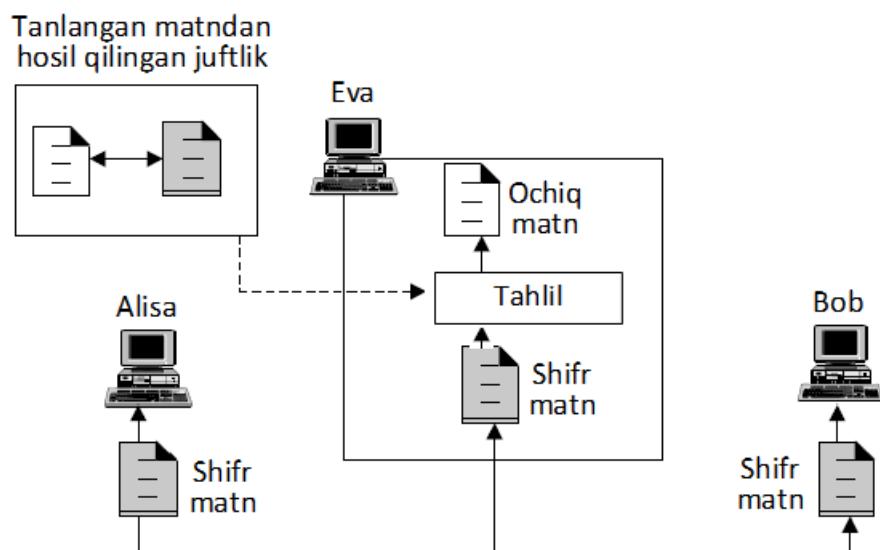
Shifr matn asosidagi hujum (ciphertext-only attack). Ushbu hujum faqat shifrmatnga asoslangan, ya’ni hujumchida faqatgina shifrmatn ma’lum, ammo u ochiq matnga ega emas. 1.1-rasmida ushbu hujum tasvirlangan. Bu rasm va keying rasmlarda Alisa va Bob – qonuniy foydalanuvchilar, Eva odatdagidek buzg’unchi vazufasini bajaradi [14].



1.2-rasm. Hujumchiga ma’lum ochiq matn asosidagi hujum.

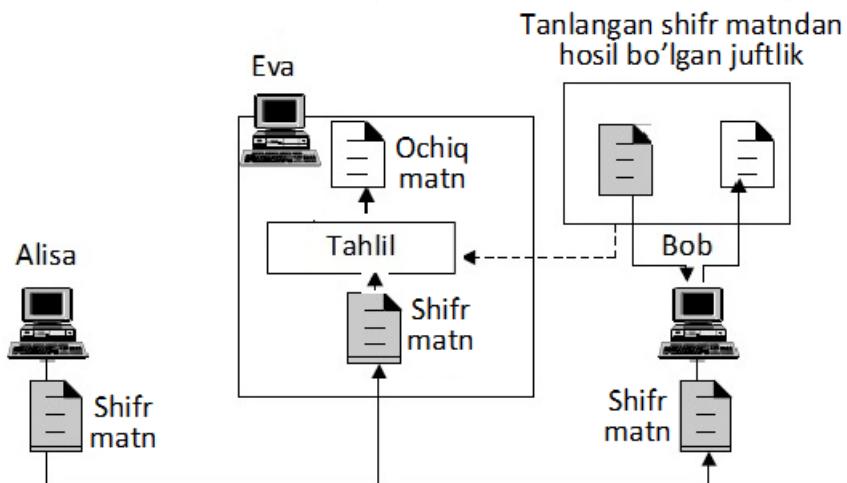
Ochiq matn asosidagi hujum (*known plaintext attack*). Hujumchida ochiq matn va unga mos keluvchi shifrmattan ham mavjud (1.2-rasm).

Ochiq matnni tanlash asosidagi hujum (*chosen plaintext attack*). Ushbu usul raqib (buzg'unchi) da u tomonidan tanlangan ochiq matnni kriptotizimni haqiqiy foydalanuvchisi tomonidan shifrlashga majburlash hamda buning natijasida hosil bo'ladigan shifrlangan xabarni kuzatish imkoniyatining mavjudligiga asoslangan (1.3-rasm).



1.3-rasm. Tanlangan ochiq matn asosidagi hujum.

Shifr matnni tanlash asosidagi hujum (*chosen ciphertext attack*). Ushbu hujum shifr matnni tanlash va unga mos keluvchi ochiq matnni noma'lum kalit bilan olish yo'li bilan kriptotahlilchi shifr haqida axborot yig'ishga asoslangan (1.4-rasm). Kriptotahlilchi shifr matndan ochiq matnni tiklash uchun bir yoki bir necha marta dastlabki matnga o'girish qurilmasidan foydalanishi mumkin. Kriptotahlilchi to'plangan ma'lumotlardan foydalanib, maxfiy shifrlash kalitini topishga harakat qiladi.



1.4-rasm. Tanlangan shifr matn asosidagi hujum.

Bir-biriga bog'liq kalitlar asosidagi hujum (related key attack). Ushbu hujum usuli kalitlarni o'zlari emas, balki ular o'rtaSIDAGI qandaydir munosabat ma'lum bo'lGanda qo'llaniladi.

Adaptiv hujum. Kriptotizimga qilinadigan ushbu hujum usulida kriptotizim qonuniy foydalanuvchisining harakati yoki boshqa sharoitlarga bog'liq holda kripthujumning tabiatini vaqt bog'liq holda o'zgarishi mumkin.

Kriptotahlilchida mavjud axborotlarga ko'ra kriptotahlil turlari va ularning maqsadlari quyidagi 1.1-jadvalda keltirilgan.

1.1-jadval. Kriptotahlilchida mavjud bo'lgan axborotga ko'ra kriptotahlil turlarining umumlashtirilgan ro'yxati.

Nº	Kriptotahlilchiga ma'lum bo'lgan ma'lumotlar	Kriptotahlil turlari
1	1.1. shifrmattn.	Shifrlash kaliti va algoritmi haqida ma'lumotga ega bo'lish maqsadida shifr matnni tahlil qilish.
2	2.1. shifrmattn; 2.2. shifrlash algoritmi.	Shifrlash kaliti haqida ma'lumotga ega bo'lish maqsadida shifr matnni tahlil qilish.
3	3.1. shifrmattn; 3.2. shifrlash algoritmi; 3.3. ochiq matnning bir qismi.	Shifrlash kaliti haqida ma'lumotga ega bo'lish maqsadida ochiq matnni tahlil qilish.
4	4.1. shifrmattn; 4.2. shifrlash algoritmi; 4.3. kriptotahlilchida mavjud ochiq matnlar orasidan u tomonidan tanlab olingan ochiq matn va unga mos keluvchi shifr matn.	Shifrlash kaliti haqida ma'lumotga ega bo'lish maqsadida tanlab olingan ochiq matnni tahlil qilish.
5	5.1. shifrmattn; 5.2. shifrlash algoritmi;	Shifrlash kaliti haqida ma'lumotga ega bo'lish maqsadida tanlab olingan shifr matnni tahlil qilish.

	5.3. kriptotahlilchi tomonidan tanlab olingan shifr matn va unga mos keluvchi deshifrlangan ochiq matn.	
6	6.1. shifrmavn; 6.2. shifrlash algoritmi; 6.3. kriptotahlilchi tomonidan tanlab olingan ochiq matn va unga mos keluvchi shifrlangan matn; 6.4. kriptotahlilchi tomonidan tanlab olingan shifr matn va unga mos keluvchi deshifrlangan ochiq matn.	Shifrlash kaliti haqida ma'lumotga ega bo'lish maqsadida tanlab olingan matnlarni tahlil qilish.
7	7.1. shifrmavn; 7.2. shifrlash algoritmi; 7.3. bir-biri bilan bog'langan shifrlash kalitlari.	Haqiqiy shifrlash kaliti haqida ma'lumotga ega bo'lish maqsadida tanlab olingan shifrlash kalitlarini tahlil qilish.

1.1-jadvalda kriptotahlilchida mavjud bo'lgan axborotga ko'ra, kriptotahlil har xil turlarining umumlashtirilgan ro'yxati keltirilgan. Jadvalda taqdim etilgan vazifalar ichida eng murakkabi kriptotahlilchi tasarrufida faqat shifrlangan matn bo'lgan holat hisoblanadi. Ayrim hollarda hattoki shifrlash algoritmi ham noma'lum bo'ladi, biroq asosan shifrlash algoritmini raqib biladi deb taxmin qilish kerak. Bunday sharoitlarda kriptotahlil yondashuvlaridan biri barcha ehtimoliy kalitlar variantlarini oddiygina birma-bir ko'rib chiqishdan iborat bo'ladi. Biroq agar barcha ehtimoliy kalitlar fazosi juda katta bo'lsa, bunday yondashuv noreal bo'lib qoladi. Shuning uchun raqib shifrlangan matnning o'zini tahlil qilishga ko'proq tayanishiga to'g'ri keladi, bu esa, qoidaga ko'ra, uning turli statistik xususiyatlarini aniqlashni anglatadi. Buning uchun raqib ochiq matn mazmuni haqida ayrim umumiyl taxminlarga ega bo'lishi, masalan, u qaysi tilda yozilgan ekanligini, bank hisob raqamlari kabi axborotli fayl ekanligi va boshqalarni bilishi lozim.

Raqibda faqat shifrlangan matn mavjudligida buzish harakatlariga qarshilik ko'rsatish juda ham oson, chunki bu holatda raqibda mavjud bo'lgan axborot hajmi minimal hisoblanadi. Biroq, ko'p hollarda kriptotahlilchiga ko'proq narsa ma'lum bo'ladi. Bunday mutaxassis ko'pincha mos keluvchi shifrlangan matnlar bilan birgalikda bitta yoki bir nechta ochiq xabarlarni ushlab qolish imkoniyatiga ega bo'ladi. Yoki kriptotahlilchi xabarda u yoki bu belgilar albatta mavjud bo'lishi haqida bilishi mumkin. Agar raqib umuman xabar mavzusi haqida tasavvurga ega

bo'lmasa, uning izlanishni qaysi yo'nalishda olib borishini hal qilishi qiyin bo'ladi. Biroq, agarda u xabar mazmuni haqida bironta maxsus axborotni bilsa, xabarning bir qismi uning uchun katta ehtimollik bilan ma'lum bo'lishi mumkin. Masalan, agar jo'natiladigan fayl tarkibida bank hisob raqamlari haqida axborot mavjud bo'lsa, raqib shu faylda ma'lum bir so'zlar qanday joylashishi lozimligini fahmlashi mumkin.

Agar kriptotahlilchida u yoki bu tarzda xabarni generasiya qilgan tizimga ulanish imkoniyati bo'lsa, bu holatda kriptotahlilchi tanlangan ochiq matnli kriptotahlil o'tkazish imkoniyatini qo'lga kiritadi. Bunday strategiya, masalan, differensial kriptotahlilda foydalaniladi.

Umumiy holatda, agar kriptotahlilchi o'z xohishiga ko'ra xabar tanlash va uni shifrlash imkoniga ega bo'lsa, shifrlash uchun xabarni to'g'ri tanlashda u kalitni topishdan umid qilishi mumkin.

Faqat nisbatan kuchsiz algoritmlar faqat shifrlangan matn tahlilida buzilishi mumkin. Umumiy holatda har qanday shifrlash algoritmi shunday ishlab chiqiladiki, ushbu algoritm ochiq matni ma'lum bo'lgan tahlil yordamida buzish harakatlariga chidamli bo'ladi. An'anaviy shifrlash sxemalari uchun deyarli barcha kriptotahlil shakllari ochiq matn strukturasiga xos bo'lgan ayrim xususiyatlar shifrlangan matn strukturasining mos keluvchi xususiyatlarida namoyon bo'lgan holda shifrlashda saqlanib qolishi mumkin.

§1.6. Bardoshlilik va shifrni buzish

Axborotni himoyalanganlik darajasi uni himoyalashda foydalanilgan kriptotizimning bardoshliligiga bevosita bog'liq, ya'ni kriptografik tizimlarning bardoshliligi ham turlicha bo'ladi. Quyida kriptotizimlar bardoshliligining asosiy turlari keltiriladi [7]:

1. amaliy bardoshlilik;
2. nazariy bardoshlilik;

3. isbotlanuvchi bardoshlilik.

Amaliy bardoshlilik kriptotizimga eng yaxshi hujumni amalga oshiruvchi algoritmning hisoblash murakkabligini anglatadi.

Ko'pchilik hollarda *amaliy bardoshlilik deyilganda* kriptotizim va foydalaniladigan hisoblash texnikasining real xususiyatlarini bilgan holda ma'lum bo'lgan algoritmlar ichidan eng tezkor algoritm bilan muvaffaqiyatli hujumni amalga oshirishning vaqt murakkabligi tushuniladi.

Qandaydir matematik model doirasida aniqlanadigan kriptografik bardoshlilik *nazariy bardoshlilik deyiladi*. Shifrlarning nazariy bardoshliligi haqidagi masalalarni birinchi marta Klod Shannon shakllantirdi. Abstrakt matematik modellar asosida nazariy bardoshlilikni o'rganish isbotlanuvchi bardoshlilik haqida fikr yuritish imkonini beradi.

Hozirgi kunda echilishi murakkab yoki imkonsiz hisoblangan matematik masalalardan kriptotizimlarni loyihalashda keng foydalaniladi. Masalan, katta natural sonlarni faktorlash, chekli maydonda yoki maxsus ko'rinishdagi elliptik egri chiziqda diskret logarifmlash masalalarini amalda yechish imkon mavjud emas. *Isbotlanuvchi bardoshlilikga ega bo'lgan kriptografik tizimlar* aynan shu kabi matematik murakkab masalalardan foydalanish asosida yaratiladi.

Umuman olganda buzg'unchi har qancha shifrmatlarga ega bo'lsa-da, lekin unga hech qanday axborot olish imkonini bermaydigan kriptotizimlar mavjudmi degan masala ko'pchilik o'quvchilarni qiziqtirishi tabiiy. Ha, bunday kriptotizimlar mavjud. Bunday xususiyatga ega bo'lgan *kriptotizimlar mutlaqo maxfiy hisoblanadi*. Mutlaqo maxfiy kriptotizimlar katta uzunlikdagi kalitlardan foydalanishni talab etishi sababli ulardan amalda kam foydalaniladi.

Agar shifrning to'liq saralash usuliga nisbatan samarali kriptotahlil o'tkazish imkonini beruvchi zaif tomoni aniqlansa, u hoda ushbu shifr *buzilgan éki sindirilgan shifr deb nomlanadi*. Masalan, to'liq saralash usuli 2^{128} ta bo'lishi mumkin bo'lgan kalitlarni saralashni talab etsin. Agar 2^{100} ta kalitlarni saralashni talab etuvchi usul taklif qilinsa, u holda shifrni buzilgan deb hisoblash mumkin.

Boshqacha aytganda, *shifrning buzilishi deyilganda*, shifrning muallifi tomonidan ta'kidlangan xarakteristikasiga mos kelmaydigan kriptografik xususiyatini anglatuvchi zaiflikning kriptoalgoritmda mavjudligi tasdiqlanganligini bildiradi.

To'liq saralash usuliga nisbatan samarali bo'lgan ixtiyoriy kriptotahlil usulining yaratilishi, agar ushbu usulni qo'llash amalda imkonsiz bo'lsa-da, shifrning kriptografik bardoshliligini pasaytiradi.

Ko'pchilik hollarda kriptotahlil algoritmning soddaroq modifikasiyasini buzishga harakat qilishdan boshlanadi. Agar ushbu harakat muvaffaqiyatlama yuzunlansa, undan so'ng to'laqonli algoritmni kriptotahlil qilishga o'tiladi. Masalan, N raundli shifrni buzishdan oldin ishni nisbatan kichik raundli shifrni, misol uchun $N/2$ raundli shifrni buzishga harakat qilishdan boshlash lozim.

Nazorat savollari

1. Shifr deb nimaga aytildi?
2. Shifrlash va kodlash tushunchalari o'rtasida farq bormi? Farq mavjud bo'lsa, ushbu farq nimadan iborat?
3. Kriptografik tizim (yoki qisqacha kriptotizim) nima?
4. Shifr va kriptotizim tushunchalari o'rtasida farq bormi? Farq mavjud bo'lsa, ushbu farq nimadan iborat?
5. Kriptografiyaning asosiy vazifasi nimadan iborat?
6. Shifrlash, imitohimoyalash va identifikasiyalash tizimlariga ta'rif bering.
7. Kriptografik tahlil (yoki oddiy qilib kriptotahlil) deb nimaga aytildi?
8. Kriptotahlil natijalari kimlar tomonidan qanday maqsadda ishlataladi?
9. Kriptografik bardoshlilik nima?
10. Kriptotizimni kriptotahlili nimalardan tashkil topadi?
11. Qachon kriptografik algoritm kriptografik bardoshli deyiladi?
12. Kriptotahlil usulining xarakteristikasi nimalardan iborat?
13. Hozirgi kundagi kriptotahlil usullari haqida qanday ma'lumotlarni bilasiz?

14. Kalitlarni to'liq saralash usuli nimaga asoslangan?
15. Kalitlarni ketma-ket saralash usulining mohiyati nimadan iborat?
16. «O'rtada uchrashuv» usulini tushuntirib bering.
17. Ekvivalent kalitlar usuli nimaga asoslangan?
18. Chastotaviy tahlil usulining mohiyati nimadan iborat?
19. Statistik usullar nimaga asoslangan?
20. Statistik usullarga misollar keltiring.
21. Algebraik tahlil usulining mohiyati nimadan iborat?
22. Kriptotizimga hujum deb nimaga aytildi?
23. Kriptotizimga hujum qanday farazlar asosida bajariladi?
24. Hozirgi kunda simmetrik blokli shifrlarga nisbatan hujumning qanday asosiy hujum turlari mavjud?
25. Matematik usullardan foydalanish jihatiga ko'ra kriptotahvil qanday turlarga bo'linadi?
26. Kriptotahvil usulini qo'llanish xarakteriga ko'ra qanday turlarga ajratish mumkin?
27. Kriptotahhlchida mavjud axborotlarga ko'ra kriptotahvil usullari qanday turlarga bo'linadi?
28. Shifr matn asosidagi hujum (ciphertext-only attack) ni tavsiflab bering.
29. Ochiq matn asosidagi hujum (known plaintext attack) ning mohiyati nimada?
30. Ochiq matnni tanlash asosidagi hujum (chosen plaintext attack) nimaga asoslangan?
31. Shifr matnni tanlash asosidagi hujum (chosen ciphertext attack) da maxfiy shifrlash kaliti qanday topiladi?
32. Bir-biriga bog'liq kalitlar asosidagi hujum (related key attack) ni qanday sharoitda qo'llash mumkin?
33. Adaptiv hujumning mohiyati nimada?
34. Kriptotizimlar bardoshliligining qanday asosiy turlari mavjud?
35. Nazariy bardoshlilik nima?

36. Isbotlanuvchi bardoshlilikga ega bo'lgan kriptografik tizimlar qanday yaratiladi?

37. Qachon kriptotizimlar mutlaqo maxfiy hisoblanadi?

38. Shifrnинг buzilishi deyilganda nimani tushunish lozim?

2-BOB. KRIPTOTAHYLIL JARAYONIDA QO'LLANILADIGAN SHIFRLARNING TAVFSIFI

O'quvchilarga qulaylik yaratish maqsadida ushbu bobda mazkur o'quv qo'llanmasi doirasida kriptotahylil usullari qo'llaniladigan ayrim simmetrik blokli shifrlar hamda ulardan foydalanish haqida ma'lumotlar qisqacha bayon qilinadi. Kriptotahylil usullarini qo'llashda ushbu shifrlarga o'nlab marta murojaat qilishga to'g'ri keladi.

§2.1. DES shifri

DES shifrining asosiy xarakteristikalari quyidagilardan iborat [7]:

- bloklar uzunligi 64 bit;
- dastlabki shifrlash kaliti uzunligi 56 bit;
- raundlar soni 16 ta.

DES shifrining birinchi raundida amalga oshiriladigan almashtirish va akslantirishlar. DES shifrlash algoritmi bo'yicha shifrlash jarayonining umumiyyxemasi 2.1-rasmda keltirilgan. Shifrlanishi lozim bo'lgan ochiq matn blokiga birinchi navbatda IP almashtirish qo'llaniladi (2.1-jadval), IP almashtirishdan so'ng u quyidagi ikki qismga bo'linadi (2.2-rasm):

L_0 – 32 ta katta razryadli bitlar ketma-ketligi;

R_0 – 32 ta kichik razryadli bitlar ketma-ketligi.

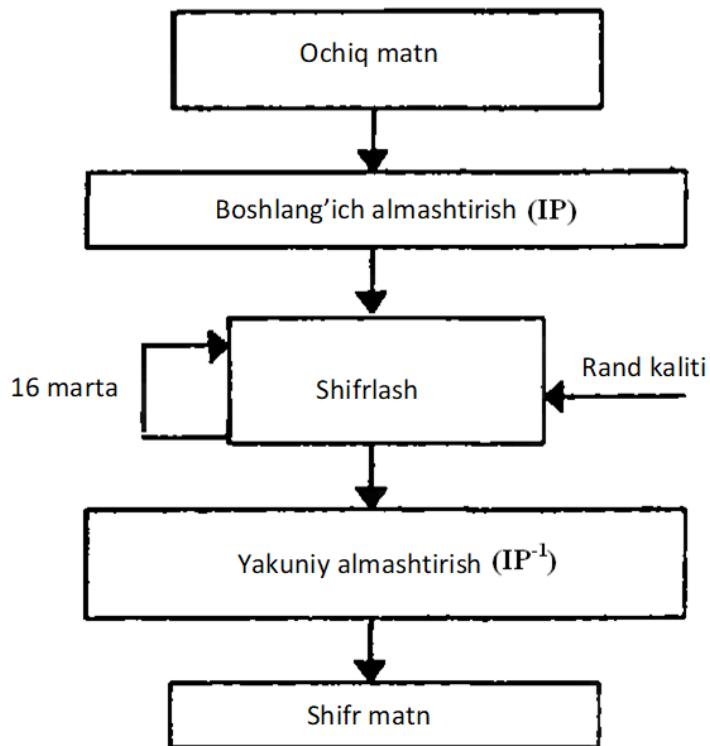
$T_{i-1} = L_{i-1}R_{i-1} - (i-1)$ -chi raund natijasi bo'lsin. U holda i -chi raund natijasi $T_i = L_iR_i$ quyidagicha hosil qilinadi:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i) \quad (i=1, 2, \dots, 16).$$

Bu erda $f(R_{i-1}, k_i)$ – shifrlash funksiyasi. O'n qismiy blok R_{i-1} bilan k_i raund kaliti f shifrlash funksiyasiga kiradi. O'z navbatida shifrlash funksiyasining natijasi L_{i-1} chap qismiy blok bilan 2 ning moduli bo'yicha qo'shiladi va bu qo'shish natijasi

keying raundga R_i o'n qismiy blok vazifasini o'tash uchun uzatiladi. Xuddi shunga o'xhash, joriy raunddagi R_{i-1} o'n qismiy blok keying raundga L_i chap qismiy blok vazifasini o'tash uchun uzatiladi (2.2-rasm).



2.1-rasm. DES algoritmi bo'yicha shifrlash jarayonining umumiyligini sxemasi.

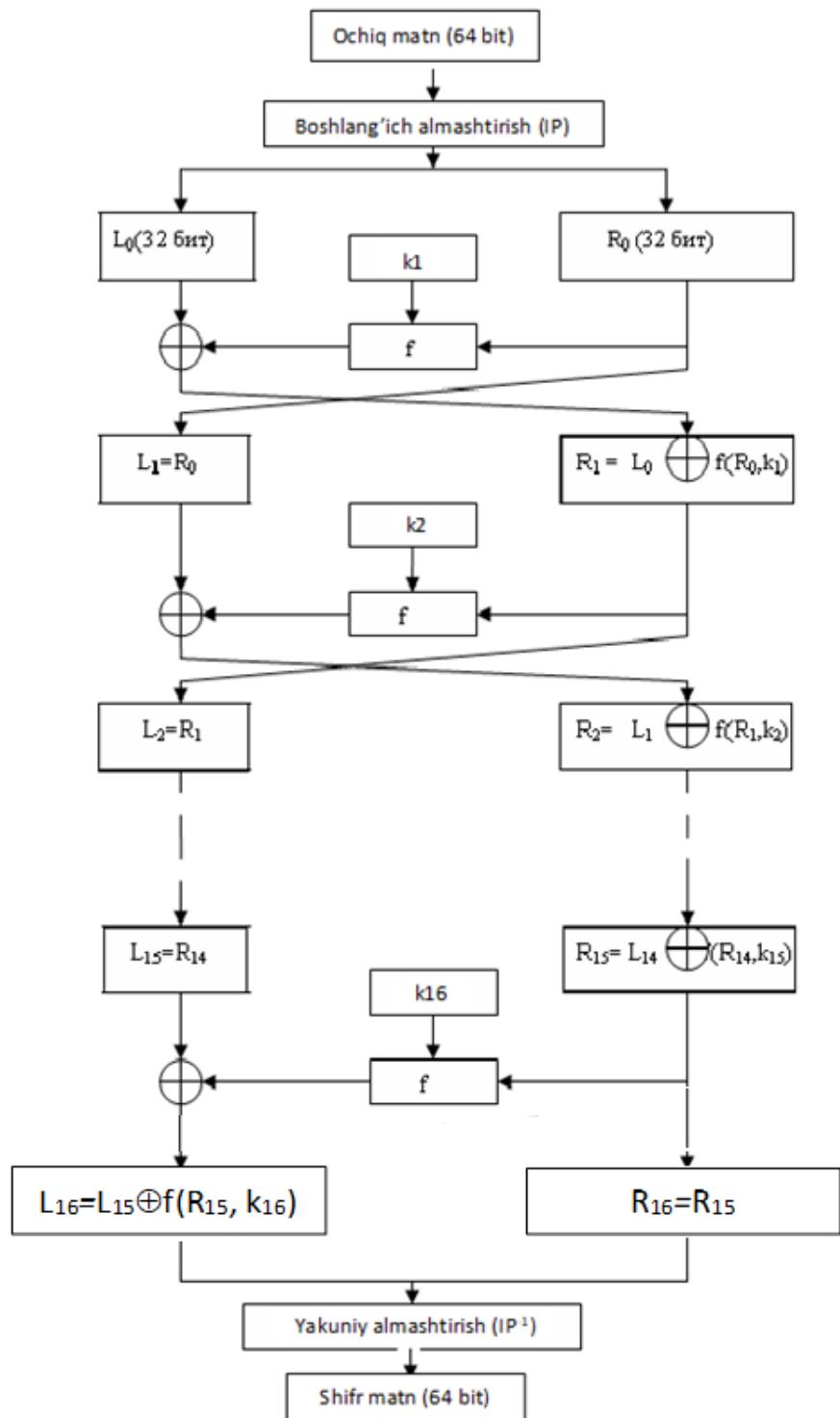
2.1-jadval. Boslang'ich almashtirish (IP).

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Shifrlashning boshqa qolgan raundlarida ham shifrlash jarayoni birinchi raunddagidek tarzda olib boriladi. Ushbu raundlarda faqatgina IP boshlang'ich almashtirish qo'llanilmaydi. Oxirgi o'n oltinchi raundda hosil bo'lgan qismiy blok natijalari konkatenasiya amali bilan birlashtiriladi va birlashtirish natijasiga teskari

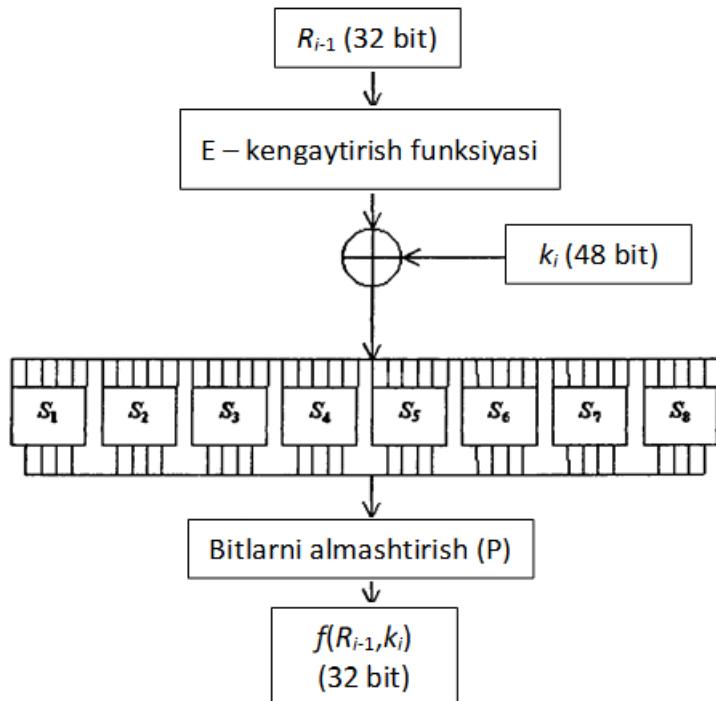
IP^{-1} yakuniy almashtirish qo'llaniladi. Ushbu yakuniy almashtirish natijasi ochiq matnga mos keluvchi shifr matnni ifodalaydi (2.1-rasm).

DES shifrlash algoritmi bo'yicha shifrlash va dastlabki matnga o'girishda bitta algoritmdan foydalilanadi. Dastlabki matnga o'girishda raund kalitlari teskari, ya'ni $k_{16}, k_{15}, \dots, k_1$ tartibda ishlataladi.



2.2-rasm. DES algoritmi bo'yicha shifrlash jarayoni.

$f(R_{i-1}, k_i)$ shifrlash funksiyasi. f shifrlash funksiyasida qo'llaniladigan kriptografik almashtirish va akslantirishlar 2.3-rasmida keltirilgan. Unga ko'ra f shifrlash funksiyasida quyidagi kriptografik almashtirish va akslantirishlar amalga oshiriladi. 32 bitli o'n qismiy blok 2.2-jadval bo'yicha kengaytiriladi. Natijada R_{i-1} o'n qismiy blokning uzunligi 32 bitdan 48 bitgacha kengayadi va unung bitlari o'rinnal mashadilar. Ushbu kengaytirish natijasi 48 bitli raund kaliti bilan 2 ning moduli bo'yicha qo'shiladi. 2 ning moduli bo'yicha qo'shish natijasi 48 bitli bitlar ketma-ketligidan iborat. 48 bitli bitlar ketma-ketligi 8 ta S blokka 6 bitdan taqsimlanadi. Har bir S blokka 6 bit kirib, ularning har biridan 4 bitli ketma-ketlik chiqadi. S bloklardan chiqqan 32 bitli bitlar ketma-ketligiga 2.3-jadvalga asosan P almashtirish qo'llaniladi. Buning natijasida bitlarning o'rni almashadi. Shu bilan $f(R_{i-1}, k_i)$ shifrlash funksiyasi o'z ishini yakunlaydi. P almashtirish natijasi $f(R_{i-1}, k_i)$ shifrlash funksiyasining qiymati hisoblanadi.



2.3-rasm. f shifrlash funksiyasi.

DES shifrlash algoritmi raund kalitlarini hosil qilish. Foydalanuvchi avval shifrlash kaliti, ya'ni 56 bitli tasodifiy bitlar ketma-ketligini tanlaydi. Ushbu ketma-ketlikda har bir baytdagi 1 lar soni toq bo'lishi nuqtai nazaridan ketma-ketlikning

8, 16, ..., 64 pozisiyalariga 8 ta bit qo'shiladi. Bu 8 ta bitlar shifrlash jarayonida ishlatilmaydi. Ushbu harakat shifrlash kalitini almashish va saqlashda yuzaga keladigan xatoliklarni aniqlash maqsadida qilinadi. 64 bitlardan tashkil topgan 8 ta bitlarni chiqarib tashlahdan hosil bo'lgan 56 ta bitlar ketma-ketligi C_0 va D_0 jadvallarga joylashtiriladi (2.4-jadval).

2.2 –jadval. R_{i-1} ni kengaytiruvchi E-funksiya.

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

2.3-jadval. S-bloklardan chiqqan betlar ketma-ketligini almashtirish (R).

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

2.4-jadval. C_0 va D_0 jadvallari.

$C_0 =$	57	49	41	33	25	17	9
	1	58	50	42	34	26	18
	10	2	59	51	43	35	27
	19	11	3	60	52	44	36
$D_0 =$	63	55	47	39	31	23	15
	7	62	54	46	38	30	22
	14	6	61	53	45	37	29
	21	13	5	28	20	12	4

Agar C_{i-1} va D_{i-1} jadvallar ma'lum bo'lsa, u holda C_i va D_i jadvallar chapga ularni 2.5-jadvajda keltirilgan 1 yoki 2 pozisiyaga raundik surishlar natijasida hosil qilinadi.

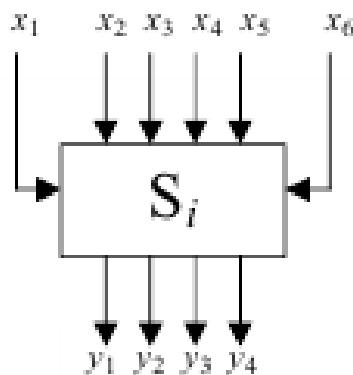
2.5-jadval. Siklik surishlar jadvali.

Raundlar	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Siljitch soni	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Raund kalitlari k_i ($i=1,16$) $C_i D_i$ jadvallarning 48 bitlari asosida shakllantiriladi. $C_i D_i$ jadvallardagi 9, 18, 22, 25, 35, 38, 43, 54 pozisiyalarda joylashgan bitlar hosil qilingan k_i raund kalitlarida ishtirok etmaydi (2.6-jadval).

2.6-jadval. k_i raund kalitini hosil qilishda $C_i D_i$ jadvallardagi ishtirok etadigan bitlar.

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32



2.4-rasm. DES algoritmi S bloklaridagi kiruvchi va chiquvchi bitlar ketma-ketliklari.

DES shifrlash algoritmi S bloklari. Algoritmda sakkizta S blokning har biriga oltita bit kirib, ularning har biridan to'rttadan bit chiqadi (2.4-rasm). Ushbu S bloklarning har biri 4×16 o'lchovli matrisadir. S bloklardan chiqish quyidagi qoida

asosida amalga oshiriladi. Faraz qliaylik, $x_1x_2x_3x_4x_5x_6$ bitlar ketma-ketligi S_5 blokka kirsin. U holda birinchi va oxirgi (ketma-ketlikning chetlarida joylashgan) x_1x_6 bitlari S_5 blokdagi satr nomerini, ketma-ketlikning o'rtasida joylashgan $x_2x_3x_4x_5$ bitlari S_5 blokdagi ustun nomerini ikkilik ko'rinishidagi qiymatini anglatadi. S_5 blokdagi mana shu satr va ustunlar kesishgan joyda ko'rsatilgan o'nlik sanoq tizimidagi sonning ikkilki ko'rinishi ushbu holda S_5 blokdan chiquvchi bitlar ketma-ketligini bildiradi. Xuddi shu qoida bo'yicha boshqa S bloklardan chiquvchi bitlar bitlar ketma-ketligi aniqlanadi. Misol uchun, 110001 bitlar ketma-ketligi S_3 blokka kirsin. U holda satr nomeri 11 (ya'ni, o'nlik sanoq tizimidagi 3), ustun nomeri 1000

2.7-jadval. DES shifrlash algoritmi S bloklari.

		U s t u n l a r															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S	0	14	4	13	1	5	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	2	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	4	8	14	6	2	11	15	12	9	4	3	10	5	0
	3	15	12	8	2	13	9	1	7	5	11	3	14	10	0	6	13
	0	15	1	8	14	4	11	3	4	9	7	2	13	12	0	5	10
	1	3	13	4	7	6	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	15	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	10	15	4	2	11	6	7	12	0	5	14	9
a	0	10	0	9	14	3	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	6	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	3	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
	0	7	13	14	3	3	6	9	10	1	2	8	5	11	12	4	15
	1	13	8	11	5	8	15	0	3	4	7	2	12	1	10	14	9
	2	13	6	9	0	6	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	0	1	13	8	9	4	5	11	12	7	2	14
t	0	2	12	4	1	6	10	11	6	8	5	3	15	13	4	14	9
	1	14	11	2	12	12	7	13	1	5	0	15	10	3	0	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	9	0	14
	3	11	8	12	7	7	14	2	13	6	15	0	9	10	3	5	3
	0	12	1	10	15	4	2	6	8	0	13	3	4	14	4	5	11
	1	10	15	4	2	10	12	9	5	6	1	13	14	0	7	3	8
	2	9	14	15	5	1	8	12	3	7	0	1	10	1	11	1	6
	3	4	3	2	12	9	5	15	10	11	14	0	7	6	13	8	13
r	0	4	11	2	14	7	0	8	13	3	12	14	7	10	0	6	1
	1	13	0	11	7	2	9	1	10	14	3	12	12	14	10	8	6
	2	1	4	11	13	9	3	7	14	10	15	3	8	5	15	9	2
	3	6	11	13	8	15	4	10	7	9	5	15	15	0	5	3	12
	0	13	2	8	4	4	15	11	1	10	9	5	14	15	2	12	7
	1	1	15	13	8	12	3	7	4	12	5	9	11	3	0	9	2
	2	7	11	4	1	1	12	14	2	0	6	5	13	2	14	5	8
	3	2	1	14	7	6	10	8	13	15	12	6	0	5	3	11	6

(ya’ni, o’nlik sanoq tizimidagi 8) ekanligini aniqlash mumkin. Endi S bloklar jadvalidan S_3 blokning uchinchi satri va sakkizinchisini ustuni kesihmasida 4 soni (ikkilki ko’rinishi **0100**) turganligini ko’rish mumkin. Demak, **110001** bitlar ketma-ketligi S_3 blokka kirsa, undan **0100** bitlar ketma-ketligi chiqadi.

Yakuniy IP^{-1} almashtirish. Oxirgi – o’n oltinchi raund natijasidan boshqacha foydalaniladi: $L_{16} = L_{15} \oplus F(R_{15}, k_{16})$ va $R_{16} = R_{15}$. Ya’ni, bunda bloklar o’z o’rinlarini almashtirmaydilar. Shundan so’ng $L_{16} R_{16}$ blokka IP^{-1} – yakuniy almashtirish qo’llaniladi (2.8-jadval). Bu almashtirish natijasi shifrmatnni tashkil qiladi.

2.8-jadval. Yakuniy IP^{-1} almashtirish.

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

§2.2. S-DES-1 shifri

Odatda biror bir kriptotizimni bardoshlilgini kriptotahvil qilishda ish uning bitta raundini yoki blok va kalit uzunliklari kichik bo’lgan, soddalashtirilgan modelini tahlil qlishdan boshlanadi. Tahlil qilish jarayonida ushbu modellar murakkablashtirilib boriladi. Kriptotizimning tahlil qilish uchun tanlab olingan modellari ushbu kriptotizimning barcha kriptografik xususiyatlarini o’zida aks ettirgan bo’lishi lozim. Agar kriptotahvil kriptotizimning soddalashtirilgan modelllariga nisbatan muvaffaqiyatli bajarilsa, u holda bevosita kriptotizimni o’zini tahlil qilishga o’tish mumkin. Shu maqsadda DES shifrlash algoritmining soddalashtirilgan ikkita o’quv algoritmi keltiriladi.

Soddalashtirilgan DES bu amaliy ahamiyatdan ko’ra ko’proq o’quv ahamiyatiga ega bo’lgan shifrlash algoritmi hisoblanadi [1]. Xususiyatlari va strukturasiga ko’ra u DES kabi, biroq ancha kichik ko’rsatkichlarga ega. Ushbu

algoritm Santa-Klara universiteti professori Edvard Sheyfer tomonidan ishlab chiqilgan. Qulaylik uchun kelgusida bu algoritmni S-DES-1 deb ataymiz.

Mazkur algoritm kirishda 8 bitli ochiq matn blokidan va 10 bitli kalitdan foydalanadi, chiqishda esa 8 bitli shifrlangan matn bloki hosil qilinadi. S-DES-1 dastlabki matnga o'girish algoritmi boshlang'ich ma'lumotlar sifatida 8 bitli shifrlangan matn blokidan va shifrlash uchun foydalanilgan 10 bitli kalitdan foydalanadi, dastlabki matnga o'girish algoritmi natijasida 8 bitli ochiq matn bloki hosil qilinishi lozim.

S-DES-1 shifrlash algoritmi ikkita raunddan iborat bo'lib, unda qyuidagi almashtirish va akslantirishlar ketma-ket bajariladi (2.6-rasm):

- boshlang'ich almashtirish IP ;
- f shifrlash funksiyasi;
- ma'lumotlar ketma-ketligining ikkita qismi oddiygina o'rinn al mashadigan SW almashtirish;
- yana bir marta f shifrlash funksiyasi;
- boshlang'ich almashtirishga teskari bo'lgan almashtirish (IP^{-1}).

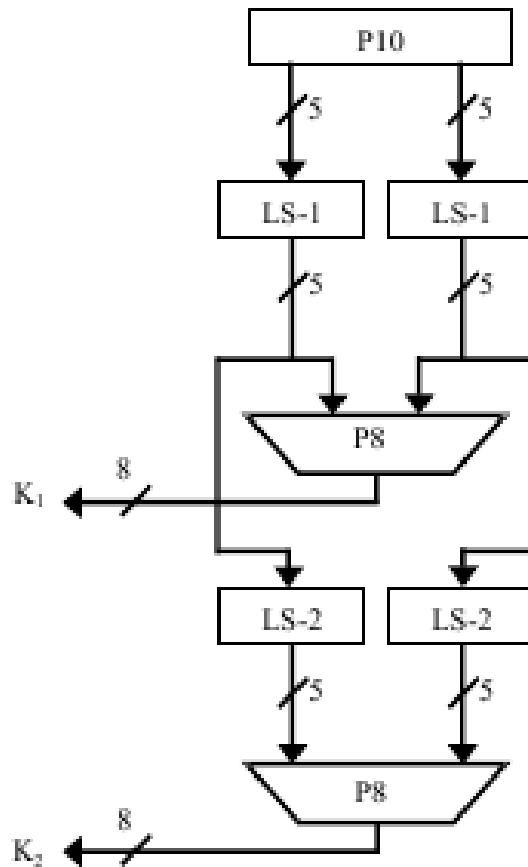
S-DES-1 raund kalitlarini hisoblash. S-DES-1 algoritmida foydalaniladigan dastlabki shifrlash kaliti uzunligi 10 bitdan iborat. Bu kalitdan shifrlash va dastlabki matnga o'girishning ma'lum bir bosqichlarida ikkita 8 bitli qismiy kalit yaratiladi. 2.5-rasmda bu qismiy kalitlar yaratish jarayonlari sxemasi ko'rsatilgan.

Dastlab kalit bitlarini joy almashtirishi quyidagi tarzda bajariladi. Agar 10-bitli kalit ($k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10}$) ko'rinishida ifodalansa, u holda R10 almashtirishni formula bilan berish mumkin:

$$\begin{aligned} R10(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10}) &= \\ &= (k_3, k_5, k_2, k_7, k_4, k_{10}, k_1, k_9, k_8, k_6). \end{aligned}$$

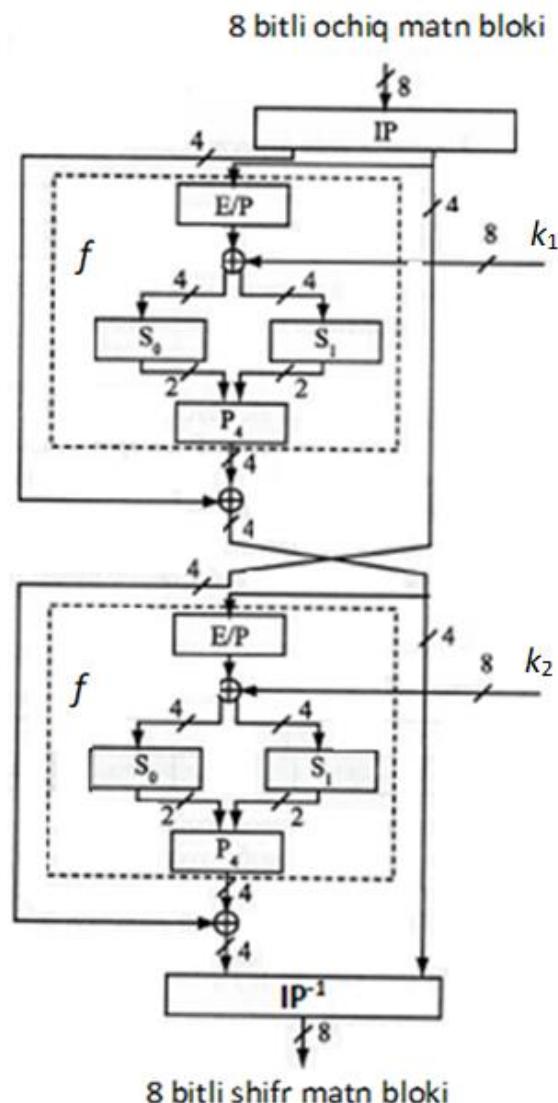
2.9-jadval. R10 almashtirish jadvali

R10									
3	5	2	7	4	10	1	9	8	6



2.5-rasm. S-DES-1shifri kalitlarini hisoblab chiqish.

Shuningdek, R10 almashtirishni 2.9-jadvalda ko'rsatilganidek shaklda ham aks ettirish mumkin. Bu jadvalni chapdan o'ngga qarab o'qish lozim. Ushbu jadvalga asosan boshlang'ich kalitning birinchi biti $R10$ almashtirish natijasida ettinchi, oltinchi biti o'ninchi bitga aylanadi va h.k. Masalan, 2.1-jadvalga muvofiq dastlabki ko'rinishi (1010000010) bo'lgan kalit quyidagi ko'rinishga keltiriladi - (1000001100) (2.10-jadval). $R10$ almashtirish natijasi 10 bitli ketma-ketlik bo'lib, ushbu ketma-ketlik ikkita 5 bitli o'n va chap qismiy bloklarga bo'linadi: (10000, 01100). Undan so'ng $LS-1$ funksiyani qo'llash natijasida ushbu qismiy bloklarning har biri chapga bir pozisiyaga siklik suriladi. Bizning holatda siklik surish natijasida quyidagi ketma-ketlik olinadi – (00001, 11000).



2.6-rasm. S-DES-1 shifrlash algoritmi.

2.10-jadval. $P10(1010000010)$ almashtirish natijasi.

R10									
3	5	2	7	4	10	1	9	8	6
1	0	0	0	0	0	1	1	0	0

2.11-jadval. $P8$ almashtirish jadvali.

R8							
6	3	7	4	8	5	10	9

2.12-jadval. $P8(00001, 11000)$ almashtirish natijasi.

R8							
6	3	7	4	8	5	10	9
1	0	1	0	0	1	0	0

Endi siklik surish natijasiga 2.11-jadvalga muvofiq $R8$ almashtirishi qo'llanadi, buning natijasida 10 bitli kalitdan joyi almashtirigan 8 ta bit tanlab olinadi (2.12-jadval). $P8$ almashtirish natijasida K_1 kalit hosil qilinadi, K_1 kalit quyidagi ko'rinishga ega bo'ladi - (10100100).

2.13-jadval. $LS-2(00001, 11000)$ funksiyani qo'llash natijasi.

0	0	0	0	1	1	1	0	0	0
0	0	1	0	0	0	0	0	1	1

2.14-jadval. $R8(00100, 00011)$ funksiyani qo'llash natijasi.

R8								
6	3	7	4	8	5	10	9	
0	1	0	0	0	0	1	1	

$LS-1$ funksiyani qo'llash natijasida olingan ikkita 5 bitli ketma-ketliklarga qaytiladi va bu ketma-ketliklarni har biri $LS-2$ funksiyaga muvofiq ikki pozisiya chapga suriladi. Bizning muayyan misolda (00001 11000) qiymat quyidagi ko'rinishga keltiriladi - (00100, 00011). Endi $LS-2$ funksiyani qo'llash natijasiga $R8$ almashtirishni qo'llab, $K_2=01000011$ ko'rinishda hosil qilinadi (2.14-jadval).

Boshlang'ich va yakuniy almashtirishlar. Shifrlash algoritmiga kirishga shifrlanishi lozim bo'lgan ochiq matnning 8 bitli bloki kelib tushadi, unga nisbatan 2.15-jadvalda keltirilgan IP funksiyasi qo'llaniladi. Ushbu IP almashtirish natijasida ochiq matnning barcha 8 biti o'z o'rinalarini o'zgartiradilar, ya'ni bitlarning joylashish tartibi o'zgaradi.

2.15-jadval. Boshlang'ich almashtirish (IP).

IP							
2	6	3	1	4	8	5	7

2.16-jadval. Yakuniy teskari almashtirish (IP^{-1}).

IP^{-1}							
4	1	3	5	7	2	8	6

Algoritmning yakunlovchi bosqichida 2.16-jadvalga muvofiq teskari joy almashtiriladi. Oddiy tekshiruv yordamida osonlik bilan ishonch hosil qilish mumkinki, yuqorida keltirilgan almashtirishlarning ikkinchisi haqiqatda birinchisiga nisbatan teskari hisoblanadi, ya’ni $IR^{-1}(IR(X)) = X$.

2.17-jadval. Kengaytirib, o’rin almashtirish.

E/P							
4	1	2	3	2	3	4	1

2.18-jadval. P4 o’rin almashtirish.

R4			
2	4	3	1

f shifrlash funksiyasi. 4 bitli o’n qismiy blok va 8 bitli raund kaliti odatdagidek f shifrlash funksiyasining argumentlari hisoblanadi: $f(R, k)$. f shifrlash funksiyasida quyidagi 4 ta kriptografik almashtirish va akslantirishlardan tashkil topgan:

1. E/P – kengaytirib o’rin almashtirish;
2. ikkining moduli bo’yicha qo’shish (chiziqli almashtirish);
3. chiziqsiz almashtirish (S blok);
4. chiziqli almashtirish (P_4 o’rin almashtirish).

Shifrlanishi lozim bo’lgan ochiq matnnig 8 bitli ketma-ketligi bitlari IP almashtirish (2.15-jadval) yordamida o’rin almashadilar. Undan so’ng hosil bo’lgan ushbu ketma-ketlik har bibrining uzunligi 4 bit bo’lgan L_0 va R_0 qismiy bloklarga b’olinadi. R_0 qismiy blok k_1 raund kaliti bilan birgalikda f shifrlash funksiyasiga kiradi (2.6-rasm).

f shifrlash funksiyasi S-DES-1 shifrining eng murakkab tarkibiy qismi hisoblanadi. f shifrlash funksiyasi birinchi raundi kirishiga beriladigan 8 bitli ketma-ketlik (ochiq matnning 8 bitli blokiga IP funksiyani qo’llash natijasi) ning oxirgi 4 biti va birinchi raund kaliti k_1 bo’ladi.

Shifrlash funksiyasining birinchi vazifasi o’n qismiy blok R_0 ni E/P kengaytirib o’rin almashtirish funksiyasi (2.17-jadval) dan foydalanib, 8 bitga kengaytirishdan iborat. Hosil bo’lgan 8 bitli ketma-ketlik birinchi raund kaliti k_1 bilan ikkining moduli bo’yicha qo’shiladi. Ikkinning moduli bo’yicha qo’shish

natijasi ham 8 bitli ketma-ketlik bo'lib, ushbu ketma-ketlik 4 bitdan S_0 va S_1 bloklarga taqsimlanadi. S_0 va S_1 bloklarning har biridan 2 bitli ketma-ketlik chiqadi va ularning konkatenasiyasidan hosil bo'lgan 4 bitli ketma-ketlikka $P4$ o'rin almashtirish (2.18-jadval) qo'llaniladi. $P4$ o'rin almashtirish natijasi $f(R_0, k_1)$ shifrlash funksiyasining qiymati hisoblanadi. Shu bilan $f(R_0, k_1)$ shifrlash funksiyasi o'z ishini yakunlaydi.

Endi L_0 chap qismiy blok $f(R_0, k_1)$ shifrlash funksiyasining qiymati bilan ikkinining moduli bo'yicha qo'shiladi. Qo'shish natijasi ikkinchi raundning o'n qismiy blokiga kirish sifatida uzatiladi: $R_1 = L_0 \oplus f(R_0, k_1)$. Birinchi raunddagi o'n qismiy blok R_0 ning qiymati ikkinchi raundning chap qismiy blokiga kirish sifatida uzatiladi: $L_1 = R_0$.

Ikkinci raunddagi shifrlash jarayoni ham birinchi raunddagidek bo'ladi. R_1 o'n qismiy blok va k_2 raund kaliti ikkinchi raund shifrlash funksiyasining argumentlari hisoblanadi: $f(R_1, k_2) = f(L_0 \oplus f(R_0, k_1), k_2)$. $f(R_1, k_2)$ shifrlash funksiyasining natijasi L_1 chap qismiy blokning qiymati bilan ikkinining moduli bo'yicha qo'shiladi. Ushbu qo'shish natijasiga IP^{-1} yakuniy teskari almashtirish amali qo'llaniladi va uning natijasi shifr matn sifatida qabul qilinadi.

S-DES-1 algoritmi b'oyicha dastlabki matnga o'girishda birinchi raundda k_2 kalit, ikkinichi raundda k_1 kalitdan foydalilanadi.

Kelgusida E/P kengaytirib almashtirish natijalarni quyidagi shaklda aks ettirish qulayroq bo'ladi:

$$\begin{array}{c} n_4 | n_1 \ n_2 | n_3 \\ n_2 | n_3 \ n_4 | n_1. \end{array}$$

Bu qiymatga XOR operasiyasi yordamida 8 bitli $k_1 = (K_{11}, K_{12}, K_{13}, K_{14}, K_{15}, K_{16}, K_{17}, K_{18})$ kalit qo'shiladi:

$$\begin{aligned} & n_4 + K_{11} | n_1 + K_{12} \quad n_2 + K_{13} | n_3 + K_{14} \\ & n_2 + K_{15} | n_3 + K_{16} \quad n_4 + K_{17} | n_1 + K_{18}. \end{aligned}$$

Hosil qilingan 8 bitni qayta belgilaymiz:

$$r_{0,0} | r_{0,1} \ r_{0,2} | r_{0,3}$$

$$r_{1,0} | r_{1,1} \quad r_{1,2} | r_{1,3}.$$

Dastlabki to'rt bit (yuqorida keltirilgan matrisaning birinchi satri) S_0 modulga kirishga tushadi va undan chiqishda 2 bitli ketma-ketlik hosil bo'ladi, qolgan to'rt bit esa (matrisaning ikkinchi satri) S_1 modulga kirishga tushadi va o'z navbatida bu moduldan chiqishida boshqa 2 bitli ketma-ketlik hosil bo'ladi. S_0 va S_1 modullarni 2.19 va 2.20-jadvallarda ko'rsatilgan tarzda aniqlash mumkin.

2.19-jadval. S_0 blok.

S_0	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	1

2.20-jadval. S_1 blok.

S_1	0	1	2	3
0	1	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

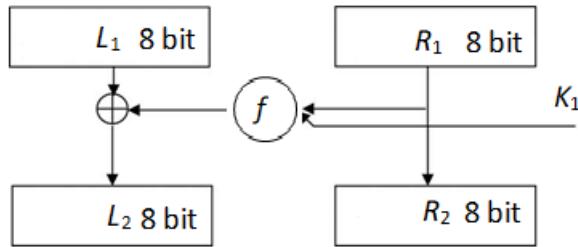
Bu S modullar (kodlash matrisalari) quyidagi tarzda ishlaydi. Kirish ketma-ketligining birinchi va to'rtinchi bitlari satrni belgilab beradigan 2 bitli sonlar sifatida, ikkinchi va uchinchi bitlar esa S matrisa ustunini aniqlab beradi. Mos keluvchi satr va ustun kesishuvida joylashgan elementlar 2 bitli kirish qiymatlarini beradi. Masalan, agar $(r_{0,0} \ p_{0,3})=(00)$ va $(r_{0,1} \ p_{0,2})=(10)$ bo'lsa, chiquvchi ikki bit S_0 matrisaning 0-chi satri va 2-chi ustuni kesishuvida joylashgan qiymat (u 3 yoki 11 ga teng) bilan beriladi. Xuddi shu tarzda $(p_{1,0} \ p_{1,3})$ va $(p_{1,1} \ p_{1,2})$ ikkinchi ikki bitni beradigan qiymat ularning kesishuvida yotadigan S_1 matrisa satr va ustunini aniqlash uchun xizmat qiladi.

Endi S_0 va S_1 modullardan chiqishda olingan 4 bitning o'rirlari 2.18-jadvalga muvofiq o'zgartiriladi.

§2.3. S-DES-2 shifri

S-DES-2 shifri DES shifrlash algoritmining ikkinchi o'quv algoritmi hisoblanadi. S-DES-2 shifrlash algoritmi sxemasi 2.7-rasmida aks ettirilgan [7]. Kiruvchi ochiq matn bloki ikki qismga bo'linadigan 16 bitli ketma-ketlikni ifodalaydi. Ushbu ketma-ketlikning chap tomondan birinchi 8 ta bit L_1 chap, qolgan

8 ta biti R_1 o'n qismiy blokka beriladi. R_1 o'n qismiy blok K_1 raund kaliti bilan birgalikda f shifrlash fuksiyasi orqali o'tadi, shundan so'ng shifrlash fuksiyasining natijasi 2 ning moduli bo'yicha chap tomon bilan qo'shiladi. CHiquvchi shifrlangan xabar ikkita 8 bitli qismdan iborat bo'lib, o'ng tomoni kiruvchi xabarning o'ng qismini, chap tomoni esa 2 ning moduli bo'yicha qo'shish natijasini ifodalaydi.



2.7-rasm. S-DES-2 algoritmining bitta raundi.

2.21-jadval. Kengaytirib, o'rin almashtirish jadvali.

3	4	1	2	6	8	5	7	3	8	2	4
---	---	---	---	---	---	---	---	---	---	---	---

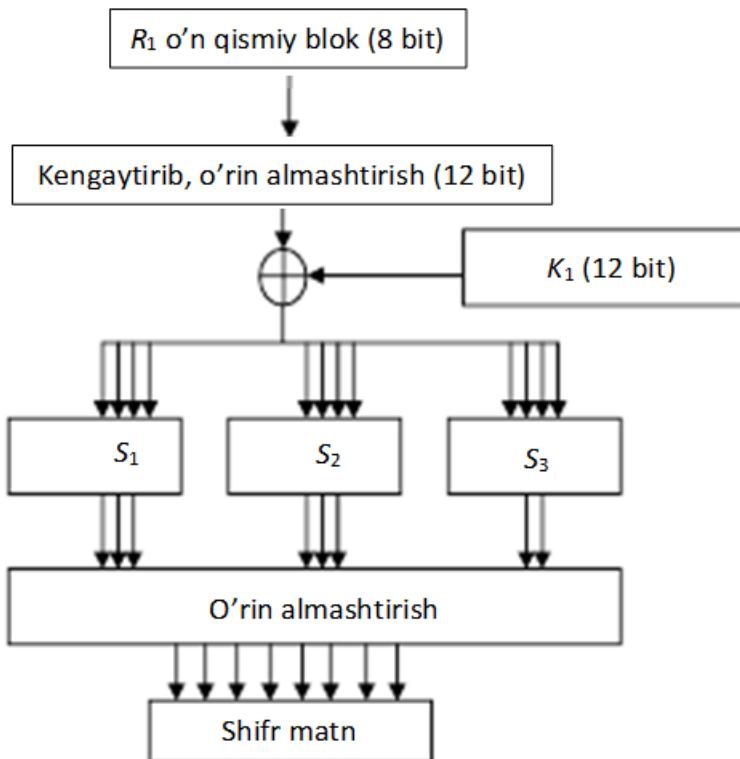
f shifrlash fuksiyasi. Usbu funksiya 2.8-rasmida keltirilgan. Kiruvchi 8 bitli R_1 o'n qismiy blokni kengaytirib, o'rin almashtirish natijasida 12 bitli ketma-ketlik hosil qilinadi. Kengaytirib, o'rin almashtirish jadvali 2.21-jadvalda keltirilgan. Jadvalni chapdan o'ngga qarab o'qish lozim. Ya'ni, uchinchi bit birinchi, to'rtinchi bit ikkinchi, birinchi bit uchinchi pozisiyaga qo'yiladi va h.k. Shundan keyin 12 bitli raund kaliti va kengaytirilgan o'n qismiy blok bilan 2 ning moduli bo'yicha qo'shiladi. Qo'shish natijasi to'rt bitdan uchta blokga taqsimlanib, ularning har biri mos holda S_1 , S_2 va S_3 bloklarga kiradi (2.8-rasm). Dastlabki ikkita S blokdan uch bitdan, uchinchi S blokdan esa ikki bit chiqadi.

2.22-jadval. S₁-blokdagi almashtirishlar jadvali.

a₂a₃a₄	000	001	010	011	100	101	110	111
a₁								
0	4	6	1	3	5	7	2	5
1	5	7	2	4	6	1	3	6

2.23-jadval. S₂-blokdagi almashtirishlar jadvali.

$a_2 a_3 a_4$	000	001	010	011	100	101	110	111
a_1								
0	3	5	7	2	4	6	1	7
1	4	6	1	3	5	7	2	1



2.8-rasm. Shifrlash algoritmining f shifrlash funksiyasi.

2.24-jadval. S₃-blokdagi almashtirishlar jadvali.

$a_2 a_3$	00	01	10	11
$a_1 a_4$				
00	1	3	2	1
01	2	1	3	2
10	3	2	1	3
11	1	3	2	1

2.25-jadval. O'rIN-almashtirish jadvali.

8	7	3	2	5	4	1	6
---	---	---	---	---	---	---	---

Birinchi ikki S blokdagi almashtirishlar 2.22 va 2.23-jadvallarda keltirilganidek quyidagi tamoyil bo'yicha amalga oshiriladi. Blokka to'rtta bit: a_1, a_2, a_3, a_4 kirsin. Bunda birinchi bit satr raqamini (agar $a_1 = 0$ bo'lsa, bu

birinchi satrga, agar $a_1 = 1$ bo'lsa – ikkinchi satrga mos keladi), qolgan uchta $a_2a_3a_4$ bitlar esa ustun raqami (masalan, 000 – birinchi ustun, 111 – sakkizinchı ustunni) ni belgilab beradi.

Uchinchi S blok bilan bog'liq vaziyat biroz boshqacha. Dastlabki ikki blokdan farqli ravishda, undan ikki bit chiqadi. Almashtirish 2.24-jadvalga muvofiq amalga oshiriladi. Bunda agar a_1, a_2, a_3, a_4 – S_3 -blokning kiruvchi bitlari bo'lsa, a_1 va a_4 bitlar satr raqamini, a_2 va a_3 bitlar esa – ustun raqamini (xuddi DES shifrlash algoritmining S bloklari kabi) belgilab beradi. SHundan keyin sakkiz bitli xabar 2.25-jadvalga muvofiq joy almashtirishga uchraydi va chiqishda tayyor shifr matn olinadi.

§2.4. GOST 28147-89 shifri

Shifrnинг xarakteristikalari. GOST 28147-89 shifri quyida keltirilgan kriptografik xarakteristikalarga ega [11]:

Ochiq matn bloki uzunligi – 64 bit;

Raundlar soni – 32 ta;

Dastlabki shifrlash kaliti uzunligi 256 bit;

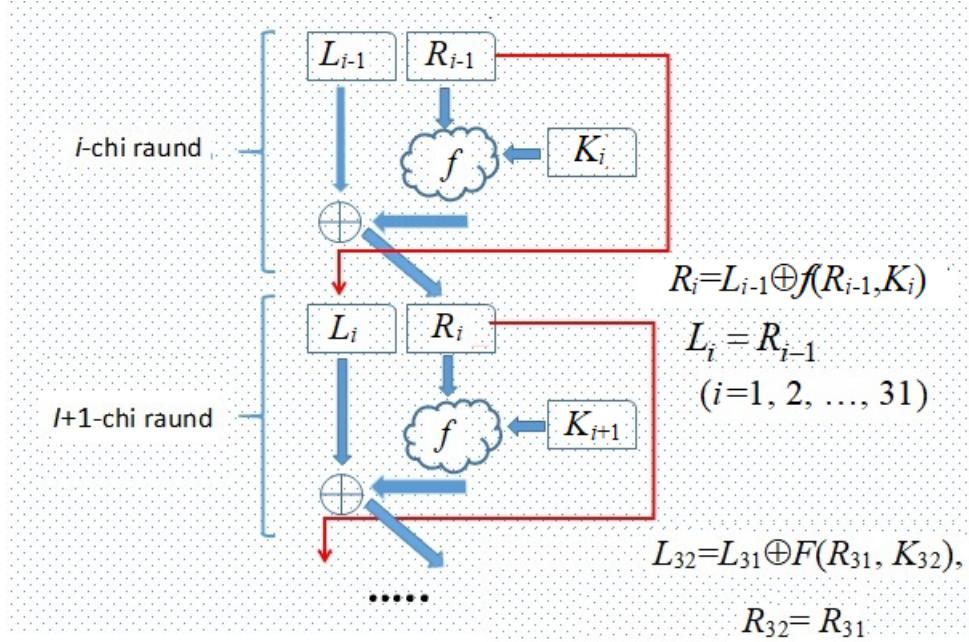
Raund kalitlari uzunligi 32 bit.

Raund kalitlarini hosil qilish. $K=(k_1, k_2, \dots, k_{256})$ shifrlash kaliti 8 ta 32 bitli qismiy kalitlarga quyidagi tartibda bo'linadi:

$$K_1=(k_{32}, k_{31}, \dots, k_1), K_2=(k_{64}, k_{63}, \dots, k_{33}), \dots, K_8=(k_{256}, k_{255}, \dots, k_{225}).$$

Birinchi raundan sakkizinchı raundgacha, to'qqizinchı raundan o'n oltinchi raundgacha hamda o'n yettinchi raundan yigirma to'rtinchi raundgacha K_1, K_2, \dots, K_8 kalitlardan mos holda raund kalitlari sifatida foydalaniladi.

Yigirma beshinchi raundan o'ttiz ikkinchi raundgacha K_8, K_7, \dots, K_1 kalitlardan raund kalitlari sifatida foydalaniladi.



2.9-rasm. GOST 28147-89 shifri bo'yicha shifrlashning umumiy ko'rinishi.

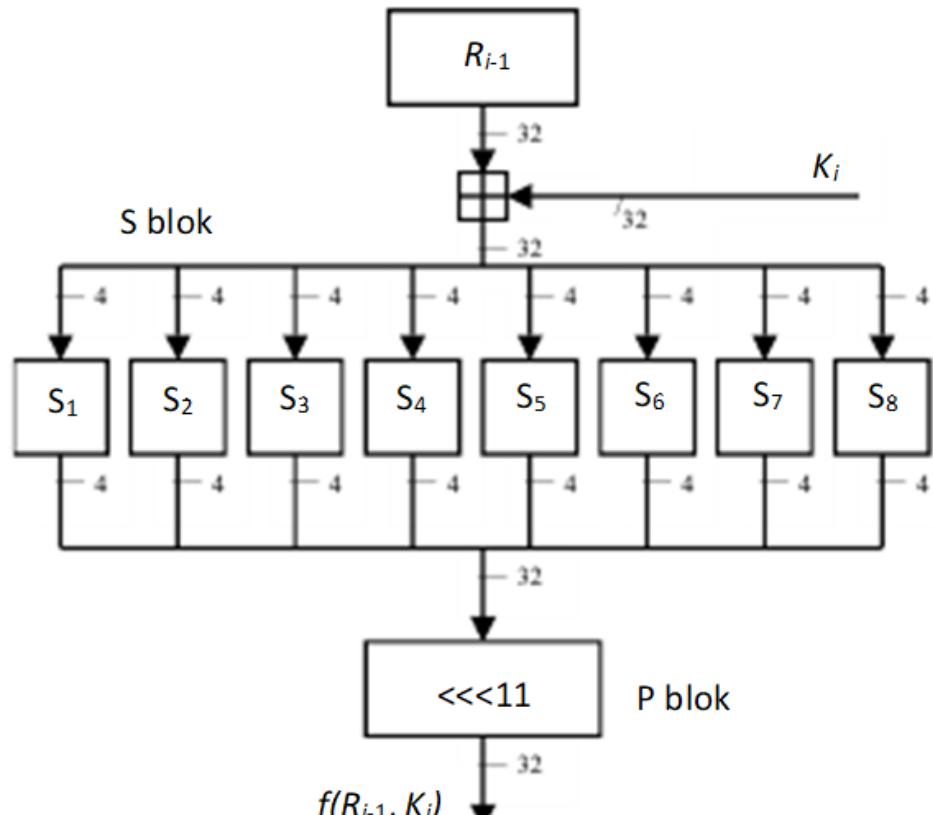
GOST 28147-89 algoritmi bo'yicha shifrlash. Shifrlanishi lozim bo'lgan $M=(m_1, m_2, \dots, m_{64})$ ochiq matn bloki shifrlash jarayonidan oldin $L_0=(m_{64}, m_{63}, \dots, m_{33})$ va $R_0=(m_{32}, m_{31}, \dots, m_1)$ qismiy bloklarga bo'linadi. Asosiy almashtirish va akslantirishlar o'n qismiy blok ustida olib boriladi.

Ushbu algoritm bo'yicha shifrlashning umumiy ko'rinishi 2.9-rasmida keltirigan. Unga ko'ra ixtiyoriy i -chi raundda R_{i-1} o'n qismiy blok k_i raund kaliti bilan f shifrlash funksiyasiga kiradi. Shifrlash funksiyasining natijasi L_{i-1} chap qismiy blok bilan ikkining moduli bo'yicha qo'shiladi va qo'shish natijasi keyingi $i+1$ raund uchun o'n qismiy blok sifatida uzatiladi: $R_i=L_{i-1}\oplus f(R_{i-1}, K_i)$ ($i=1,2,3,\dots,31$). Joriy raunddagи R_{i-1} o'n qismiy blok keyingi $i+1$ raund uchun chap qismiy blok sifatida uzatiladi: $L_i=R_{i-1}$ ($i=1,2,3,\dots,31$). Oxirgi 32-chi raundning chiqish qiymatlari boshqa raundlarga kirish sifatida uzatilmasligi sababli $L_{32}=L_{31}\oplus f(R_{31}, K_{32})$, $R_{32}=R_{31}$ tengliklar bilan ifodalanadi. Natijada $L_{32}=(s_{64}, s_{63}, \dots, s_{33})$ va $R_{32}=(s_{32}, s_{31}, \dots, s_1)$ qismiy bloklar hosil bo'ladi. Shifrmatn esa $C=(c_1, c_2, \dots, c_{64})$ ko'rinishda bo'ladi..

$f(R_{i-1}, K_i)$ shifrlash funksiyasi. Shifrlash funksiyasi yordamida 2.10-rasmida keltirilganidek, quyidagi amallar bajariladi:

- ❖ R_{i-1} o'n qismiy blok bilan K_i raund kaliti 2^{32} ning moduli bo'yicha qo'shiladi;

- ❖ 2^{32} ning moduli bo'yicha qo'shish natijasi S bloklarga kiradi;
- ❖ S bloklardan chiqqan 32 bitli ketma-ketlik 11 bit chapga siklik suriladi (bu surish natijasi $f(R_{i-1}, K_i)$ shifrlash funksiyasining qiymati hisoblanadi).



2.10-rasm. f shifrlash funksiyasi.

$f(R_{i-1}, K_i)$ shifrlash funksiyasida bajariladigan amallarnin e'tiborga olib, GOST 28147-89 algoritmi bo'yicha shifrlashni quyidagicha ifodalash mumkin:

$$(L, R) \rightarrow (R, L \oplus S_{11}(R+K)).$$

Bu yerda va 2.10-rasmda quyida keltirigan belgilashlardan foydalanilgan;

$+$ – 2^{32} ning moduli bo'yicha qo'shish;

S_{11} – S bloklardan chiqqan 32 bitli ketma-ketlik 11 bit chapga siklik surish;

\oplus – 2 ning moduli bo'yicha qo'shish;

$<<<11$ – bitlar ketma-ketligini 11 bit chapga siklik surish (P blok).

S bloklar. GOST 28147-89 shifrida 8 ta S blokdan foydalaniladi. Bu S bloklarning har biriga 4 bitli ketma-ketlik kirib, ularning har bibridan 4 bitli ketma-

ketlik chiqadi (2.10-rasm). Masalan, S₄ blokka 4 bitli 0101 kirsin, ya’ni 5₁₀ (amalda kirish qiymatlaridagi ustun nomerini anglatadi). U holda 2.26-jadvaldan kirish qiymatlaridan S₄ blokka 5₁₀ kirganda 8₁₀, ya’ni 1000 bitli ketma-ketlik chiqishini ko’rish mumkin.

2.26-jadval. S bloklar.

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

Shifrda qo’llaniladigan primitiv amallar.

2³² moduli bo'yicha qo'shish:

$$a+b = a + b, \text{ agar } a + b < 2^{32},$$

$$a+b = a + b - 2^{32}, \text{ agar } a + b \geq 2^{32}.$$

11 bit chapga raundik surish:

$$<<<11 [R(r_{32}, r_{31}, r_{30}, r_{29}, r_{28}, r_{27}, r_{26}, r_{25}, r_{24}, r_{23}, r_{22}, r_{21}, r_{20}, \dots, r_2, r_1)] =$$

$$= (r_{21}, r_{20}, \dots, r_2, r_1, r_{32}, r_{31}, r_{30}, r_{29}, r_{28}, r_{27}, r_{26}, r_{25}, r_{24}, r_{23}, r_{22}).$$

Nazorat savollari

1. DES shifrining asosiy xarakteristikalari nimalardan iborat?
2. DES shifrining birinchi raundi boshlanishidan oldin amalga oshiriladigan almashtirish va akslantirishlarni aytинг.
3. DES shifrining shifplash funksiyasida amalga oshiriladigan akslantirishlarni aytинг.
4. DES shifplash algoritmi raund kalitlari qanday hosil qilinadi?

5. DES shifrida kengaytirib, o’rin almashtirish funksiyasi qanday vazifa bajaradi?

6. DES shifrlash algoritmi S bloklarini tavsiflang.

7. DES shifrlash algoritmi S bloklariga kirgan bitlar ketma-ketligidan qanday tartibda bitlar ketma-ketligi chiqadi?

8. S-DES-1 shifrining asosiy xarakteristikalari nimalardan iborat?

9. S-DES-1 shifrlash algoritmida qanday almashtirish va akslantirishlar ketma-ket bajariladi?

10. S-DES-1 shifrining shifrlash funksiyasida amalga oshiriladigan akslantirishlarni ayting.

11. S-DES-1 shifrlash algoritmi raund kalitlari qanday hosil qilinadi?

12. S-DES-1 shifrida E/P kengaytirib, o’rin almashtirish funksiyasi qanday vazifa bajaradi?

13. S-DES-1 shifrlash algoritmi S bloklarini tavsiflang.

14. S-DES-1 shifrlash algoritmi S bloklariga kirgan bitlar ketma-ketligidan qanday tartibda bitlar ketma-ketligi chiqadi?

15. S-DES-2 shifrining asosiy xarakteristikalari nimalardan iborat?

16. S-DES-2 shifrlash algoritmida qanday almashtirish va akslantirishlar ketma-ket bajariladi?

17. S-DES-2 shifrining shifrlash funksiyasida amalga oshiriladigan akslantirishlarni ayting.

18. S-DES-2 shifrida E/P kengaytirib, o’rin almashtirish funksiyasi qanday vazifa bajaradi?

19. S-DES-2 shifrlash algoritmi S bloklarini tavsiflang.

20. S-DES-2 shifrlash algoritmi S bloklariga kirgan bitlar ketma-ketligidan qanday tartibda bitlar ketma-ketligi chiqadi?

21. GOST 28147-89 shifri qanday kriptografik xarakteristikalarga ega?

22. GOST 28147-89 shifrida raund kalitlari qanday hosil qilinadi?

23. GOST 28147-89 shifrida raund kalitlaridan qanday tartibda foydalaniladi?

24. GOST 28147-89 shifrining shifrlash funksiyasida amallar bajariladi?
25. 2^{32} ning moduli bo'yicha qo'shish amali qanday amalga oshiriladi?
26. GOST 28147-89 shifrlash algoritmi S bloklarini tavsiflang.
27. GOST 28147-89 shifrida qo'llaniladigan primitiv amallarni ayting.

3-BOB. FEYSTE TARMOG'IGA ASOSLANGAN BLOKLI SHIFRLARNING DIFFERENSIAL KRIPTOTAHLLI

Differensial kriptotahllil tushunchasi birinchi marta 1990 yil Eli Bixam va Adi Shamir tomonidan kiritilgan. Ushbu usuldan foydalanib, Bixam va Shamir tanlangan ochiq matndan foydalanib, «to'g'ridan-to'g'ri» hujumdan ko'ra samaraliroq bo'lган, DES algoritmiga hujum usulini taklif qildilar.

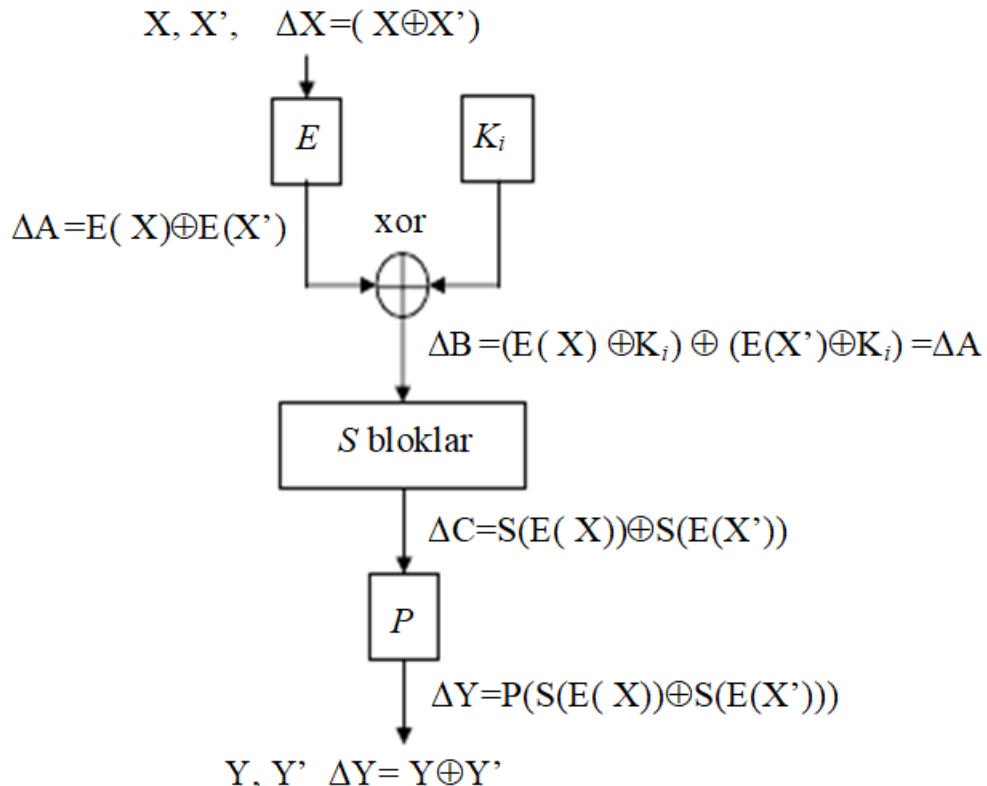
§3.1. Differensial kriptotahllil usulining asosiy g'oyasi

Kriptotahllilning differensial tahlil usulining asosini tanlangan ochiq matn asosidagi hujum tashkil qiladi. Differensial kriptotahllil g'oyasi dastlabki aniq tafovutlarga ega bo'lган ochiq matnlar ikkita juftligining bitta kalit bilan shifrlash raundlari orqali o'tish jarayonida o'zgarishlarining o'xhash emasligini tahlil qilishdan iborat [1,5,11]. Ochiq matnlarni tanlashga hech qanday cheklov yo'q. Ayrim pozisiyalarda tafovut bo'lishi kifoya. O'xhash emaslik o'lchovi sifatida, qoidaga ko'ra, Xemming masofasi foydalaniladi.

Shifr matnlardan hosil bo'lган tafovutlardan kelib chiqib, kalitlarga turli ehtimolliklar beriladi. Haqiqiy kalit shifrmatnlar juftliklarini keyinchalik tahlil qilish jarayonida aniqlanadi – bu ko'plab da'vogar kalitlar orasida ehtimoli eng yuqori bo'lган kalitdir. Differensial kriptotahllilni izohlash uchun DES kriptografik almashtirishining raundlaridan birini ko'rib chiqamiz (3.1-rasm).

O'xhash emasligi ΔX bo'lган X va X' kirish juftliklari berilgan bo'lsin. Mos holda Y va Y' chiqishlar ma'lum, demak, ΔY o'xhash emaslik ham ma'lum. R o'rinn almashtirish va E kengaytirish funksiyasi ma'lum, demak, ΔA va ΔC lar ham ma'lum. 2 ning moduli bo'yicha (xor bo'yicha qo'shish) chiqishdagi qiymatlar noma'lum, biroq ularning o'xhash emasligi ΔV ma'lum va ΔA ga teng. Isbot qilinganki, har qanday berilgan ΔA uchun ΔC ning hamma qiymatlari ham bir xil ehtimollikka ega emas. ΔA va ΔC kombinasiyasi $E(X) \oplus K_i$ va $E(X') \oplus K_i$ lar uchun

bitlar qiymatini taxmin qilishga imkon beradi. $E(X)$ va $E(X')$ larning ma'lum ekanligi bizga kalitlar - K_i haqida axborot beradi.



**3.1-rasm. Ikkita X va X' kiruvchi bloklar uchun
DES almashtirishning bitta raundi.**

DES algoritmining har bir raundida boshlang'ich 56 bitli maxfiy kalitning 48 bitli qismiy kaliti ishtirot etadi. Shunday qilib, oxirgi raunddagi K_{16} kalitni ochib berish 56 bitli maxfiy kalitning 48 bitini tiklashga imkon beradi. Qolgan sakkiz bitni to'liq saralash usuli asosida tiklash mumkin.

Ochiq matnlar turli juftliklarining o'xshash emasliklari ma'lum bir ehtimollik bilan olinadigan shifrmatnlar o'xshash emasligiga olib keladi. Bu ehtimolliklarni har bir almashtirish bloklari uchun jadval tuzib, aniqlash mumkin bo'ladi. Jadvallar quyidagi tamoyil bo'yicha tuziladi: vertikal bo'ylab ΔA ning barcha mumkin bo'lgan kombinasiyalari, gorizontal bo'ylab – barcha ΔC ning mumkin bo'lgan kombinasiyalari, ularning kesishuvida esa – ushbu ΔC ning ushbu ΔA ga mos kelishlar soni joylashadi.

Eng katta mos kelishlar soni ular yordamida maxfiy kalitni aniqlash mumkin bo'lgan ΔA va ΔC lar juftligini beradi. Ushbu ΔA va ΔC larga mos keladigan ochiq matnlar juftligi *to'g'ri juftlik deb*, ΔA va ΔC larga mos kelmaydigan ochiq matnlar juftligi esa *noto'g'ri juftlik deb ataladi*. To'g'ri juftlik raundning to'g'ri kalitini, noto'g'ri juftlik esa – tasodifiy kalitini aniqlash imkonini beradi.

3.1-jadval. DES algoritmi differensial tahlili.

Raundlar soni	Tanlangan ochiq matnlar	Ma'lum ochiq matnlar	Tahlil qilingan ochiq matnlar	Hujumning ish hajmi
8	2^{14}	2^{38}	4	2^9
9	2^{24}	2^{44}	2	2^{32}
10	2^{24}	2^{43}	2^{14}	2^{15}
11	2^{31}	2^{47}	2	32
12	2^{31}	2^{47}	2^{21}	21
13	2^{39}	2^{52}	2	2^{32}
14	2^{39}	2^{51}	2^{29}	2^{29}
15	2^{47}	2^{56}	27	2^{37}
16	2^{47}	2^{55}	2^{36}	2^{37}

To'g'ri kalitni topish uchun etarli miqdordagi taxminlar to'plash zarur. Qismiy kalitlardan biri qolganlaridan ko'ra ko'proq uchraydi. Amalda to'g'ri qismiy kalit barcha tasodifiy qismiy kalitlardan paydo bo'ladi. Ko'rinish turibdiki, maxfiy kalitni muvaffaqiyatli olib berish uchun katta miqdordagi ma'lumotlar kerak bo'ladi.

3.1-jadvalda raundlar miqdori turlicha bo'lgan muvaffaqiyatli DES algoritmi differensial tahlili eng yaxshi natijalarining sharhi keltirilgan. Birinchi ustun raundlar miqdoridan iborat. Keyingi ikki ustun hujumni amalga oshirish uchun zarur bo'lgan tanlangan yoki berilgan (ma'lum) ochiq matnlar sonining quyi bahosidan iborat. To'rtinchi ustun haqiqatda tahlil qilingan ochiq matnlar miqdoridan iborat bo'ladi. Oxirgi ustunda talab qilingan juftlik aniqlangandan so'ng hujumning ish hajmini baholash o'tkaziladi.

§3.2. Differensial kriptotahlilni S-DES-2 shifriga qo'llanishi

Ushbu usul qanday ishlashiga aniq ishonch hosil qilish uchun S-DES-2 shifriga qo'llab ko'ramiz [1]. Ma'lumotlar bilan ishlash qulay bo'lishi uchun almashtirish bloklari chiqishlarining kiruvchi ma'lumotlarga bog'liqligini aks ettiradigan 3.2-jadvalni keltiramiz.

S-bloklarga kirish va chiqish ma'lumotlarining bog'liqli. 2-jadval

Almashtirish blokiga kirish	1-chi blokdan chiqishi	2-chi blokdan chiqishi	3-chi blokdan chiqishi
0000	100	011	01
0001	110	101	10
0010	001	111	11
0011	011	010	01
0100	101	100	10
0101	111	110	11
0110	010	001	01
0111	101	111	10
1000	101	100	11
1001	111	110	01
1010	010	001	10
1011	100	011	11
1100	110	101	01
1101	001	111	10
1110	011	010	11
1111	110	001	01

Tayyorgarlik ishlari bajarilgandan so'ng, ΔA va ΔC bog'liqligi jadvalini tuzish va almashtirish bloklarini tahlil qilishga o'tish mumkin.

Jadval ma'lumotlari quyidagi ravishda tuziladi. Har bir almashtirish blokiga kirishga to'rttadan bit uzatilishi sababli ularning 2 moduli bo'yicha yig'indisi ham to'rt bitdan oshmaydi. Shu bois, ΔA ning qiymatlari 0000 – 1111 oralig'ida yotadi. Biroq, tahlil qilinayotgan matnlar juftligi hech bo'lmasa bir bit bilan farq qilishi lozimligi sababli $\Delta A=0000$ dan foydalanishga hojat yo'q. Shu sababli ΔA ning o'zgarish chegarasi 0001 dan 1111 gacha bo'lgan 15 ta qiymatlardan tashkil topadi. ΔA qiymatlarining har biri almashtirish bloklariga kiruvchi ma'lumotlarning

mumkin bo’lgan o’n oltita kombinasiyasi bilan olinishi mumkin. Masalan, $\Delta A=0001$ quyidagi mumkin bo’lgan kombinasiyalar bilan olinishi mumkin:

- | | |
|---------------|----------------|
| 1. 0000⊕0001; | 9. 1000⊕1001; |
| 2. 0001⊕0000; | 10. 1001⊕1000; |
| 3. 0010⊕0011; | 11. 1010⊕1011; |
| 4. 0011⊕0010; | 12. 1011⊕1010; |
| 5. 0100⊕0101; | 13. 1100⊕1101; |
| 6. 0101⊕0100; | 14. 1101⊕1100; |
| 7. 0110⊕0111; | 15. 1110⊕1111; |
| 8. 0111⊕0110; | 16. 1111⊕1110. |

Bunda almashtirish blokiga kiruvchi ma’lumotlar istalgan juftligining almashtirish blokidan chiquvchi ma’lumotlarining 2 moduli bo’yicha yig’indisi boshqa juftlik almashtirish blokining chiqishlar summasiga doim ham mos kelavermaydi.

Aytilganlarni misol yordamida quyidagicha tushuntirish mumkin. $0011\oplus0010$ kirishlar juftligini ko’rib chiqamiz. 0011 1-blok dan o’tishda 011 ni, 0010 esa 001 beradi. Bu chiqishlarning 2 moduli bo’yicha yig’indisi quyidacha bo’ladi: $\Delta C = 011\oplus001 = 010$.

Endi $0110\oplus0111$ kirishlar juftligini ko’rib chiqamiz. S_1 blok orqali o’tishda 0110 bizga 010 ni, 0111 esa 101 ni beradi. Bu chiqishlarning 2 moduli bo’yicha yig’indisi $\Delta C = 010\oplus101 = 111$. Bu misoldan yaqqol ko’rinib turibdiki, ΔA ning bitta qiyomatiga turlicha ΔC lar mos kelishi mumkin. Almashtirish bloklari tahlili mos hollarda 3.3, 3.4 va 3.5-jadvallarda keltirilgan. 3.3-jadvaldan ko’rinib turibdiki, $\Delta A=0001$ bo’lgan holatda 8 marta $\Delta C = 010$, 2 marta $\Delta C = 101$ va $\Delta C = 110$, 4 marta $\Delta C = 111$ paydo bo’ladi.

3.3-jadval. S₁ blok da ΔC ning ΔA ga bog'liqligi.

ΔC ΔA	000	001	010	011	100	101	110	111
0001	0	0	8	0	0	2	2	4
0010	0	0	2	2	0	6	0	6
0011	4	2	2	0	0	4	0	4
0100	0	6	2	4	0	0	4	0
0101	0	4	0	4	6	0	0	2
0110	0	2	0	2	6	2	4	0
0111	0	2	2	4	4	0	4	0
1000	0	6	0	6	0	0	2	2
1001	0	4	0	4	4	2	2	0
1010	0	2	2	0	8	0	4	0
1011	2	0	0	6	4	0	4	0
1100	6	2	4	0	0	2	0	2
1101	4	0	4	0	0	2	2	4
1110	2	0	4	2	0	0	0	8
1111	4	2	2	0	0	8	0	0

3.4-jadval. S₂ blokda ΔC ning ΔA ga bog'liqligi.

ΔC ΔA	000	001	010	011	100	101	110	111
0001	0	0	8	2	0	2	4	0
0010	0	2	0	0	2	6	2	4
0011	0	2	2	2	2	2	0	6
0100	0	4	2	4	0	2	2	2
0101	4	4	0	6	0	2	0	0
0110	0	0	4	2	6	0	2	2
0111	0	2	0	0	6	2	6	0
1000	0	6	0	4	0	0	4	2
1001	2	2	0	6	2	4	0	0
1010	2	6	2	2	4	0	4	2
1011	2	2	2	0	4	2	4	0
1100	6	0	2	2	2	2	2	0
1101	4	0	6	0	2	0	4	0
1110	0	4	2	0	2	8	0	0
1111	2	0	2	2	0	0	0	10

3.5 -jadval. S₃ blokda ΔC ning ΔA ga bog'liqligi.

ΔC	00	01	10	11
ΔA				
0001	0	4	6	6
0010	0	4	6	6
0011	8	4	2	2
0100	0	4	6	6
0101	8	4	2	2
0110	8	4	2	2
0111	4	0	6	6
1000	0	4	6	6
1001	8	4	2	2
1010	8	4	2	2
1011	4	0	6	6
1100	8	4	2	2
1101	4	0	6	6
1110	4	0	6	6
1111	6	10	0	0

Tahlil o'tkazilgan va jadval tuzilgandan so'ng eng yaxshi ΔA va unga mos keladigan ΔC, ya'ni (ΔA , ΔC) juftlikni aniqlashga kirishish mumkin. 3.4 va 3.5-jadvallardan ko'rinish turibdiki, S₂ blok uchun optimal juftlik (1111,111), S₃ blok uchun esa - (1111,01) hisoblanadi. Shunday qilib, birdan aytish mumkinki, ΔA (E(X)) va E(X1) larning 2 moduli bo'yicha yig'indisi bilan olinadigan ΔA ning oxirgi 8 ta biti uzil-kesil bir qiymatli aniqlandi, ya'ni $\Delta A = xxxx\textcolor{red}{1111}1111$. Demak, unga mos keluvchi ΔC ($\Delta C = xxx\textcolor{red}{111}01$) ning oxirgi besh biti uzil-kesil bir qiymatli aniqlandi.

3.3-jadval bilan vaziyat biroz boshqacha. Unda ehtimoli bir xil bo'lган bir nechta juftlik (ΔA , ΔC) larni ajratish mumkin: (0001,010), (1010,100), (1110,111), (1111,101). Mos ravishda 12 bitli ΔA ning 4 varianti vujudga keladi. Biroq, yana bir muhim jihatni hisobga olish kerak: ΔA joyi o'zgartirilgan va kengaytirilgan kiruvchi bitlarning 2 moduli bo'yicha yig'indisiga teng. Shu sababli, ushbu algoritmda foydalananiladigan kengaytiruvchi o'rinni almashtirish jadvaliga muvofiq, ΔA da mos ravishda quyidagi bit juftliklari teng bo'lishi lozim: 1-chi pozisiyadagi 11-chi pozisiyadagi bilan, 2-chi pozisiyadagi 9-chi pozisiyadagi bilan, 3-chi pozisiyadagi

7-chi pozisiyadagi bilan, 4-chi pozisiyadagi 12-chi pozisiyadagi bilan. Bu shartni yagona $\Delta A = \textcolor{red}{111111111111}$ qiymat qanoatlantiradi, unga $\Delta C = \textcolor{red}{10111101}$ mos keladi. Kelgusi ishlar aynan u bilan amalga oshiriladi. Eng yaxshi 12 bitli ΔA ni aniqlash bo'yicha ma'lumotlar 3.6-jadvalda keltirilgan.

4.6-jadval. Eng yaxshi 12 bitli ΔA ni tanlash.

ΔA	ΔX	ΔS
000111111111	$010\textcolor{blue}{111}01$
101011111111	$100\textcolor{red}{111}01$
111011111111	11111101
111111111111	xxxxxxxx11111111	10111101

Endi, eng yaxshi ΔA ni bilgan holda, kalitni topishga kirishish mumkin. buning uchun bizga $\Delta A = E(X) \oplus E(X_1) = 111111111111$, $\Delta C = S(E(X)) \oplus S(E(X_1)) = 10111101$ bo'lgan bir nechta ochiq matn juftliklari (X, X_1) kerak bo'ladi. Shifrlangan X xabardan $S(E(X))$ ni ajratish uchun shifrlangan xabarning birinchi sakkiz bitiga ochiq matnning birinchi sakkiz bitini qo'shish, so'ngra oxirgi o'rinn almashtirishni hisobga olish kerak. Ishning qulayligi uchun ushbu matnlar va ularga taalluqli ma'lumotlar 3.7-jadvalga kiritilgan. Ularni natijalari quyidagicha:

Birinchi ochiq matnlar (00000000 00000001 , 00000000 11111110) juftligi uchun:

$$Y \oplus X = \textcolor{red}{1101}1000 \oplus 00000000 = \textcolor{red}{1101}1000,$$

$$Y_1 \oplus X_1 = \textcolor{red}{0111}0111 \oplus 00000000 = \textcolor{red}{0111}0111.$$

3-10 jadvaldagi o'rinn almashtirishni teskarisini topish orqali $S(E(X))$ va $S(E(X_1))$ larni aniqlash mumkin. Buning uchun $Y \oplus X$ va $Y_1 \oplus X_1$ yig'indilar natijalarini har birini jadvalga muvofiq 8, 7, 3, 2, 5, 4, 1, 6 pozisiyalar bilan belgilab chiqamiz va bundan foydalanib, ularni har birini ketma-ket 1,2, ..., 8 pozisiyalar bo'yicha qaytadan joylashtiramiz. Natijada $S(E(X))$ va $S(E(X_1))$ ni hosil qilamiz:

$$S(E(X)) = R^{-1}(Y \oplus X) = R^{-1}(\textcolor{red}{1101}1000) = \textcolor{blue}{01001011},$$

$$S(E(X_1)) = R^{-1}(Y_1 \oplus X_1) = R^{-1}(\textcolor{red}{0111}0111) = \textcolor{red}{111101}10.$$

Qolgan juftliklar uchun ham $S(E(X))$ va $S(E(X_1))$ lar shu tarzda aniqlanadi.

3.7-jadval. Eng yaxshi (ΔA , ΔS) larga mos keladigan (X , X_1) ochiq matnlar juftliklari.

Nº	X	E(X)	S(E(X))	Y
1	0000000000000001	000001000100	01001011	1101100000000001
2	0000000000000010	000000010000	01001110	0101100100000010
3	00000000000011010	010000110001	01111011	111111000011010
Nº	X1	E(X1)	S(E(X1))	Y1
1	0000000011111110	111110111011	11110110	0111011111111110
2	0000000011111101	111111011111	11110011	1111011011111101
3	0000000011100101	101111001110	11000110	010100111100101

Keltirilgan ochiq matn juftliklarini ko'rib chiqamiz. Shuni ham hisobga olish zarurki, f shifrlash funksiyasi natijasi boshlang'ich xabarning chap qismiga 2 ning moduli bo'yicha qo'shiladi. Biroq, bizning holatda boshlang'ich xabarlarning chapdagi sakkiz biti nolga teng ekanligi sababli, xulosa chiqarish mumkinki, shifrlangan xabarning chapdagi sakkiz biti f shifrlash funksiyasi chiqishidir. Almashtirish bloklari kirishiga E(X) qiymatlar kelib tushishi sababli barcha X va X1 lar uchun quyidagi ko'rinishga ega bo'lamiz:

S₁ blok uchun:

1. (0000000000001, 0000000011111110) ochiq matnlar juftligi:

Blokka kirishga E(X) $\oplus K_1$ qiymat kelib tushishi sababli quyidagi ko'rinishga ega bo'lamiz:

0000 $\oplus K_1$ blokdan chiqishda 010 ni beradi;

1111 $\oplus K_1$ blokdan chiqishda 111 ni beradi.

3.2-jadvaldan aniqlaymizki, S₁ blok ning chiqishida 010 qiymat uning kirishiga 0110 yoki 1010 qiymatlardan biri berilgan holda, 111 qiymat esa – kiruvchi 1001 yoki 0101 da olinadi. Bundan kelib chiqib, quyidagi mumkin bo'lgan variantlarga ega bo'lamiz:

0000 $\oplus K_1 = 0110$; $K_1 = 0110$;

0000 $\oplus K_1 = 1010$; $K_1 = 1010$;

1111 $\oplus K_1 = 1001$; $K_1 = 0110$;

1111 $\oplus K_1 = 0101$; $K_1 = 1010$.

2. (0000000000000010, 0000000011111101) ochiq matnlar juftligi:

S_1 blok uchun ushbu juftlikni ko'rib chiqish zarurati yo'q, chunki $E(X)$ va $E(X_1)$ ning birinchi to'rt biti xuddi oldingi juftlik bitlari kabi bo'ladi, demak, xuddi shunday natija beradi.

3. (0000000000011010,0000000011100101) ochiq matnlar juftligi:

Xuddi punkt 1 kabi aniqlaymiz:

$0100 \oplus K_1$ blokdan chiqishda 011 beradi;

$1011 \odot K_1$ blokdan chiqishda 110 beradi.

3.2-jadvaldan aniqlaymizki, S_1 blok dan chiqishida 011 qiymat uning kirishiga 0011 yoki 1110 qiymatlardan biri berilgan holda, 110 qiymat esa – kiruvchi 0001 yoki 1100 da olinadi. Bundan kelib chiqib, quyidagi mumkin bo'lган variantlarga ega bo'lamiciz:

$$0100 \oplus K_1 = 0011; \quad K_1 = 0111;$$

$$0100 \oplus K_1 = 1110; \quad K_1 = 1010;$$

$$1011 \oplus K_1 = 0001; \quad K_1 = 1010;$$

$$1011 \oplus K_1 = 1100; \quad K_1 = 0111.$$

Xulosa: hatto ochiq matnlarning ikki juftligini tahlil qilib chiqib ham ko'rishimiz mumkinki, qismiy kalitlardan biri, aynan oladigan bo'lsak $K_1=1010$ boshqalardan ko'proq uchraydi. Shunday qilib, taxmin qilish mumkinki, bu birinchi qismiy kalit hisoblanadi.

S_2 blok uchun:

1. (0000000000000001, 0000000011111110) ochiq matnlar juftligi:

Blokka kirishda $E(X) \oplus K_2$ qiymat kelib tushishi sababli quyidagi ko'rinishga ega bo'lamiciz:

$0100 \oplus K_2$ chiqishda 010 beradi;

$1011 \oplus K_2$ chiqishda 101 beradi;

3.2-jadvaldan aniqlaymizki, S_2 blokdan chiqishida 010 qiymat uning kirishiga 1110 yoki 0011 qiymatlardan biri berilgan holda, 101 qiymat esa – kiruvchi 0001 yoki 1100 da olinadi. Bundan kelib chiqib, quyidagi variantlar bo'lishi mumkin:

$$0100 \oplus K_2 = 1110; \quad K_2 = 1010;$$

$0100 \oplus K_2 = 0011$; $K_2 = 0111$;

$1011 \oplus K_2 = 0001$; $K_2 = 1010$;

$1011 \oplus K_2 = 1100$; $K_2 = 0111$.

2. (000000000000010, 00000001111101) ochiq matnlar juftligi:

$0001 \oplus K_2$ chiqishda 011 beradi;

$1110 \oplus K_2$ chiqishda 100 beradi;

3.2-jadvaldan aniqlaymizki, S_2 blok dan chiqishda 011 qiymat uning kirishiga 0000 yoki 1011 qiymatlardan biri berilgan holda, 100 qiymat esa – kiruvchi 0100 yoki 1000 da olinadi. Bundan kelib chiqib, quyidagi ehtimoliy variantlarga ega bo'lamiz:

$0001 \oplus K_2 = 0000$; $K_2 = 0001$;

$0001 \oplus K_2 = 1011$; $K_2 = 1010$;

$1110 \oplus K_2 = 0100$; $K_2 = 1010$;

$1110 \oplus K_2 = 1000$; $K_2 = 0110$.

3. (0000000000011010, 000000011100101) ochiq matnlar juftligi:

Xuddi punkt 1 kabi aniqlaymiz:

$0011 \oplus K_2$ chiqishda 110 beradi;

$1100 \oplus K_2$ chiqishda 001 beradi.

3.2-jadvaldan aniqlaymizki, S_2 blok dan chiqishda 110 qiymat uning kirishiga 0101 yoki 1001 qiymatlardan biri berilganda, 001 qiymat esa – 0110 yoki 1010 da olinadi. Bundan kelib chiqib, quyidagi variantlar bo'lishi mumkin:

$0011 \oplus K_2 = 0101$; $K_2 = 0110$;

$0011 \oplus K_2 = 1001$; $K_2 = 1010$;

$1100 \oplus K_2 = 0110$; $K_2 = 1010$;

$1100 \oplus K_2 = 1010$; $K_2 = 0110$.

Xulosa: ochiq matnlar uch juftligini tahlil qilib shuni ko'rish mumkinki, qismiykalitlardan biri, aynan $K_2=1010$ boshqalardan ko'proq uchraydi. Shunday qilib, bu ikkinchi qsmiy kalit deb taxmin qilish mumkin.

S₃ blok uchun:

1. (0000000000000001, 000000001111110) ochiq matnlar juftligi:

Blokka kirishda E(X) \oplus K3 qiymat kelib tushishi sababli quyidagi ko'inishga ega bo'lamiz:

0100 \oplus K3 chiqishda 11 beradi;

1011 \oplus K3 chiqishda 10 beradi.

3.2-jadvaldan aniqlaymizki, S₃ blok dan chiqishda 11 qiymat uning kirishiga beshta qiymatdan biri: 0010 yoki 0101 yoki 1000 yoki 1011 yoki 1110 berilganda, 10 qiymat esa - kiruvchi 0000 yoki 0011 yoki 0110 yoki 1001 yoki 1100 da olinadi. Bundan kelib chiqib, quyidagi variantlar bo'lishi mumkin:

0100 \oplus K3=0010; K3 = 0110;

0100 \oplus K3=0101; K3 = 0001;

0100 \oplus K3=1000; K3 =1100;

0100 \oplus K3=1011; K3 = 1111;

0100 \oplus K3=1110; K3 =1010;

1011 \oplus K3=0000; K3 = 1010;

1011 \oplus K3=0011; K3 = 1111;

1011 \oplus K3=0110; K3 =1100;

1011 \oplus K3=1001; K3 =0001;

1011 \oplus K3=1100; K3 = 0110.

2. (0000000000000010, 0000000011111101) ochiq matnlar juftligi:

0000 \oplus K3 chiqishda 10 beradi;

1111 \oplus K3 chiqishda 11 beradi.

3.2-jadvaldan aniqlaymizki, S₃ blok dan chiqishda 10 qiymat uning kirishiga quyidagi beshta qiymatdan biri: 0001 yoki 0100 yoki 0111 yoki 1010 yoki 1101, 11 qiymat esa – kiruvchi 0010 yoki 0101 ili 1000 yoki 1011 yoki 1110 da olinadi. Bundan kelib chiqib, quyidagi quyidagi variantlar bo'lishi mumkin:

0000 \oplus K3=0001; K3 =0001;

0000 \oplus K3 =0100; K3 =0100;

$0000 \oplus K_3 = 0111;$	$K_3 = 0111;$
$0000 \oplus K_3 = 1010;$	$K_3 = 1010;$
$0000 \oplus K_3 = 1101;$	$K_3 = 1101;$
$1111 \oplus K_3 = 0010;$	$K_3 = 1101;$
$1111 \oplus K_3 = 0101;$	$K_3 = 1010;$
$1111 \oplus K_3 = 1000;$	$K_3 = 0111;$
$1111 \oplus K_3 = 1011;$	$K_3 = 0100;$
$1111 \oplus K_3 = 1110;$	$K_3 = 0001.$

3. $(0000000000011010, 00000000011100101)$ ochiq matnlari juftligi:

$0001 \oplus K_3$ chiqishda 11 beradi;

$1110 \oplus K_3$ chiqishda 10 beradi.

3.2-jadvaldan aniqlaymizki, S_3 blok dan chiqishda 11 qiymat uning kirishiga beshta qiymatdan biri: 0010 yoki 0101 yoki 1000 yoki 1011 yoki 1110, 10 qiymat esa – kiruvchi 0001 yoki 0100 yoki 0111 yoki 1010 yoki 1101 da olinadi. Bundan kelib chiqib, quyidagi variantlar bo'lishi mumkin:

$0001 \oplus K_3 = 0010;$	$K_3 = 0011;$
$0001 \oplus K_3 = 0101;$	$K_3 = 0100;$
$0001 \oplus K_3 = 1000;$	$K_3 = 1001;$
$0001 \oplus K_3 = 1011;$	$K_3 = 1010;$
$0001 \oplus K_3 = 1110;$	$K_3 = 1111;$
$1110 \oplus K_3 = 0001;$	$K_3 = 1111;$
$1110 \oplus K_3 = 0100;$	$K_3 = 1010;$
$1110 \oplus K_3 = 0111;$	$K_3 = 1001;$
$1110 \oplus K_3 = 1010;$	$K_3 = 0100;$
$1110 \oplus K_3 = 1101;$	$K_3 = 0011.$

Xulosa: ochiq matnlari uch juftligini tahlil qilib, shuni ko'rish mumkinki, qismiy kalitlardan biri, aynan $K_3 = 1010$ qolganlardan ko'proq uchraydi. Shunday qilib, bu uchinchi qismiy kalit deb taxmin qilish mumkin.

Tahlil natijalarini birlashtirib, izlanayotgan $K = 101010101010$ kalitni olamiz. Eksperimental yo'l bilan ishonch hosil qilish mumkinki, ushbu ochiq matnlar ma'lumotlarini shifrlashda aynan shu kalit foydalanilgan.

§3.3. R-raunddan iborat bo'lgan blokli shifrlar uchun differensial kriptotahlilning umumiyligining sxemasi

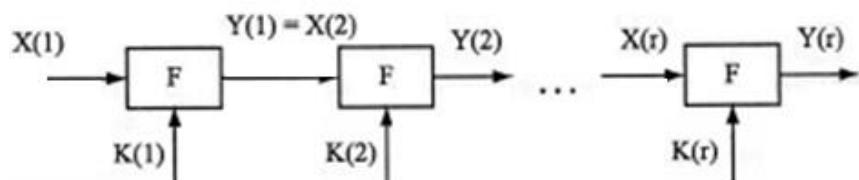
Blok uzunligi N bo'lgan qandaydir blokli shifrator 3.2-rasmida keltirilgan sxema bo'yicha tuzilsin. Bu erda $K = (K(1), K(2), \dots, K(r))$ ma'lum bir sxema bo'yicha K_0 dan olinadi yoki mustaqil va teng ehtimollik bilan har bir raund uchun tanlab olinadi. $X(1)$ va $X'(1)$ – ochiq matnlar juftligi bo'lsin [3]. Quyidagi o'xshashmasliklarni ko'rib chiqamiz:

$$\Delta X(1) = X(1) \oplus X'(1);$$

$$\Delta Y(i) = Y(i) \oplus Y'(i).$$

Differensial kriptotahlil g'oyasi shundan iboratki, shunday $\Delta X(1)$ ni topish kerakki, $X(1), K(1), K(2), \dots, K(r-1)$ larni tasodifiy teng ehtimollik bilan tanlashda $1/(2^N)$ dan katta ehtimollik bilan $\Delta Y(r-1)$ lar paydo bo'lsin.

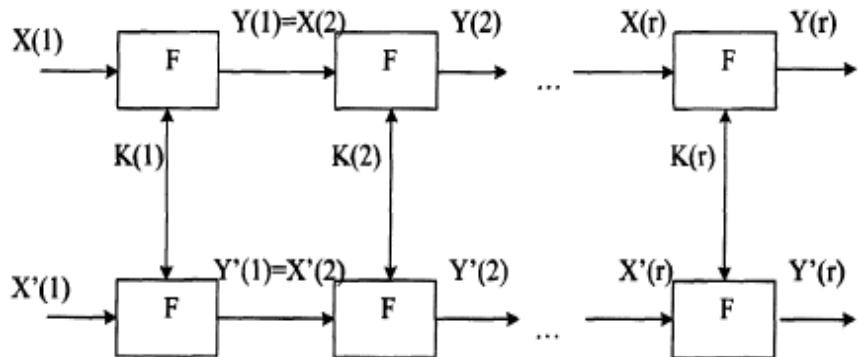
Ta'rif. $(\Delta X(1), \Delta Y(i))$ vektorlarning mumkin bo'lgan qiymatlari juftligi (α, β) ni *i-chi raund differensiali yoki ayirmali xarakteristikasi* yoki oddiy qilib xarakteristikasi deb atash qabul qilingan.



3.2-rasm. Blokli shifrator sxemasi.

Boshqacha aytganda, i -chi raund chiqish differensiali keyingi $i+1$ -chi raund uchun kirish vazifasini o'taydigan kirish-chiqish differensiallari ketma-ketligi *differensial xarakteristika* deyiladi.

U holda differensial tahlil quyidagi 3.3-rasmda keltirilgan modelъ bilan tavsiflanadi.



3.3-rasm. Differential tahlil modeli.

Blokli shifrlarga differensial tahlilni qo'llash uchun quyida keltirigan tamoyil asosida olib boriladi [15]:

1. hujum modeli (criptotahlilchining harakat modeli)ni tanlash, ya'ni r raundli blokli shufr uchun ($\Delta X(1), \Delta Y(r-1)$) juftlikni katta ehtimollik bilan paydo bo'lislini ta'minlaydigan differensial hujumni tanlash;
2. tanlangan model asosida yuqori ehtimolli differensial xarakteristikalarini aniqlash;
3. aniqlangan differensial xarakteristikalar yordamida matnlarning to'g'ri juftliklarini aniqlash;
4. yig'ilgan matnlarning to'g'ri juftliklarini tahlil qilish va bo'lishi mumkin bo'lgan kalitlarni statistikasini olib borish.

n raundli shifr uchun $n - 1$ raundgacha qurilgan differensial xarakteristika differensial kriptotahlilni o'tkazish va shifrlash kaliti bitlarini aniqlash imkonini beradi. Shifrning $n - 1$ raundgacha qurilgan differensial xarakteristikasining ehtimolligi p bo'lsa, u holda differensial kriptotahlilni o'tkazish uchun

$$O\left(\frac{1}{p}\right)$$

tartibidagi ochiq matn-shifr matnlari juftligi kerak bo'ladi.

Oxirgi shifrlash raundining qismiy kalitini quyidagi algoritmdan foydalanib topish mumkin:

1. ($r-1$)-raund uchun (α, β) differensialni shunday tanlaymizki, ularni ehtimoli $R(\Delta X(1)) = \alpha$, $\Delta Y(r-1) = \beta$ katta bo'lsin.
2. Tasodifiy ravishda $X(1)$ tanlaymiz va $X'(1)$ shunday tanlaymizki, $\Delta X(1) = \alpha$ bo'lsin. $Y(r)$ va $Y'(r)$ lar ma'lum bo'lsin.
3. $\Delta Y(r-1) = \beta$ deb faraz qilamiz va $Y(r)$ va $Y'(r)$ ni bilgan holda $K(r)$ ni topamiz.
4. 2 va 3 bandlarni to qismiy kalitlardan biri boshqa qismiy kalitlardan ko'proq uchray boshlamagunga qadar takrorlaymiz.

Yuqorida keltirilgan algoritm bir qarashda sodda bo'lib ko'rinishiga qaramay, bir qator sezilarli muammolar mavjud. Birinchidan, etarli hajmda ma'lumotlar to'planmagunga qadar to'g'ri qismiy kalitni ajratishning imkoniy yo'q. DES ga hujum qilishda bo'lishi mumkin bo'lgan 2^{48} barcha kalitlar ehtimolini saqlash uchun hisoblagichlardan foydalanish zarur, buning ustiga, ochish uchun ham juda ko'plab ma'lumotlar talab qilinadi.

§3.4. DES shifrlash algoritmining bitta raundi differensial kriptotahlili

Bundan oldingi mavzularda differensial kriptotahlilning g'oyasi 2 ta xabarning tafovuti (differensiali yoki ayirmasi) ni shifrlash raundlaridan o'tishini kuzatishdan iborat ekanligi ta'kidlangan edi. Shifrlanadigan axborot ikkilik sanoq tizimida bo'lganligi sababli bu erda xabarlearning tafovuti deyilganda ularning 2 ning moduli bo'yicha yig'indisi (XOR amali) nazarda tutiladi.

Ishni o'rniga qo'yish jadvali, ya'ni S bloklarni tahlil qilish hamda kirish va chiqish ayirmalari (ΔA va ΔC) ni bog'liqlik jadvalini qurishdan boshlash lozim. DES shifridagi S bloklarga har bir 64 ta kirishning mos chiqish qiymatlari mavjud.

3.8-jadval. DES shifri S bloklari uchun kirish va chiqishlarning mosligi.

S blokka kirish	S ₁ blok dan chiqish	S ₂ blok dan chiqish	S ₃ blok dan chiqish	S ₄ blok dan chiqish	S ₅ blok dan chiqish	S ₆ blok dan chiqish	S ₇ blok dan chiqish	S ₈ blok dan chiqish
	2 lik							
10 lik	t i z i m	t i z i m	10 lik	t i z i m	10 lik	t i z i m	10 lik	t i z i m
0	000000	1110	14	1111	15	1010	10	0111
1	000001	0000	0	0011	3	1101	13	1101
2	000010	0011	3	0001	1	0000	0	1101
3	000011	1111	15	1101	13	0111	7	1000
4	000100	1101	13	1000	8	1001	9	1101
5	000101	0111	7	0100	4	0000	0	1101
6	000110	0001	1	1110	14	1110	14	0100
7	000111	0100	4	0111	7	1001	9	1111
8	001000	0010	2	0110	6	0110	6	0000
9	001001	1110	14	1111	15	0011	3	0110
10	001010	1111	15	1011	11	0011	3	0110
11	001011	0010	2	0010	2	0100	4	1111
12	001100	1011	11	0011	3	1111	15	0000
13	001101	1101	13	1000	8	0110	6	1111
14	001110	1000	8	0100	4	0101	5	1101
15	001111	0001	1	1110	14	1010	10	0110
16	010000	0011	3	1001	9	0001	1	0100
17	010001	1010	10	1100	12	0010	2	1110
18	010010	1010	10	0111	7	1101	13	0100
19	010011	0110	6	0000	0	1000	8	0001
20	010100	0110	6	0010	2	1100	12	0011
21	010101	1100	12	0001	1	0101	5	0110
22	010110	1100	12	1101	13	0111	7	1110
23	010111	1011	11	1010	10	1110	14	1100

3.8-jadval (davomi). DES shifri S bloklari uchun kirish va chiqishlarning mosligi.

24	011000	0101	5	1100	12	1011	11	1011	11	1101	13	1110	14	0101	5	0101	5
25	011001	1001	9	0110	6	1100	12	0001	1	0011	3	0000	0	0010	2	0000	0
26	011010	1001	9	0000	0	0100	4	1100	12	0000	0	0111	7	1010	10	0000	0
27	011011	0101	5	1001	9	1011	11	1010	10	1001	9	1011	11	1111	15	1110	14
28	011100	0000	0	0101	5	0010	2	0100	4	1110	14	0101	5	0110	6	1100	12
29	011101	0011	3	1011	11	1111	15	1110	14	1000	8	0011	3	1000	8	1001	9
30	011110	0111	7	1010	10	1000	8	1111	15	1001	9	1011	11	0001	1	0111	7
31	011111	1000	8	0101	5	0001	1	1001	9	0110	6	1000	8	0110	6	0010	2
32	100000	0100	4	0000	0	1101	13	1010	10	0100	4	1001	9	0001	1	0111	7
33	100001	1111	15	1101	13	0001	1	0011	3	1011	11	0100	4	0110	6	0010	2
34	100010	0001	1	1110	14	0110	6	0110	6	0010	2	1110	14	0100	4	1011	11
35	100011	1100	12	1000	8	1010	10	1111	15	1000	8	0011	3	1011	11	0001	1
36	100100	1110	14	0111	7	0100	4	1001	9	0001	1	1111	15	1011	11	0100	4
37	100101	1000	8	1010	10	1101	13	0000	0	1100	12	0010	2	1101	13	1110	14
38	100110	1000	8	1011	11	1001	9	0000	0	1011	11	0101	5	1101	13	0001	1
39	100111	0010	2	0001	1	0000	0	0110	6	0111	7	1100	12	1000	8	0111	7
40	101000	1101	13	1010	10	1000	8	1100	12	1010	10	0010	2	1100	12	1001	9
41	101001	0100	4	0011	3	0110	6	1010	10	0001	1	1001	9	0001	1	0100	4
42	101010	0110	6	0100	4	1111	15	1011	11	1101	13	1000	8	0011	3	1100	12
43	101011	1001	9	1111	15	1001	9	0001	1	1110	14	0101	5	0100	4	1010	10
44	101100	0010	2	1101	13	0011	3	0111	7	0111	7	1100	12	0111	7	1110	14
45	101101	0001	1	0100	4	1000	8	1101	13	0010	2	1111	15	1010	10	1000	8
46	101110	1011	11	0001	1	0000	0	1101	13	1000	8	0011	3	1110	14	0010	2
47	101111	0111	7	0010	2	0111	7	1000	8	1101	13	1010	10	0111	7	1101	13
48	110000	1111	15	0101	5	1011	11	1111	15	1111	15	0111	7	1010	10	0000	0
49	110001	0101	5	1011	11	0100	4	1001	9	0110	6	1011	11	1001	9	1111	15
50	110010	1100	12	1000	8	0001	1	0001	1	1001	9	0000	0	1111	15	0110	6
51	110011	1011	11	0110	6	1111	15	0100	4	1111	15	1110	14	0101	5	1100	12
52	110100	1001	9	1100	12	0010	2	0011	5	1100	12	0100	4	0110	6	1010	10
53	110101	0011	3	0111	7	1110	14	0101	5	0000	0	0001	1	0000	0	1001	9
54	110110	0111	7	0110	6	1100	12	1110	14	0101	5	1010	10	1000	8	1101	13
55	110111	1110	14	1100	12	0011	3	1011	11	1001	9	0111	7	1111	15	0000	0
56	111000	0011	3	1001	9	0101	5	0101	5	0110	6	0001	1	0000	0	1111	15
57	111001	1010	10	0000	0	1011	11	1100	12	1010	10	0110	6	1110	14	0011	3
58	111010	1010	10	0011	3	1010	10	0010	2	0011	3	1101	13	0101	5	0011	3
59	111011	0000	0	0101	5	0101	5	0111	7	0100	4	0000	0	0010	2	0101	5
60	111100	0101	5	0010	2	1110	14	1000	8	0000	0	1011	11	1001	9	0101	5
61	111101	0110	6	1110	14	0010	2	0010	2	0101	5	1000	8	0011	3	0110	6
62	111110	0000	0	1111	15	0111	7	0100	4	1110	14	0110	6	0010	2	1000	8
63	111111	1101	13	1001	9	1100	12	1110	14	0011	3	1101	13	1100	12	1011	11

3.9-jadval. Differensial tahlilni qo'llash uchun DES shifri S₁ blokining tahlili.

ΔA	ΔC	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111	1111
0000001	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4	4	
0000010	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2	2	
0000011	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0	0	
0001000	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2	2	
0001001	4	8	6	2	2	4	4	2	0	4	4	0	12	2	4	6	6	
0001010	0	4	2	4	8	2	6	2	8	4	4	2	4	2	0	12	12	
0001011	2	4	10	4	0	4	8	4	2	4	8	2	2	2	4	4	4	
0010000	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4	4	
0010001	10	2	4	0	2	4	6	0	2	2	8	0	10	0	2	12	12	
0010100	0	8	6	2	2	8	6	0	6	4	6	0	4	0	2	10	10	
0010101	2	4	0	10	2	2	4	0	2	6	2	6	6	4	2	12	12	
0011000	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2	2	
0011001	6	6	4	8	4	8	2	6	0	6	4	6	0	2	0	2	2	
0011100	0	4	8	8	6	6	4	0	6	6	4	0	0	4	0	8	8	
0011101	2	0	2	4	4	6	4	2	4	8	2	2	2	6	8	8	8	
0100000	0	0	0	0	0	0	2	14	0	6	6	12	4	6	8	6	6	
0100001	6	8	2	4	6	4	8	6	4	0	6	6	0	4	0	0	0	
0100010	0	8	4	2	6	6	4	6	6	4	2	6	6	0	4	0	0	
0100011	2	4	4	6	2	0	4	6	2	0	6	8	4	6	4	6	6	
0101000	0	8	8	0	10	0	4	2	8	2	2	4	4	8	4	0	0	
0101001	0	4	6	4	2	2	4	10	6	2	0	10	0	4	6	4	4	
0101100	0	8	10	8	0	2	2	6	10	2	0	2	0	6	2	6	6	
0101101	4	4	6	0	10	6	0	2	4	4	4	6	6	6	2	0	0	
0110000	0	6	6	0	8	4	2	2	2	4	6	8	6	6	2	2	2	
0110001	2	6	2	4	0	8	4	6	10	4	0	4	2	8	4	0	0	
0110010	0	6	4	0	4	6	6	6	2	2	0	4	4	6	8	8	8	
0110011	4	4	2	4	10	6	6	4	6	2	2	4	2	2	4	2	2	
0111000	0	10	10	6	6	0	0	12	6	4	0	0	2	4	4	0	0	
0111001	4	2	4	0	8	0	0	2	10	0	2	6	6	6	14	0	0	
0111010	0	2	6	0	14	2	0	0	6	4	10	8	2	2	6	2	2	
0111111	2	4	10	6	2	2	2	8	6	8	0	0	0	4	6	4	4	
1000000	0	0	0	10	0	12	8	2	0	6	4	4	4	2	0	12	12	
1000001	0	4	2	4	4	8	10	0	4	4	10	0	4	0	2	8	8	
1000010	10	4	6	2	2	8	2	2	2	6	0	4	0	4	0	4	10	

$\Delta A=000001$ qiymat turli usullar bilan olinishi mumkin:

$\Delta A=000001=000111 \oplus 000110$, $\Delta A=000001=000001 \oplus 000000$ va h.k. Agar S₁ blokni qaraydigan bo'lsak, 3.8-jadvaldan ko'rish mumkinki, 000111 kirishga 0100,

000110 kirishga 0001 chiqish mos keladi. U holda $\Delta A=000001$ qiymatiga $\Delta C=0100\oplus0001=0101$ chiqish ayirmasi mos keladi. Xuddi shuningdek, 000001 kirishga 0000, 000000 kirishga 1110 chiqish mos keladi va bu holda chiqish ayirmasi $\Delta C=0000\oplus1110=1110$ ga teng bo'ladi. Shunday tarzda S_1 blokga kirish va chiqishlarni tahlil qilib, ($\Delta A, \Delta C$) ning to'gri juftliklarini va ularning ehtimolliklarini aniqlash mumkin bo'ladi (3.9-jadval, qulaylik uchun ushbu jadvalning bir qismi keltirigan, bunday jadvallar qolgan S bloklarning har biri uchun mavjud). Ehtimollikning qiymati esa ΔC berilgan qiymatining mos kelishlar sonini qiymatlarning umumiy soniga bo'lishdan hosil qilinadi.

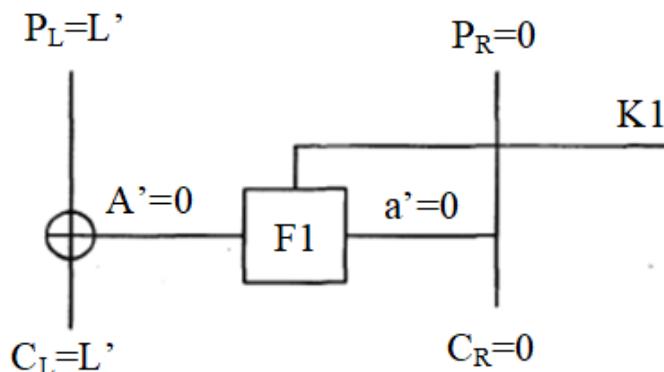
3.9-jadvalni tahlil qilib, quyidagi qonuniyatlarni ko'rish mumkin:

- ❖ har bir satrni yig'indisi, ya'ni ΔA ning bitta qiymatiga mos keluvchi ΔC ning turli qiymatlarining miqdori 64 ga teng;
- ❖ DES shifri uchun $1/4$ dan yuqori ehyimollikka ega bo'lган ($\Delta A, \Delta C$) mavjud emas;
- ❖ ΔA ning aynan bitta qiymatiga ΔC ning bitta qiymatini mos kelishlari soni doimo juft bo'ladi. Bu esa ΔA ning aynan bitta qiymati ikki xil usul bilan hosil qilinishi bilan bog'liq: $\Delta A=X\oplus X'=X'\oplus X$.

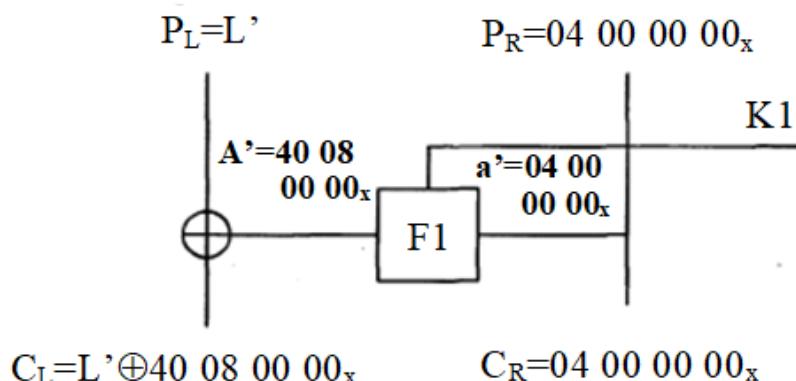
Jadvallarni asosiy xususiyatlari aniqlandi, endi differensil tahlilga o'tish mumkin. Birinchi navbatda shuni qayd etish lozimki, differensial kriptotahlilni o'rghanishda blokli shifrlash algoritmlariga xos bo'lган (shu jumladan, DES shifrlash algoritmiga ham) boshlang'ich va yakuniy almashtirishlarni hisobga olmaslik mumkin. Ya'ni, bu holatni ushbu almashtirishlar shifrlash algoritmining kriptobardoshligiga ta'sir qilmasligi bilan izohlash mumkin. 3.4-rasmida bir raundli shifrlash ko'rsatilgan. Bunda o'n qismiy blokni ayirmasi $P_R=0$. Ushbu holda f shifrlash funksiyaidan bir ehtimollik bilan 0 chiqadi.

$(\Delta A, \Delta C)$ nig to'gri juftliklarini tanlash lozim. DES shifri uchun bunday juftliklar bir nechta va ularning ehtimolliklari $0,25$ ga teng. S_2 blokni tahlil qilishdan hosil qilingan, ulardan bittasi – $(001000, 1010)_2=((8,10)_{10}$ (3.10-jadval). Agar biz

usbu xarakteristikadan S_2 blok uchun, qolgan bloklar uchun nol xarakteristikadan foydalansak, natijada 3.5-rasmida ko'rsatilgan ayirmaga ega bo'lish mumkin.



3.4-rasm. Bir raundli xarakteristika.



3.5-rasm. Kirish ayirmasi nol bo'limgan bir raundli akslantirishga misol.

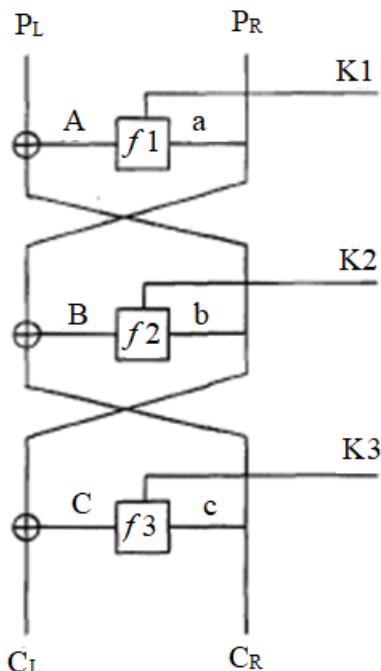
DES shifrlash algoritmining bitta raundi misolida qanday mexanizmlar hisobiga differensial kriptotahlil usulini qo'llash mumkinligini ko'rib chiqamiz. Buning uchun DES shifrlash algoritmi kriptografik almashtirishlarining bitta raundini ko'rib chiqamiz. Shifrlash algoritmining bitta raundi xarakteristikasini bilan holda algoritmning bir necha raundi uchun differensial xarakteristikani qurish mumkinligi E.Bixam va A.Shamirlar tomonidan ko'rsatilgan. Ular "oddiylikdan-murakkablikka" tamoyili asosida ish ko'rdilar, ya'ni differensial kriptotahlilni bir raundli shifrlashdan boshladilar. Keyingi qadam nisbatan murakkabroq masalani, ya'ni bir raunddan ortiq, masalan uch randli algoritmni tahlil qilish bo'ladi.

3.10-jadval. Differensial tahlilni qo'llash uchun DES shifri S₂ blokining tahlili.

ΔC ΔA	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000001	9	3	6	4	0	2	6	4	1	14	8	6	5	6	6	2
000010	0	3	6	2	0	4	6	4	1	0	4	6	10	10	12	0
000011	4	9	4	8	4	6	4	2	4	2	2	4	6	2	0	4
000100	0	3	6	0	0	6	0	14	1	6	10	4	10	5	4	4
000101	2	0	4	8	2	4	6	6	2	0	8	4	2	4	10	2
000110	0	12	6	4	6	4	6	2	2	10	2	8	2	0	0	0
000111	4	6	6	4	2	4	4	2	6	4	2	4	4	6	0	6
001000	0	0	0	4	0	4	0	8	0	10	16	6	6	0	6	4
001001	14	2	4	10	2	8	2	6	2	4	0	0	2	2	2	4
001010	0	6	6	2	10	4	10	2	6	2	2	4	2	2	4	2
001011	6	2	2	0	2	4	6	2	10	2	0	6	6	4	4	8
001100	0	0	0	4	0	14	0	10	0	6	2	4	4	8	6	6
001101	6	2	6	2	10	2	0	4	0	10	4	2	8	2	2	4
001110	0	6	12	8	0	4	2	0	8	2	4	4	6	2	0	6
001111	0	8	2	0	6	6	8	2	4	4	4	6	8	0	4	2
010000	0	0	0	8	0	4	10	2	0	2	8	10	0	10	6	4
010001	6	6	4	6	4	0	6	4	8	2	10	2	2	4	0	0
010010	0	6	2	6	2	4	12	4	6	4	0	4	4	6	2	2
010011	4	0	4	0	8	6	6	0	0	2	0	6	4	8	2	14
010100	0	6	6	4	10	1	2	12	6	2	2	2	4	4	2	2
010101	6	8	2	0	8	2	0	2	2	2	2	2	2	14	10	2
010110	0	8	6	4	2	2	4	2	6	4	6	2	6	0	6	6
010111	6	4	8	6	4	4	0	4	6	2	4	4	4	2	4	2
011000	0	6	4	6	10	4	0	2	4	8	0	0	4	8	2	6
011001	2	4	6	4	4	2	4	2	6	4	6	8	0	6	4	2
011010	0	6	8	4	2	4	2	2	8	2	2	6	2	4	4	8
011011	0	6	4	4	0	12	6	4	2	2	2	4	4	2	10	2
011100	0	4	6	6	12	0	4	0	10	2	6	2	0	0	10	2
011101	0	6	2	2	6	0	4	16	4	4	2	0	0	4	6	8
011110	0	4	8	2	10	6	6	0	8	4	0	2	4	4	0	6
011111	4	2	6	6	2	2	2	4	8	6	10	6	4	0	0	2
100000	0	0	0	2	0	12	10	4	0	0	0	2	14	2	8	10
100001	0	4	6	8	2	10	4	2	2	6	4	2	6	2	0	6
100010	4	12	8	4	2	2	0	0	2	8	8	6	0	6	0	2
100011	8	2	0	2	8	4	2	6	4	8	2	2	6	4	2	4
100100	10	4	0	0	0	4	0	2	6	8	6	10	8	0	2	4
100101	6	0	12	2	8	6	10	0	0	8	2	6	0	0	2	2
100110	2	2	4	4	2	2	10	14	2	0	4	2	2	4	6	4
100111	6	0	0	2	6	4	2	4	4	4	8	4	8	0	6	6
101000	8	0	8	2	4	12	2	0	2	6	2	0	6	2	0	10
101001	0	2	4	10	2	8	6	4	0	10	0	2	10	0	2	4
101010	4	0	4	8	6	2	4	4	6	6	2	6	2	2	4	4
101011	2	2	6	4	0	2	2	6	2	8	8	4	4	4	8	2
101100	10	6	8	6	0	6	4	4	4	2	4	4	0	0	2	4

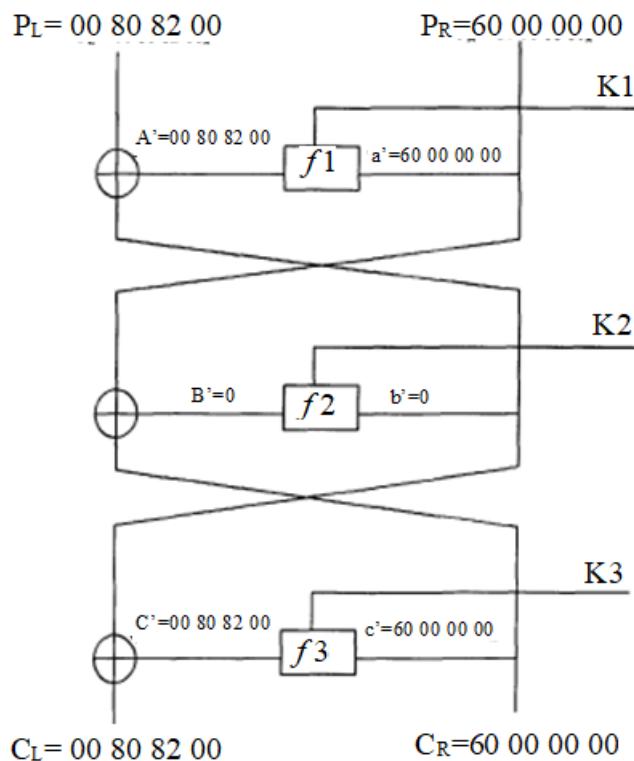
§3.5. DES shifrlash algoritmining uchta raundi differensial kriptotahlili

3.6-rasmda uchta raundli DES shifrlash algoritmining umumiy sxemasi keltirilgan. Ushbu rasmdan ko'rinib turibdiki, ochiq matnlarning ($P_L=b$, $P_R=a$) ayirmasi birinchi raund kirishiga kelib tushmoqda.



3.6-rasm. DES shifrlash algoritmining uchta raundi.

Faraz qilaylik, ochiq matnlar kiruvchi ayirmasining o'ng qismi $P_R=0$ ($a=0$). U holda birinchi raund shifrlash funksiyasi f_1 dan chiqish ayirmasining qiymati ham nol ($A=0$) bo'ladi. Bu vaziyatda dastlabki ayirma (b,a) ayirmaning chap qismi $P_L=b$ ikkinchi raundning o'ng qismi kirishiga kelib tushadi. U holda uchinchi raund chiqishiing chap qismi C_L ikkinchi raundga kiruvchi o'ng ayirma $P_L=b$ bilan uchinchi raund shifrlash funksiyasi f_3 dan chiqish ayirmasi C ning ikki modul bo'yicha yig'indisiga teng bo'ladi: $C_L = P_L \oplus S = b \oplus S$. Ushbu tenglikdan P_L va S_L ayirmalarning qiymati ma'lumligidan S ayirmaning ham qiymatini topish mumkin. Natijada shifrlashning uchinchi raund qismiy kaliti bitlarini osongina topish mumkin.



3.7-rasm. DES shifrinining uch raundli xarakteristikasi.

3.11-jadval. PR ni kengaytiruvchi E-funksiya.

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

3.12-jadval. S-bloklardan chiqqan bitlar ketma-ketligini almashtirish (P).

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

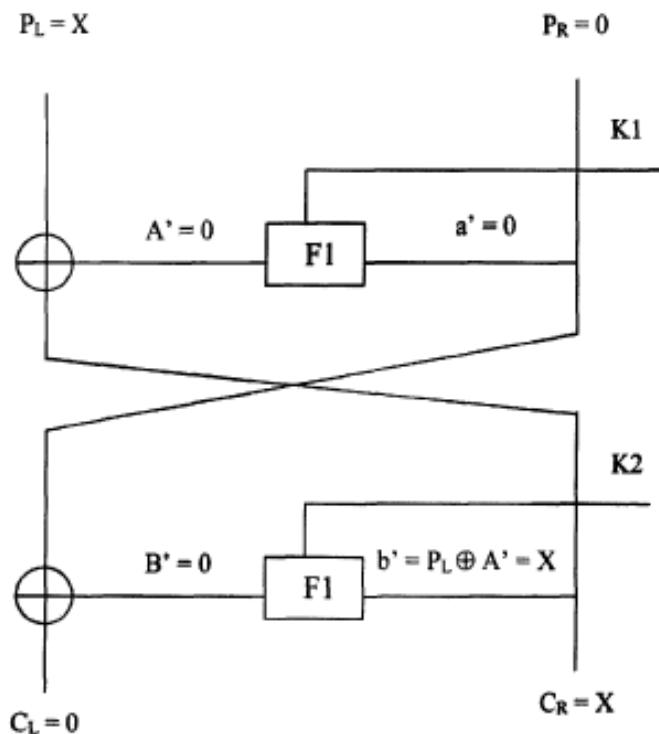
Uch raundli shifrlash algoritmini tahlil qilishning 3.7-rasmida keltirilgan yana bitta usuli mayjud. Birinchi raundga kiruvchi (P_L, P_R) ayirmaning qiymatini shunday tanlash kerakki, birinchi raund shifrlash funksiyasi f_1 dan chiqish ayirmasining qiymati kiruvchi ayirmaning chap qismi P_L bilan bir xil bo'lsin. Bu holda ikkinchi raundning o'ng qismi kirishiga qiymati nol bo'lган ayirma kelib tushadi. Buning natijasida ikkinchi raund shifrlash funksiyasi f_2 dan chiqish ayirmasining qiymati har doim nol bo'ladi. Shunday qilib, uchinchi raundning o'ng qismi kirishiga birinchi raunddagi o'ng qismiy blok kelib tushadi. Bu holda ochiq matn-shifr matn juftligini to'g'ri tanlash kalit bitlarini to'g'ri topishni ta'minlaydi. E. Bixam va A. Shamir $P_R=60\ 00\ 00\ 00_{16}=0110\ 000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$ qiymatdan foydalananishni tavsiya etdilar. Ushbu ayirma 3.11-jadvalga asosan kengaytirib o'rinni almashtirishdan keyin $E(P_R)=001100\ 000000\ 000000\ 000000\ 000000\ 000000\ 000000\ 000000$ ko'rinishdagi ayirma ko'rinishiga ga ega bo'ladi.

S_1 blokka $\Delta A=001100$ noldan farqli ayirma kiradi, 3.9-jadvalga asosan $p=14/64$ ehtimollik bilan S_1 blokdan $\Delta C=1110$ ayirma chiqadi. Qolgan barcha S bloklarga nol qiymatli ayirmalar kirib, ushbu bloklardan nol qiymatli ayirmalar chiqadi.

S bloklardan chiqqan $1110\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000$ bitlar ketma-ketligi 3.12-jadvalga asosan P o'rinni almashtirishga uchraydi (shu bilan f_1 shifrlash funksiyasi o'z ishini tugatadi). f_1 shifrlash funksiyasini natijasi esa $P(S)=C_L=0000\ 0000\ 1000\ 0000\ 1000\ 0010\ 0000\ 0000=00\ 80\ 82\ 00_{16}$.

Ko'rini turibdiki, Bixam va Shamir maksimal ehtimollikka ega bo'lмаган juftlikdan foydalaishni taklif qilishgan. Bu esa to'g'ri juftlikni aniqlashda tahlilda qancha S blok qatnashganligini ham hisobga olish bilan bog'liq bo'lsa kerak. Agar to'g'ri juftlikni aniqlashda $S_1(110100, 0010)$ ni tanlaganimizda, o'rinni almashtirish jadvaliga muvofiq S_8 blokni ham tahlilda hisobga olishimizga to'g'ri kelar edi. Bu esa umumi ehtimollikni tushirib yuborar edi.

§3.6. DES shifrlash algoritmining to’liq raundi differensial kriptotahlli



3.8-rasm. Ikki raundli xarakteristika.

DES shifrlash algoritmining to’liq, 16 raundi nisbatan differensial kriptotahliga asoslangan hujumni qo’llash uchun E.Bixam va A.Shamirlar tomonidan bitta raundda shunday ayirmadan foydalanish taklif etildiki, ushbu ayirma shifrlash funksiyasidan o’tish natijasida chiqishda ayirmasi nol bo’lishi kerak [5]. Ushbu holda 1-rasmda ko’rsatilgan ikki raundli xarakteristikadan foydalanish mumkin. U holda ikki raundli xarakteristikani 3.8-rasmda ko’rsatilganidek qurish mumkin bo’ladi. O’n qismiy blokka kiruvchi ayirmaning bo’lishi mumkin bo’lgan variantlardan biri $P_R = 19\ 60\ 00\ 00_x = 0001\ 1001\ 0110\ 0000\ 0000\ 0000\ 0000_2$ ayirmadan foydalanish. Unda $0001\ 1001\ 0110\ 0000\ 0000\ 0000\ 0000_2$ da qiymati 1 bo’lgan bitlar 4, 5, 8, 10, 11 pozisiyalar ekanligi 3.11-jadvaldagি kengaytirib o’rin almashtirishdan keyin ushbu bitlar 5, 6, 7, 8, 11, 13, 15, 16 pozisiyalarga o’tishi e’tiborga olinsa, $19\ 60\ 00\ 00_x$ ni kengaytirib o’rin almashtirish natijasi $E(19\ 60\ 00\ 00_x) = 000011\ 110010\ 101100\ 000000\ 000000\ 000000\ 000000_2$.

3.13-jadval. S₃ blok uchun ΔA va ΔC ning mos kelishlari jadvali.

ΔC	000	001	010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
ΔA	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
011000	0	8	4	6	6	0	6	2	4	0	4	2	10	0	6	6
011001	4	2	4	8	4	2	10	2	2	2	6	8	2	6	0	2
011010	0	8	6	4	4	0	6	4	4	8	0	10	2	2	2	4
011011	4	10	2	0	2	4	2	4	8	2	2	8	4	2	8	2
011100	0	6	8	8	4	2	8	0	12	0	10	0	4	0	2	0
011101	0	2	0	6	2	8	4	6	2	0	4	2	4	10	0	14
011110	0	4	8	2	4	6	0	4	10	0	2	6	4	8	4	2
011111	0	6	8	0	10	6	4	6	4	2	2	10	4	0	0	2
100000	0	0	0	0	0	4	4	8	0	2	2	4	10	16	12	2
100001	10	8	8	0	8	4	2	4	0	6	6	6	0	0	2	0
100010	12	6	4	4	2	4	10	2	0	4	4	2	4	4	0	2
100011	2	2	0	6	0	2	4	0	4	12	4	2	6	4	8	8
100100	4	8	2	12	6	4	2	10	2	2	2	4	2	0	4	0
100101	6	0	2	0	8	2	0	2	8	8	2	2	4	4	10	6
100110	6	2	0	4	4	0	4	0	4	2	14	0	8	10	0	6
100111	0	2	4	16	8	6	6	6	0	2	4	4	0	2	2	2
101000	6	2	10	0	6	4	0	4	4	2	4	8	2	2	8	2
101001	0	2	8	4	0	4	0	6	4	10	4	8	4	4	4	2
101010	2	6	0	4	2	4	4	6	4	8	4	4	4	2	4	6
101011	10	2	6	6	4	4	8	0	4	2	2	0	2	4	4	6
101100	10	4	6	2	4	2	2	2	4	10	4	4	0	2	6	2
101101	4	2	4	4	4	2	4	16	2	0	0	4	4	2	6	6
101110	4	0	2	10	0	6	10	4	2	6	6	2	2	0	2	8
101111	8	2	0	0	4	4	4	2	6	4	6	2	4	8	4	6
110000	0	10	8	6	2	0	4	2	10	4	4	6	2	0	6	0
110001	2	6	2	0	4	2	8	8	2	2	2	0	2	12	6	6
110010	2	0	4	8	2	8	4	4	8	4	2	8	6	2	0	2
110011	4	4	6	8	6	6	0	2	2	2	6	4	12	0	0	2
110100	0	6	2	2	16	2	2	2	12	2	4	0	4	2	0	8
110101	4	6	0	10	8	0	2	2	6	0	0	6	2	10	2	6
110110	4	4	4	4	0	6	6	4	4	4	4	4	0	6	2	8
110111	4	8	2	4	2	2	6	0	2	4	8	4	10	0	6	2
111000	0	8	12	0	2	2	6	6	2	10	2	2	0	8	0	4
111001	2	6	4	0	6	4	6	4	8	0	4	4	2	4	8	2
111010	6	0	2	2	4	6	4	4	4	2	2	6	12	2	6	2
111011	2	2	6	0	0	10	4	8	4	2	4	8	4	4	0	6
111100	0	2	4	2	12	2	0	6	2	0	2	8	4	6	4	10
111101	4	6	8	6	2	2	2	2	10	2	6	6	2	4	2	0
111110	8	6	4	4	2	10	2	0	2	2	4	2	4	2	10	2
111111	2	6	4	0	0	10	8	2	2	8	6	4	6	2	0	4

Ushbu holatda kengaytirib o’rin almashtirishdan keyin S₁ blokka 000011, S₂ blokka 110010, S₃ blokka 101100 bitlar ketma-ketligi kelib tushadi. Qolgan barcha S bloklarga qiymatlari faqat nol bo’lgan ayirmalar kelib tushadi. 3.9, 3.10 va 3.13-jadvallarga muvofiq mos ravishda S₁ blokdan qiymati nol bo’lgan ayirmaning chiqish ehtimoli 14/64, S₂ blokdan qiymati nol bo’lgan ayirmaning chiqish ehtimoli 8/64, S₃ blokdan qiymati nol bo’lgan ayirmaning chiqish ehtimoli 10/64.

Yuqorida aytilganlarni hammasini birlashtirib, qiymati $19\ 60\ 00\ 00_x$ bo'lgan ayirma S bloklarga qirsa, ushbu S bloklardan qiymati nol bo'lgan ayirma

$$p=14/64*8/64*10/64=35/8192 \approx 2^{5,13}/2^{13} \approx 1/2^{7,87}.$$

ehtimollik bilan chiqadi.

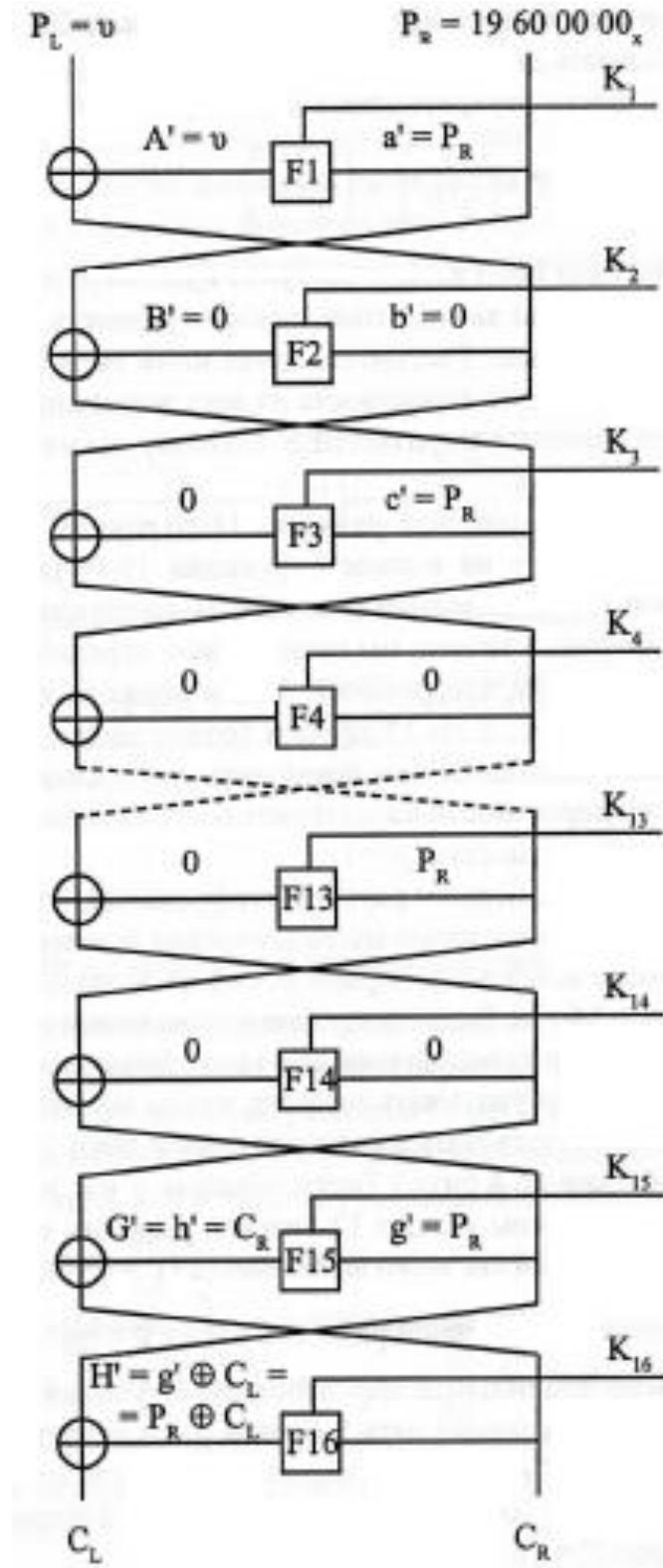
DES shifrlash algoritmining to'liq raundini differensial kriptotahlili uchun Bixam va Shamirlar ikki raundli xarakteristikadan 6 marta (2-raunddan 13-raundgacha) foydalanishni taklif qildilar. Oltita ikki raundli xarakteristikaning ehtimolligi quyidagicha bo'ladi:

$$p=(1/2^{7,87})^6=1/2^{47,22}=2^{-47,22}.$$

Ushbu holda 14-raundga qiymati nol bo'lgan ayirma kiradi va f shifrlash funksiyasidan $p=1$ ehtimollik bilan nol ayirma chiqadi (3.9-rasm). Biz yuqorida keltirgan ayirma to'liq DES shifri uchun bo'lishi mumkin bo'lgan kirish-chiqish ayirmalarining ichidan eng katta ehtimollikka ega bo'lgani hisoblanadi. Shu bois, kalitni bitlarinin topishda undan foydalanish mumkin.

Bizga 16-raundning chiqish ayirmasi ma'lumligi va 14-raund kirish ayirmasi holga teng ekanligidan 15-raund f shifrlash funksiyasidan 16-raundning o'ng qismiy chiqish ayirmasi chiqishni aniqlash mumkin. 15-raundning kirish ayirmasi ma'lum, demak, 16-raundning f shifrlash funksiyasidan chiqish ayirmasini osongina aniqlash mumkin. Shunday qilib, 2-raunddan 13-raundgacha ikki raundli xarakteristikadan foydalanish va 16-raundning chiqish ayirmasini aniq bilish xarakteristikaning umumiу ehtimolligini hisobga olishda oxirgi uchta raundni chiqarib tashlash imkonini beradi. Oxirgi uchta raund doimo $p=1$ ehtimollik bilan bajariladi.

Shuni ham qayd etish lozimki, birinchi raundning chiqishida ayirmaning birinchidan o'ng ikkinchi bitigacha nol bo'limgan bitlar bo'lishi mumkin (uchta S blokdan 4 bitlardan chiqishlarga mos holda). Buning natijasida jami 2^{12} ta chiqish ayirmasi bo'lishi mumkin. Ushbu 12 bitli ayirmalarning har biri 2^{12} ta variantning biri orqali hosil qilinishi mumkin, ya'ni kiruvchi juftliklarning umumiу kombinasiyasi $(2^{12})^2=2^{24}$. Kerakli ayirmaning paydo bo'lish ehtimoli $p=1/2^{12}$ ga teng.



3.9-rasm. To’liq DES shiffriga differensil tahlilni qo’llanilishi.

Shuningdek, to’g’ri juftliklarni tanlashda 16-raundning f shifrlash funksiyasidan chiqishda oxirgi 5 ta S blokda nol ayirma paydo bo’lishini hisobga

olish lozim. Shunday qilib, bo'lishi mumkin bo'lgan 2^{24} ta matn juftliklaridan 2^{20} tasining oxirgi 20 biti (oxirgi 5 ta S blokdan chiquvchi) nol bo'lmasligi mumkin. U holda taxminan $2^{4}=16$ ta bo'lishi mumkin bo'lan matn juftliklari qolmoqda.

Agar S_1 , S_2 va S_3 bloklar tahliliga e'tibor berilsa, berilgan kiruvshi ayirma uchun ayrim chiquvchi ayirmalar umuman paydo bo'lmasligini payqash mumkin.

Yuqoridagilarga asoslanib, birinchi raundni tahlil qilish hisobiga to'g'ri juftliklarni izlash doirasini ancha qisqartirish mumkinligini Bixam va Shamirlar ko'rsatib berishgan. Bir necha to'g'ri juftliklar topilishi bilan kalitning to'g'ri qiymatlarini aniqlash mumkin bo'ladi.

§3.7. GOST 28147-89 shifrlash algoritmi raund akslantirishlarining tahlili

Tahlil uchun GOST 28147-89shifrlash algoritmining oddiy o'rniqa qo'yish rejimini ko'rib chiqamiz. Chunki boshqa algoritmning boshqa rejimlari ham aynan shu rejimdagi akslantirishlardan foydalanadi.

Ushbu shifrlash algoritmida 8 ta S blokdan tashkil topgan o'rniqa qo'yish jadvali hamda S bloklardan chiqqan 32 bitli ketma-ketlikni 11 pozisiyaga siklik surishdan iborat o'rin almash tirish akslantirishlaridan foydalaniladi. Bu erda dastlabki 32 bitli blok 8 ta 4 bitli bloklarga bo'linadi va bu 4 bitli bloklar S bloklarga uzatiladi. Ushbu S bloklardan chiqqan 4 bitli ma'lumotlar bloki yana 32 bitga birlashtiriladi. 32 bitli ma'lumotlar ketma-ketligiga 11 bit chapga siklik surish qo'llaniladi. Bu siklik surish natijasida keyingi raundlarda 4 bitli bloklarga bo'lishda dastlabki 4 bitli blokni tashkil qiluvchi bitlar yana bitta blokda ishtirok etmaydi. Chunki dastlabki bitlar ketma-ketligi aralashib ketgan bo'ladi.

GOST 28147-89shifrlash algoritmida raund funksiyasi 3 ta asosiy amaldan tashkil topgan.

11 bit chapga siklik surish tahlili. Odatda differensial kriptotahlilda 2 ta matnni ayirmasi tadqiqot ob'ekti sifatida o'rganiladi. Faraz qilaylik, A va V matnlari berilgan bo'lsin. U holda ularning ayirmasi ($A \oplus V$) ga teng bo'ladi. Agar ushbu

matnlarni har biri s razryadga chapga surilsa, buning natijasida $(A \ll s) \oplus (V \ll s)$ ayirmaga ega bo'lish mumkin va bu ayirma quyidagi xossaga ega:

$$(A \ll s) \oplus (V \ll s) = (A \oplus V) \ll s.$$

Agar ushbu amal GOST 28147-89 shifrlash algoritmiga nisbatan qo'llanilsa, u holda quyidagiga ega bo'lish mumkin:

$$(A \ll 11) \oplus (V \ll 11) = (A \oplus V) \ll 11,$$

ya'ni siklik surish natijasida chiqishda to'g'ri ayirmani hosil qilish uchun kiruvchi ayirmani 11 pozisiyaga chapga siklik surish zarur.

2ⁿ ni moduli bo'yicha qo'shish amali. Differensial kriptotahlil usuli ikkita xabar o'rtasidagi o'xhashmaslikni o'zgarishini kuzatishga asoslangan. O'xhashmaslikni aniqlash uchun 2 ni moduli bo'yicha qo'shish amalidan foydalaniladi, buning natijasida dastlabki ikkita xabarning farqlanuvchi bitlari joylashgan pozisiyalarda nol bo'lмаган bitlar hosil qilinadi. Aynan shu sababli, ya'ni bir xil qiymatlarni 2 ni moduli bo'yicha qo'shish natijasi nol bo'lганligi sababli DES shifrlash algoritmida ayirmalarni raund akslantirishi F shifrlash funksiyasidan o'tishida raund kalitlari qiymatlari hisobga olinmaydi. GOST 28147-89 shifrlash algoritmida DES shifrlash algoritmidan farqli o'laroq raund kaliti bilan qo'shish 2^{32} ni moduli bo'yicha amalgalash oshiriladi. Shu sababli ushbu turdag'i qo'shish ta'sirini o'rganish lozim. Buning uchun 32 razryadli sonlar ustida bajarilgan amallarni to'liq tahlil qilish qiyin masala. Shu sababli 2, 3, 4 razryadli sonlarni bir-birlari bilan $2^2, 2^3, 2^4$ modullari bo'yicha qo'shishni tahlil qilingan [16]. Natijalar mos holda 3.14, 3.15, 3.16-jadvallarda keltirilgan.

3.14-jadval. $(a+b) \mod 2^2$ amalini tahlili.

	0	1	2	3
0	16	0	0	0
1	0	8	0	8
2	0	0	16	0
3	0	8	0	8

3.15-jadval. $(a+b)mod2^3$ amalini tahlili.

	0	1	2	3	4	5	6	7
0	64	0	0	0	0	0	0	0
1	0	32	0	16	0	0	0	16
2	0	0	32	0	0	0	32	0
3	0	16	0	16	0	16	0	16
4	0	0	0	0	64	0	0	0
5	0	0	0	16	0	32	0	16
6	0	0	32	0	0	0	32	0
7	0	16	0	16	0	16	0	16

Ushbu jadvallarni tahlil qilish modul bo'yicha qo'shishda ayirmalar o'zgarmasdan qolish ehtimolligini aniqlash imkonini berdi. Ushbu jadvallarning har birida (differensial tahlilni qo'llashga mo'ljallangan boshqa jadvallar kabi) vertikal bo'yicha kirish ayirmasi ΔA , gorizontal bo'yicha chiqish ayirmasi ΔC ning qiymatlari joylashtirilgan.

Bir qarashda 3.14-3.16 jadvallar bir xil tuzilmaga ega ekanligini payqash mumkin. 3.15-jadvalning chap yuqori va o'ng pastki choraklari 3.14-jadvalni tuzilmasiga ega. Xuddi shuningdek, 3.16-jadval ham 3.15-jadval bilan o'xshashligini payqash mumkin.

3.16-jadval. $(a+b)mod2^4$ amalini tahlili.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	256	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	128	0	64	0	0	0	32	0	0	0	0	0	0	0	32
2	0	0	128	0	0	0	64	0	0	0	0	0	0	0	0	64
3	0	64	0	64	0	32	0	32	0	0	0	0	0	0	32	0
4	0	0	0	0	128	0	0	0	0	0	0	0	0	128	0	0
5	0	0	0	32	0	64	0	32	0	0	0	32	0	64	0	32
6	0	0	64	0	0	0	64	0	0	0	64	0	0	0	64	0
7	0	32	0	32	0	32	0	32	0	32	0	32	0	32	0	32
8	0	0	0	0	0	0	0	256	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	32	0	128	0	64	0	0	0	0	32
10	0	0	0	0	0	0	64	0	0	0	128	0	0	0	64	0
11	0	0	0	0	0	32	0	32	0	64	0	64	0	32	0	32
12	0	0	0	0	128	0	0	0	0	0	0	0	128	0	0	0
13	0	0	0	32	0	64	0	32	0	0	0	32	0	64	0	32
14	0	0	64	0	0	0	64	0	0	0	64	0	0	0	64	0
15	0	32	0	32	0	32	0	32	0	32	0	32	0	32	0	32

Tahlil qilish natijasida olingan barcha xulosalarni nafaqat 2^{32} moduli bo'yicha qo'shish, balki butun sonlarni 2^n ni moduli bo'yicha qo'shish - $(a + b) \bmod 2^n$ ga qo'llash mumkin:

1. Ixtiyoriy kiruvchi ayirma chiqishda o'zgarmasdan qolishi mumkin. Kiruvchi ayirmaning chiqishda o'zgarmasdan qolish ehtimolligini quyidagicha hisoblash mumkin:

$$\text{agar kirish ayirmasi } \Delta_k < 2^{n-1}, \text{ u holda } p = 1/2^k; \quad (*)$$

$$\text{agar kirish ayirmasi } \Delta_k \geq 2^{n-1}, \text{ u holda } p = 1/2^{k-1}, \quad (**)$$

bu yerda k – kiruvchi ayirmadagi nol bo'lмаган bitlar soni.

Agar kirish ayirmasi $\Delta_k = 0$ bo'lsa, akslantirishning chiqishida $r=1$ ehtimollik bilan chiqish ayirmasi $\Delta_{ch} = 0$ bo'ladi.

2. Agar kirish ayirmasi $\Delta_k = 2^{n-1}$ bo'lsa, $r=1$ ehtimollik akslantirish chiqishida $\Delta_{ch} = 2^{n-1}$ ayirma bo'ladi.

Sonlarni 2^n ni moduli bo'yicha qo'shishda akslantirishga kiruvchi ayirma chiqishda qanday ehtimollik bilan o'zgarmasdan qolishini bilishda ushbu keltirilgan qoida juda muhim hisoblanadi.

S-bloklar ёрдамидаги аkslantirishlarning tahlili. Tahlil qilish uchun amalda foydalanilayotgan, fiksirlangan 3.17-jadval va tasodifiy 3.18-jadvaldan foydalanildi.

3.17-jadval. Fiksirlangan о'rniga qo'yish jadvallari (S-bloklar).

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S1	4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3
S2	14	11	4	12	6	13	15	10	2	3	8	1	0	7	5	9
S3	5	8	1	13	10	3	4	2	14	15	12	7	6	0	9	11
S4	7	13	10	1	0	8	9	15	14	4	6	12	11	2	5	3
S5	6	12	7	1	5	15	13	8	4	10	9	14	0	3	11	2
S6	4	11	10	0	7	2	1	13	3	6	8	5	9	12	15	14
S7	13	11	4	1	3	15	5	9	0	10	14	7	6	8	2	12
S8	1	15	13	0	5	7	10	4	9	2	3	14	6	11	8	12

3.18-jadval. Tasodifiy o'rniga qo'yish jadvallari (S-bloklar).

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S1	9	13	4	7	10	6	1	0	11	2	8	5	14	3	12	15
S2	15	2	4	3	1	6	5	13	10	7	9	12	8	0	11	14
S3	5	11	0	7	15	8	10	13	3	2	9	1	12	6	4	14
S4	2	6	9	5	13	14	0	4	12	10	11	7	15	3	1	8
S5	4	12	2	0	15	7	14	13	8	5	11	10	1	9	6	3
S6	10	15	12	1	13	14	11	2	7	4	6	9	0	3	8	5
S7	3	10	14	9	6	1	12	13	8	11	4	15	5	7	2	0
S8	12	9	14	2	13	15	10	11	3	6	7	4	5	0	8	1

3.19-jadval. Fiksirlangan S1 bloki tahlili.

S1	1	2	3	4	5	6	7	8	9	a	b	c	d	e	F
1	0	0	0	0	2	2	0	2	0	0	2	0	4	4	0
2	0	2	0	0	0	2	4	2	0	0	0	2	4	0	0
3	0	0	4	2	0	2	0	2	0	6	0	0	0	0	0
4	2	2	0	4	0	0	0	0	4	0	0	0	2	0	0
5	0	4	0	0	0	0	4	0	4	0	0	4	0	0	0
6	0	0	4	6	0	2	0	2	0	2	0	0	0	0	0
7	2	0	0	0	2	0	0	0	0	4	2	0	0	4	2
8	2	2	0	0	2	0	2	2	0	2	0	0	2	2	0
9	0	2	4	0	2	0	0	0	0	0	2	2	0	0	4
A	2	0	0	0	2	2	2	2	2	0	2	0	0	0	2
B	0	2	0	2	0	0	0	2	2	0	2	0	2	2	2
C	4	2	4	0	2	0	0	0	0	0	2	2	0	0	0
d	0	0	0	0	0	2	2	0	0	2	2	2	2	2	2
e	2	0	0	2	2	2	0	0	2	0	0	2	2	2	0
f	2	0	0	0	2	2	2	2	2	0	2	0	0	0	2

Tahlil qilish natijasida quyidagi qonuniyatlar aniqlandi:

1. Kirish ayirmasi ΔA ning bir xil qiymatiga mos keluvchi chiquvchi ayirma ΔC ning turli qiymatlarining umumiyligi soni, bitta satrdagi barcha qiymatlar yig'indisi doimo 2^4 ga teng.
2. Barcha bloklarda kirish ayirmasi ΔA ning nol bo'limgan qiymatlariga chiquvchi ayirma ΔC ning nol bo'limgan qiymatlari mos keladi.
3. Fiksirlangan jadvallar uchun S7 va S8 bloklar nisbatan zaif bloklardir.

4. Tasodifiy jadvallar uchun S3, S4 va S6 bloklar nisbatan zaif bloklardir.

Misol tariqasida S1 bloklarni tahlil qilish natijalari fiksirlangan jadvallar uchun 3.19-jadvalda va tasodifiy o'rniga qo'yish jadvallari uchun 3.20-jadvalda keltirilgan. Ushbu jadvallarda kirish ayirmasi ΔA ning qiymatlari birinchi ustunda, unga mos keluvchi chiqish ayirmasi ΔC ning qiymatlari gorizontal satrlarda keltirilgan. Kirish ayirmasi ΔA ning nol bo'lgan qiymatlarida S bloklardan chiqishda bir ehtimollik ΔC ning nol bo'lgan qiymatlari chiqishini hisobga olib, ayrim jadvallarda $\Delta A=0$ bo'lgan satr kiritilmagan.

3.20--jadval. Tasodifiy S1 bloki tahlili.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
1	0	2	0	4	2	0	0	0	0	2	0	0	2	4	0	
2	0	0	2	2	0	0	2	2	0	0	2	2	2	2	0	
3	0	2	0	0	0	0	0	2	0	2	4	0	0	0	4	
4	0	2	0	2	2	4	0	2	0	0	2	2	0	0	0	
5	0	0	0	0	2	0	2	4	2	2	0	0	2	0	0	
6	0	2	0	0	0	0	4	2	2	0	0	0	0	4	2	
7	0	0	2	0	2	0	0	0	0	2	0	4	2	2	0	
8	0	0	4	0	2	2	0	0	0	0	0	0	2	2	0	
9	0	2	0	0	0	0	2	0	2	2	0	2	2	0	2	
10	0	2	0	2	0	2	2	0	2	2	0	0	0	0	4	
11	0	0	2	0	0	4	2	0	0	0	2	0	4	0	2	
12	0	2	0	0	2	2	0	2	4	2	0	0	0	0	2	
13	0	0	0	2	2	0	0	0	4	0	2	4	0	2	0	
14	0	0	6	2	2	2	0	0	0	0	4	0	0	0	0	
15	0	2	0	2	0	0	2	2	0	2	0	2	0	0	2	

§3.8. GOST 28147-89 shifrlash algoritmining differrensial tahlili

Shifrlash raundidan o'tishda iloji boricha tekis taqsimlanganlik kuzatilmasligi uchun GOST 28147-89 algoritmining tahlili uchun kirish ayirmalarini turli tartibda olish maqsadga muvofiq. Shu sababli kirish ayrmalarini tanlashda quyida keltirilgan yondoshuvdan foydalanildi:

1. shifrlash raundining chiqishida katta ehtimollik bilan yagona chiqish ayirmasi paydo bo'lishi uchun kirish ayirmasi ΔA iloji boricha kamroq S bloklarga kirishi lozim;

2. 2^{32} moduli bo'yicha qo'shishda kirish ayirmasi ΔA o'ziga akslanishi, ya'ni chiqishda o'zgarmasdan qolishi uchun u iloji boricha kamroq nol bo'lмаган bitlardan tashkil topgan bo'lishi lozim;

3. ΔA kirish ayirmasi S bloklardan o'tishida iloji boricha kamroq nol bo'lмаган bitlar (ilioji bo'lsa bitta bit) dan tashkil topgan ΔC chiqish ayirmasi katta ehtimollik bilan paydo bo'lishi lozim.

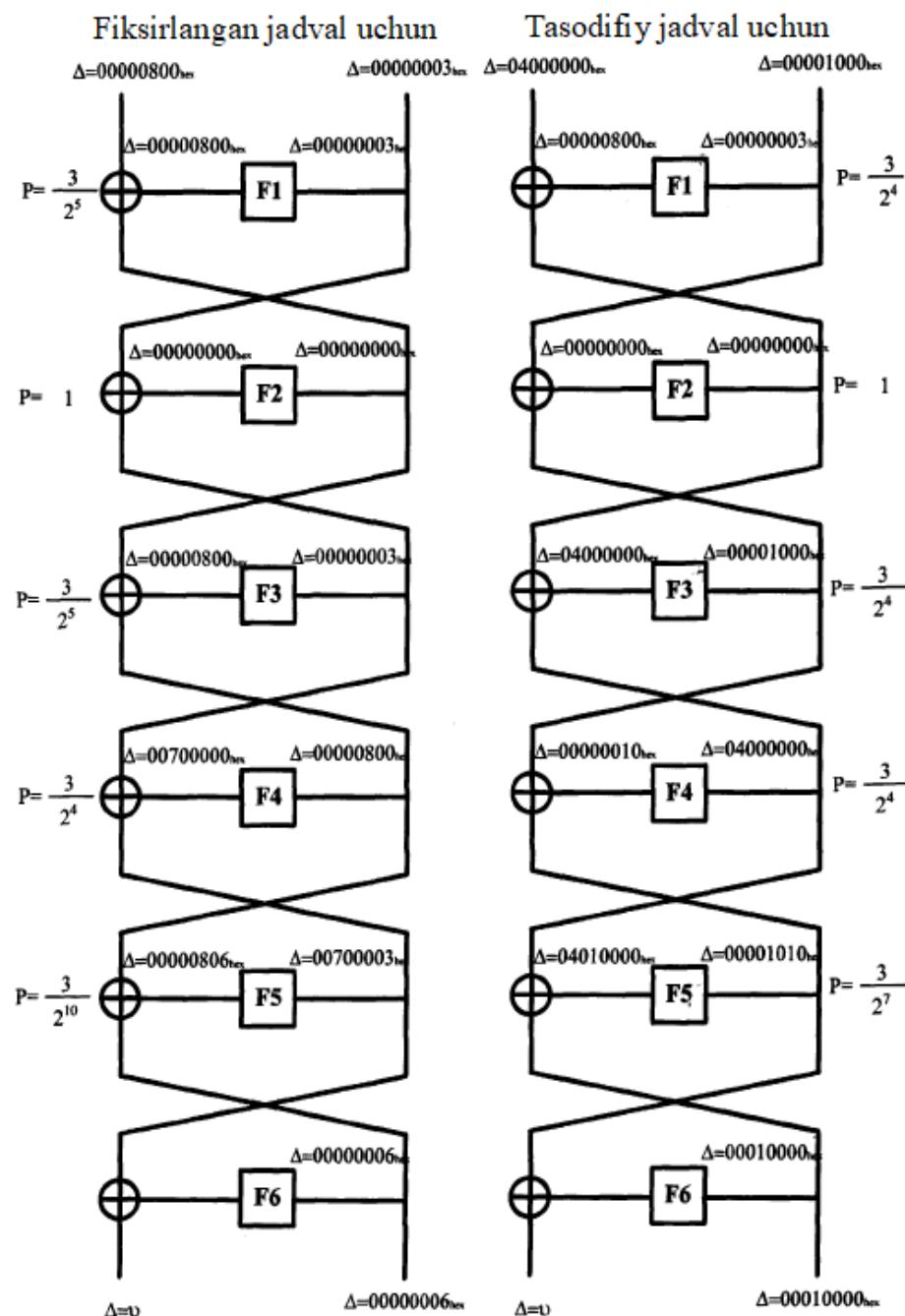
GOST 28147-89 shifrlash algoritmining 6 raundu uchun ayirmalar 3.21-jadvalda o'n otilik sanoq tizimida keltirilgan. Bu yerda p chiqish ayirmasining kirish ayirmasiga mos kelish ehtimolligini anglatadi. v chiqish ayirmasining chap qismiy bo'lagi bo'lib, u bo'lishi mumkin bo'lgan qiymatlardan birini qabul qiladi. 3.21-jadvalda ayirmalarning yuqori qismi ushbu ayirmaning chap, quyi qismi y o'n qismiy bo'lagiga mos keladi.

3.21-jadval. GOST 28147-89 shifrlash algoritmining 6 raundu uchun ayirmalar.

№	Fiksirlangan jadval uchun			Tasodifiy jadval uchun		
	Kirish ayirmasi	Chiqish ayirmasi	p	Kirish ayirmasi	Chiqish ayirmasi	p
1	00050000	v	$\frac{1}{2^{19}}$	00000010	v	$\frac{1}{2^{13}}$
	00000030	00000F80	$\frac{1}{2^{19}}$	04000000	2000000	$\frac{1}{2^{13}}$
2	00002800	v	$\frac{1}{2^{14}}$	04000000	v	$\frac{1}{2^{11}}$
	00000007	800000000	$\frac{1}{2^{14}}$	00001000	00010000	$\frac{1}{2^{11}}$
3	00000800	v	$\frac{1}{2^{17}}$	00000001	v	$\frac{1}{2^{11}}$
	00000003	000000006	$\frac{1}{2^{17}}$	00300000	05680001	$\frac{1}{2^{11}}$

3.21-jadvalda keltirilgan ayirmalardan faqatgina chiqishda katta ehtimollik bilan yagona chiqish ayirmasi paydo bo'lishini ta'minlaydigan kirish ayirmalari tahlil uchun tanlab olindi. Jadvaldan ko'rinish turibdiki, ushbu ayirma fiksirlangan bloklar uchun uchinchi, tasodifiy bloklar uchun ikkinchi satrda joylashgan.

Fiksirlangan bloklardan foydalanadigan shifrlash algoritmi kirishiga ayirmaning $\Delta_k=00000800\ 00000003$ qiymati kelib tushadi (3.10-rasm). Kirish ayirmasining o'n qismi (00000003 qiymat) shifrlash funksiyasi F ga tushadi. Ushbu shifrlash funksiyasi F ning birinchi amali kalit bilan 2^{32} moduli bo'yicha qo'shish amalidir. 00000003 qiymat 2^{31} dan kichik bo'lganligi sababli (*) ga asosan 2^{32} moduli bo'yicha qo'shish natijasi $p=1/2^k=1/2^2$ ehtimollik bilan 00000003 ga teng (ya'ni ayirma o'zgarmasdan qoladi).



3.10-rasm. GOST 28147-89 shifrlash algoritmining
6 raundu uchun differensial xarakteristika qurish.

Shifrlash funksiyasi F dagi keying amal S bloklardan foydalanib, ma'lumotlarni almashtirish amalidir. 00000003 ayirma faqatgina S8 blokiga nol bo'limgan bitlar kirishini ta'minlaydi. 3.22-jadvalda ko'ra agar S8 blokka 3 qiymat kirsa, u holda $p=6/16=3/2^3$ ehtimollik bilan 1 chiqadi va unda faqatgina bitta noldan farqli bit mavjud. Natijada S bloklardan qiymati 00000001 bo'lgan ayirma chiqadi.

Shifrlash funksiyasi F ning oxirgi amali 11 bit chapga siklik surishdan iborat:

$$00000001 << 11 = 00000800.$$

Bu yerda va undan oldin 32 bitli ayirmalaning qiymatlari qulaylik uchun o'n otilik sanoq tizimida keltirilmoqda. Shu sababli 11 bit chapga siklik surish natijasida 8 soni paydo bo'lib qolmoqda.

Shunday qilib, birinchi raund shifrlash funksiyasi F dan $p=3/2^3 \cdot 1/2^2 = 3/2^5$ ehtimollik bilan qiymati 00000800 bo'lgan ayirma chiqmoqda. Birinchi raundda kiruvchi ayirmaning chap qismi birinchi raund shifrlash funksiyasi F dan chiquvchi ayirmaning 00000800 qiymatiga teng. Shu bois, ikkinchi raund shifrlash funksiyasi F ga qiymati nol bo'lgan ayirma kiradi va shifrlash funksiyaisidan bir ehtimollik bilan nol chiqadi.

3.22-jadval. S8 blok uchun kirish va chiqish ayirmalarining mosligi.

S8	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	0	2	0	2	0	0	0	0	0	0	2	0	6	4	0
2	0	0	2	0	0	0	2	0	0	2	0	4	0	2	4
3	6	2	2	0	0	0	2	0	0	2	0	0	2	0	0
4	0	2	0	4	0	0	2	2	2	0	2	0	0	0	2
5	0	2	0	2	0	4	0	0	2	4	0	0	0	0	2
6	2	0	0	0	4	0	2	2	0	0	4	0	0	2	0
7	0	0	0	0	8	0	0	4	0	4	0	0	0	0	0
8	0	2	2	0	0	0	0	4	0	0	0	2	2	4	0
9	2	0	6	0	0	4	0	0	0	0	0	2	0	2	0
a	2	4	0	2	0	0	0	0	0	0	2	2	2	0	2
b	2	2	0	0	0	0	0	0	4	0	0	2	0	0	6
c	0	0	0	2	4	0	2	0	2	2	0	4	0	0	0
d	2	0	0	2	0	0	4	2	2	2	0	0	0	2	0
e	0	0	4	0	0	4	0	0	4	0	4	0	0	0	0
f	0	0	0	2	0	4	2	2	0	0	2	0	4	0	0

Uchinchi raund birinchi raundga o'xhash bo'ladi. Shifrlash funksiyasi F ga qiymati 00000003 bo'lgan ayirma kelib tushadi, undan $p=3/2^5$ ehtimollik bilan 00000800 ayirma chiqadi.

To'rtinchi raund shifrlash funksiyasi F ga qiymati $\Delta_k=00000800$ bo'lgan ayirma kelib tushadi. Bu ayirmaning qiymati 2^{31} dan kichik bo'lganligi sababli 2^{32} ning moduli bo'yicha qo'shish natijasida $p=1/2^k=1/2$ ehtimollik bilan o'ziga akslanadi. $\Delta_k=00000800$ ayirma faqatgina S6 blokka ta'sir qiladi va undan $p=3/2^3$ ehtimollik bilan $e_{16}=14$ chiqadi (2.23-jadval). Oxirgi amal 11 bit chapga siklik surish bo'lib, uning natijasida

$$00000e00<<<11=00700000_{16}$$

ni hosil qilish mumkin. Shunday qilib, to'rtinchi raund shifrlash funksiyasi F ning chiqishida

$$p=1/2 * 3/2^3 = 3/2^4$$

ehtimollik bilan $\Delta_{ch}=00700000$ ayirma chiqadi.

3.23-jadval. S6 blok uchun kirish va chiqish ayirmalarining mosligi.

S6	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	2	0	0	0	6	0	0	0	0	2	0	2	2	0	2
2	0	2	2	0	0	4	0	0	0	0	4	0	0	2	2
3	2	0	4	2	0	2	2	0	0	2	0	0	0	2	0
4	0	0	2	0	0	0	2	0	2	4	4	0	2	0	0
5	2	0	0	0	0	4	2	0	0	2	0	2	0	0	4
6	2	2	0	0	2	2	0	2	2	0	0	2	2	0	0
7	0	0	0	2	0	0	2	2	4	2	0	2	2	0	0
8	0	2	2	0	2	0	2	0	0	0	0	0	2	6	0
9	0	4	0	0	0	0	0	4	0	0	4	0	0	0	4
a	2	0	0	0	0	2	0	4	2	0	0	4	0	2	0
b	2	0	4	2	0	0	0	0	2	0	0	2	4	0	0
c	0	0	0	4	2	0	2	2	2	0	0	0	2	2	0
d	4	2	0	4	2	0	0	2	0	0	0	0	0	0	2
e	0	2	2	0	2	0	2	0	0	0	4	2	0	0	2
f	0	2	0	2	0	2	2	0	2	4	0	0	0	2	0

Beshinchi raund shifrlash funksiyasi F ga qiymati $\Delta_k=00700003$ bo'lgan ayirma kelib tushadi. Xuddi yuqoridagidek, shifrlash funksiyasi F dan $p=3/2^{10}$ ehtimollik bilan $\Delta_{ch}=00000806$ ayirma chiqadi.

Shifrlasning beshinchi raundidan so'ng olti raund shifrlashdan keyin chiqish ayirmasining o'n qismiy blokini qiymati 00000006 ekanligini aniqlash mumkin. Oltinchi raund shifrlash funksiyasidan o'tishda ushbu ayirmaning qiymati quyidagi 7 ta turli chiqish qiymatlariga ega bo'lishi mumkin:

00001000	00002000	00003800	00006800
00001800	00003000	00005800.	(***)

Oltinchi raund shifrlash funksiyasi F ning chiqishi mumkin bo'lgan qiymatlari (***) ni beshinchi raund o'n qismiy bloki qiymati bilan 2 ning moduli bo'yicha qo'shish natijasida quyidagi v ning 7 ta turli qiymatlariga ega bo'lishi mumkin:

00701003	00702003	00703803	00706803
00701803	00703003	00705803.	

Shunday qilib, shifrlashning olti raundi ehtimolligi quyidagiga teng:

$$p=3/2^5*1*3/2^5*3/2^4*3/2^{10} \approx 1/2^{17.7}.$$

Kirish ayirmasi $\Delta_k=04000000$, 00001000 uchun tasodifiy blokli algoritmning tahlili ham xuddi yuqoridagidek bo'ladi. 3.11-rasmida shifrlash raundlaridan o'tishda ayirmalarning akslantirilishi ko'rsatilgan.

Eng katta ehtimollik bilan paydo bo'ladigan (Δ_k, Δ_{ch}) ayirmalar juftligi aniqlangandan so'ng, matnlarning ushbu ayirmalarning qiymatlariga mos keluvchi to'g'ri juftliklarini izlash va matnlarning topilgan to'g'ri juftliklaridan foydalanib, kalit bitlarini aniqlashga kirishish mumkin bo'ladi. Buning uchun quyida keltirilgan algoritm bo'yicha tahlilni davom ettirish lozim:

1. Ayirmalari berilgan Δ_k ayirmaning qiymatiga teng bo'lgan (XL,XR) va (XL1,XR1) ochiq matn juftliklari tanlanadi.

2. Ochiq matnning tanlangan juftliklari GOST 28147-89 shifrlash algoritmi yordamida shifrlanadi. Buning natijasida (YL,YR) va (YL1,YR1) shifr matn juftliklari hosil bo'ladi.

3. $C_R = YR \oplus YR_1$ ning qiymati hisoblanadi. Agar C_R ning qiymati berilgan Δ_{ch} chiqish ayirmasining qiymatiga teng bo'lsa, algoritmning keyingi bandi bajariladi. Aks holda tahlil qilinayotgan juftlik noto'g'ri juftlik bo'lib, algoritmning 8-bandiga o'tiladi.

4. $C_L = YL \oplus YL_1$ ning qiymati hisoblanadi. Agar C_L ning ΔC_L qiymati bilan ayirmaning bundan oldingi banddagi o'n qismiy bloki bilan 2 moduli bo'yicha yig'indisi bo'lishi mumkin bo'lган qiymatlardan birini qabul qilsa, u holda tahlil qilinayotgan juftlik to'g'ri juftlik bo'lib, algoritmning keyingi bandi bajariladi. Aks holda tahlil qilinayotgan juftlik noto'g'ri juftlik bo'lib, algoritmning 8-bandiga o'tiladi.

5. ΔC_L ayirmaning qiymatiga 11 bit o'nga siklik surish qo'llanilib, ΔC_L^{-1} ayirmaning S bloklardan chiqish qiymati aniqlanadi. Har bir S bloklardan chiqishda $\Delta C_L^{-1}_j$ ning qiymati topilsin ($j=1,2,\dots,8$).

6. Har bir S blokning kirishiga maxfiy kalitning qismi bilan qo'shilgan birinchi YR_j ($j=1,2,\dots,8$) matnning qiymati kirsin. Shuningdek, har bir S blokning kirishiga maxfiy kalitning qismi bilan qo'shilgan ikkinchi YR_1_j ($j=1,2,\dots,8$) matnning qiymati kirsin.

7. Sakkizta S bloklarning har biri uchun qismiy kalitning qiymati saralanadi. Har bir S blokka 4 bit kirganligi bois, S bloklarning har biri uchun qismiy kalitning $2^4=16$ ta variantini saralash kerak bo'ladi. Buning uchun

- Navbatdagi k qismiy kalitning qiymati aniqlanadi.
- Kirishning YR_j+k qiymati uchun j-chi S blokdagi $S(YR)_j$ chiqish qiymatini aniqlash lozim.
- Kirishning YR_1_j+k qiymati uchun j-chi S blokdagi $S(YR_1)_j$ chiqish qiymatini aniqlash lozim.
- Agar $S(YR)_j \oplus S(YR_1)_j = \Delta C_L^{-1}_j$ bo'lsa, k qismiy kalitning qiymati yaroqli bo'ladi va ushbu qismiy kalitning hisoblagich qiymati 1 ga oshiriladi.
- Hisoblagichlari eng katta qiymatga ega bo'lган qismiy kalitlar qidirilayotgan kalitlar hisoblanadi.

8. Qismiy kalitning biror qiymati boshqalariga nisbatan ko'proq uchramaguncha (har bir S blok uchun) (XL,XR) va (XL1,XR1) ochiq matn juftliklarining bo'lishi mumkin bo'lgan barcha variantlari uchun bu yerda keltirilgan 1-7 bandlarni takrorlash lozim.

Nazorat savollari

1. Differensial kriptotahlil usulining asosiy g'oyasi nimadan iborat?
2. Differensial tahlil usulining asosini qanday hujum tashkil qiladi?
3. Kirish va chiqish ayirmalari differensiali nima?
4. Ochiq matnlarning to'g'ri juftligi deb nimaga aytildi?
5. Ochiq matnlarning noto'g'ri juftligi deb nimaga aytildi?
6. Kirish va chiqish differensiallari jadvali nima?
7. Differensial tahlil usulini qo'llab, S-DES-2 shifrlash algoritmining qismiy kaliti bitlari qanday topiladi?
8. i-chi raund differensiali yoki ayirmali xarakteristikasi deb nimaga aytildi?
9. Differensial xarakteristika nima?
10. Blokli shifrlarga differensial tahlilni qo'llash qanday tamoyil asosida olib boriladi?
 11. Differensial hujum modeli nima?
 12. Yuqori ehtimolli differensial xarakteristikalar qanday aniqlanadi?
 13. Aniqlangan differensial xarakteristikalar yordamida matnlarning to'g'ri juftliklari qanday aniqlanadi?
14. n raundli shifr uchun differensial kriptotahlilni o'tkazish uchun qanday raundgacha differensial xarakteristika quriladi?
15. differensial kriptotahlilni o'tkazish uchun qanday tartibidagi ochiq matn-shifr matnlar juftligi kerak bo'ladi?
16. Oxirgi shifrlash raundining qismiy kalitini topishda qo'llaniladigan algoritmda bajariladigan amallar ketma-ketligini aytинг.
17. S bloklar uchun kirish va chiqishlarning mosligi nima?

18. DES shifri S blokining tahlil qilish natijasida qanday qonuniyatlarni ko'rish mumkin?
19. Kirish ayirmasi nol bo'lмаган bir raundli akslantirishga misol keltiring.
20. DES shifrlash algoritmining uchta raundi differensial kriptotahlili qanday amalga oshiriladi?
21. DES shifrlash algoritmining to'liq raundi differensial kriptotahlili qanday amalga oshiriladi?
22. Bir xil uzunlikdagi A va V matnlari berilgan bo'lsin. U holda $(A \lll 11) \oplus (V \lll 11) = (A \oplus V) \lll 11$ munosabat o'rinnimi?
23. GOST 28147-89 shifrlash algoritmida 2^n ni moduli bo'yicha qo'shish qanday amalga oshiriladi?
24. GOST 28147-89 shifrlash algoritmida sonlarni 2^n ni moduli bo'yicha qo'shishda akslantirishga kiruvchi ayirma chiqishda qanday ehtimollik bilan o'zgarmasdan qolishini qanday qoida asosida bilish mumkin?
25. GOST 28147-89 shifrlash algoritmida S bloklar yordamidagi akslantirishlarning tahlili natijasida qanday qonuniyatni aniqlash mumkin?
26. GOST 28147-89 algoritmining differensial tahlili uchun kirish ayrmalarini tanlashda qanday yondoshuvdan foydalaniladi?
27. GOST 28147-89 shifrlash algoritmining 6 raundu uchun differensial kriptotahlil qanday amalga oshiriladi?
28. GOST 28147-89 algoritmining differensial tahlilida kalit bitlarini aniqlash algoritmini keltiring?

4-BOB. SP TARMOG'IGA ASOSLANGAN BLOKLI SHIFRNING DIFFERENSIAL KRIPTOTAHLILI

Mavzuni bayon qilishda 4.1-rasmida ko'rsatilgan, kirish bloki va raund kaliti uzunligi 16 bit bolgan o'rinniga qo'yish (SP) tarmog'iga asoslangan, 4 raundli shifrdan foydalaniladi.

§4.1. SP tarmog'iga asoslangan shifrning tavsifi

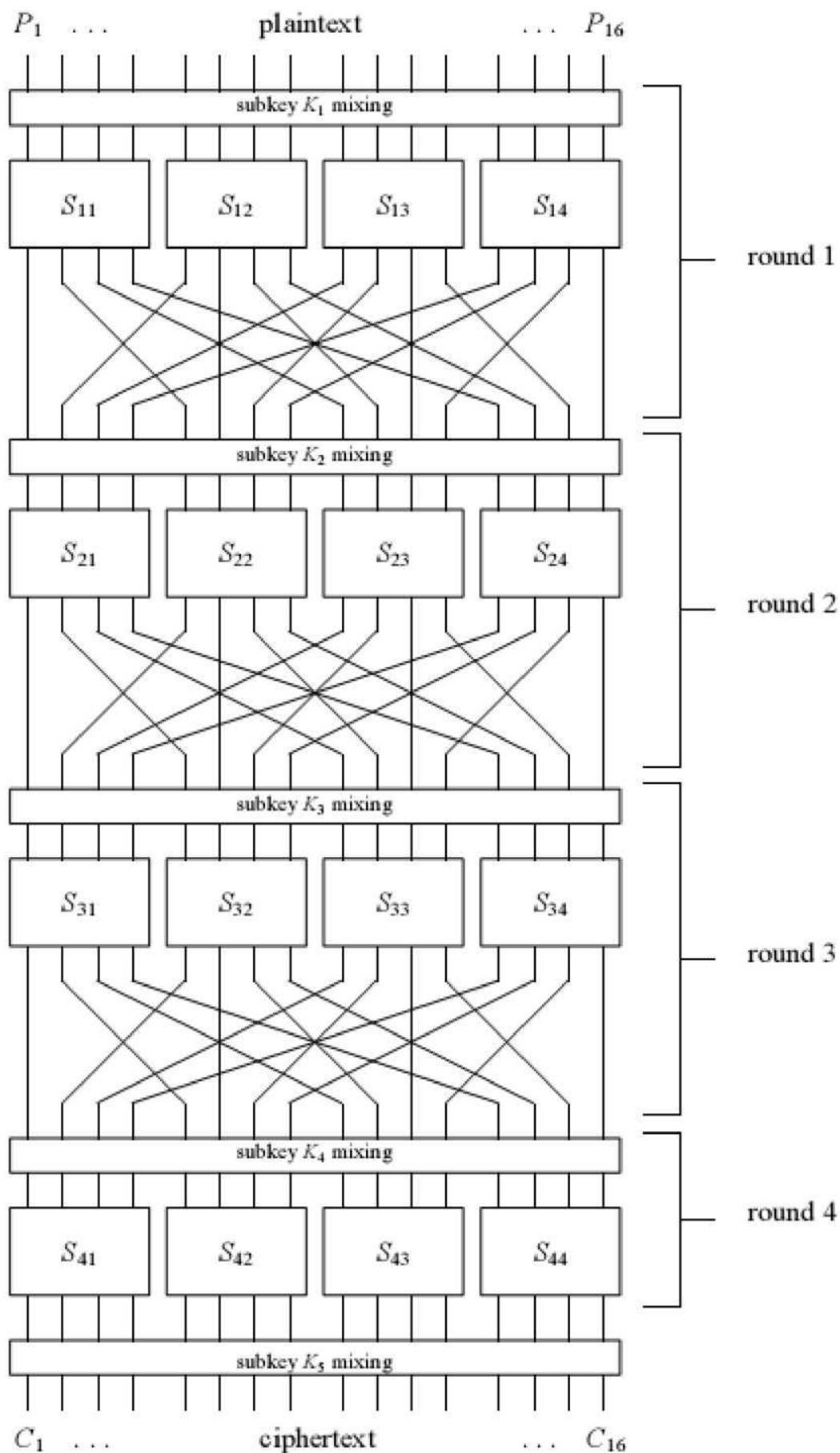
Shifrning har bir raundi quyida keltirilgan kriptografik akslantirish va almashtirishlardan iborat:

- kalitlarni aralashtirish (key mixing).
- o'rniga qo'yish (substitution);
- o'rin almashtirish (permutation).

Kalitlarni aralashtirish (Key mixing). Kalitlarni aralashtirish uchun joriy raund kaliti bitlari joriy raundga kiruvchi ma'lumotlar bloki bitlarii bilan 2 ning moduli bo'yicha qo'shiladi. Oxirgi raunddan chiqqan bitlar ketma-ketligiga kriptotahlilchi teskari yo'nalishda o'rniga qo'yishni osongina amalga oshirishini oldini olish uchun oxirgi raunddan keyin ham kalitlarni aralashtirish qo'llaniladi.

Odatda raund kaliti dastlabki shifrlash kalitidan qanaqadir usullar bilan hosil qilinadi. Biz foydalanayotgan shifrda raund kalitlari bir-biriga bog'liq bo'limgan holda generasiya qilinadi.

O'rniga qo'yish (Substitution yoki S blok). Bu algoritmda 16 bitli ma'lumotlar bloki to'rtta S blokka kiradi. Har bir S blokka 4 bitli ketma-ketlik kirib, undan mos holda 4 bitli ketma-ketlik chiqadi. S blokining eng muhim xususiyati chiziqli emasligi, ya'ni chiqish bitlari kirish bitlarining chiziqli funksiyasi sifatida ifodalanmasligidan iborat. Shifrlash algoritmida barcha S bloklar uchun bir xil chiziqsiz akslantirishdan foydalaniladi. 4.1-jadvalda shifrlash algoritmida foydalaniladigan S blok o'n otilik sanoq tizimida keltirilgan.



4.1-rasm. SP tarmog’iga asoslangan shiffr.

O'rin almashtirish (P blok). Shifrda o'rın almashtirish 4.2-jadvalda keltirilgan qoida asosida amalga oshiriladi. Ushbu jadvalga asosan chap tomondagi birinchi bit, oltinchi va o'n birinchi bitlar hamda o'ng tomondagi oxirgi (o'n oltinchi bit) bit o'z o'rınlarini almashtirmaydilar. Shuningdek, 4.2-jadval bo'yicha o'rın almashtirishni quyidagicha talqiin qilish mumkin: S_j blokdan chiquchi i soni (o'nlik sanoq tizimidagi) S_i blokdan chiquvchi j soni (o'nlik sanoq tizimidagi) bilan bog'langan.

4.1-jadval. SP shifrida qo'llaniladigan S blok.

Kirish	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Chiqish	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

4.2-jadval. O'rın almastirish.

Kirish	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Chiqish	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

4.3-jadval. S bloklar uchun differensiallar juftligiga misol.

X	Y	ΔY		
		$\Delta X = 1011$	$\Delta X = 1000$	$\Delta X = 0100$
0000	1110	0010	1101	1100
0001	0100	0010	1110	1011
0010	1101	0111	0101	0110
0011	0001	0010	1011	1001
0100	0010	0101	0111	1100
0101	1111	1111	0110	1011
0110	1011	0010	1011	0110
0111	1000	1101	1111	1001
1000	0011	0010	1101	0110
1001	1010	0111	1110	0011
1010	0110	0010	0101	0110
1011	1100	0010	1011	1011
1100	0101	1101	0111	0110
1101	1001	0010	0110	0011
1110	0000	1111	1011	0110
1111	0111	0101	1111	1011

Dastlabki matnga o'girish. Shifrlangan ma'lumotni dastlabki matnga o'girish uchun shifrlash jarayonini teskari tartibda bajarish lozim. Buning uchun shifrlashda ishlataladigan akslantirishlar o'rniغا ulargai teskari bo'lgan akslantirishlarni qo'llash (ya'ni, kirish sifatida chiqish, chiqish sifatida kirishdan foydalanish) lozim. Dastlabki matnga o'girishda raund kalitlari teskari tartibda qo'llaniladi va qismiy kalitlardan teskari almashtirishga muvofiq foydalanish kerak.

§4.2. SP tarmog'i asosidagi shifr akslatirishlarining tahlili

Birinchi navbatda S bloklar uchun differensiallar juftligini o'rganamiz. Buning uchun 4×4 o'lchamli S blokni ko'rib chiqamiz 4.2-jadvalda $X = [x_1, x_2, x_3, x_4]$ kirish bitlari vektori va $Y = [y_1, y_2, y_3, y_4]$ chiqish bitlari vektori bo'lsin. S bloklar uchun ma'lum bir ΔX ayirma uchun ΔY ayirma qiymatining hosil bo'lish ehtimolligi yuqori bo'lsa barcha mumkin bo'lgan $(\Delta X, \Delta Y)$ juftliklar uchun (X', X'') ning barcha mumkin bo'lgan juftliklaridan foydalanamiz.

(X', X'') juftliklarning tartibi muhim emas, 4×4 o'lchamli S blok uchun X' ning 16 ta qiymatini ko'rib chiqish yetarli. ΔX ning qiymatidan foydalanib, $X'' = X' \oplus \Delta X$ tenglik yordamida X'' ni hosil qilish mumkin. Shifrning S bloklarini ko'rib chiqib, har bir kirish juftligi $(X', X'') = X' \oplus \Delta X$ uchun ΔY qiymatlarini hosil qilish mumkin. Masalan, berilgan $(X, X \oplus \Delta X)$ kirishlar juftligi uchun X, Y ning ikkilik qiymatlari va unga mos keluvchi ΔY ning qiymatlari $\Delta X = 1011, 1000$ va 0100 qiymatlari uchun 3.26-jadvalda keltirilgan. 3.26-jadvaldagagi satrlardagi har bir X va ΔX ning aniq bir qiymati uchun oxirgi 3 ta ustunda ΔY ning qiymatlari ko'rsatilgan. Ushbu jadvaldan ko'rinish turibdiki, $\Delta X = 1011$ qiymat uchun $\Delta Y = 0010$ ning paydo bo'lish ehtimolligi $8/16$ ga teng. $\Delta X = 1000$ qiymat uchun $\Delta Y = 1011$ ning paydo bo'lish ehtimolligi $4/16$ ga teng. $\Delta X = 0100$ qiymat uchun $\Delta Y = 1010$ ning paydo bo'lish ehtimolligi $0/16$ ga teng va bu juftlik shartni qanoatlantirmaydi.

4.4-jadvalda S bloklar differensiallarining taqsimlanishi ko'rsatilgan. Bunda satrlar ΔX qiymatlarini (o'n otilik sanoq tizimida), ustunlar ΔY qiymatlarini (o'n

oltilik sanoq tizimida) ifodalaydi va ularning kesishmasida mos kelish soni berilgan. Shuni ham qayd etish lozimki, ushbu jadvalda $\Delta X = B$ va $\Delta Y = 2$ da eng katta qiymat mos keladi, ya'ni $\Delta X = B$ kirish ayirmasiiga $p=8/16=1/2$ ehtimollik bilan $\Delta Y=2$ chiqish ayirmasi mos keladi. Ko'pgina kirish-chiqish ayirmalarining mosligi 0 ga teng.

4.4-jadval. Differensiallarning ehtimoliy taqsimlanishi.

ΔX		$\Delta Y - \text{chiqish differensiali}$															
		0	1	2	3	4	5	6	7	8	9	A	B	S	D	E	F
K i r i s h d i f e r e n s i a l i	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
	2	0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
	3	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
	4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
	5	0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
	6	0	0	0	4	0	4	0	0	0	0	0	0	0	2	2	2
	7	0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
	8	0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
	9	0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
	A	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
	V	0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
	S	0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
	D	0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
	E	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
	F	0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

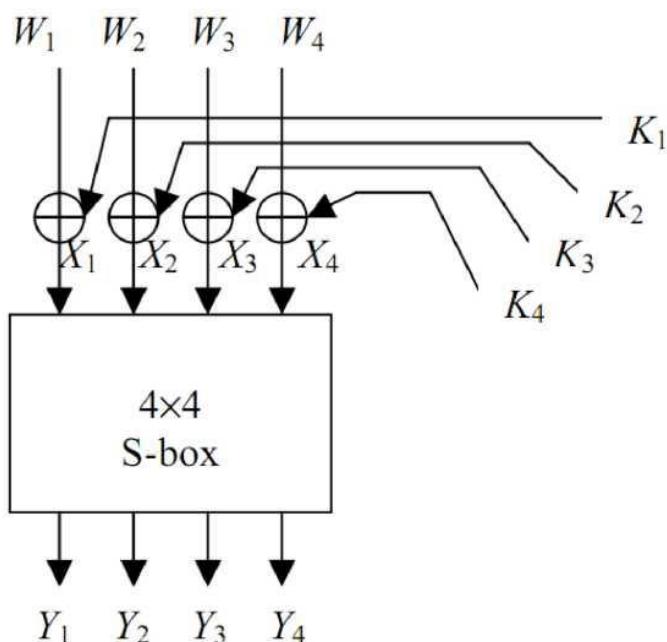
Differensiallarning taqsimlanish jadvalini bir nechta umumiylarini aytib o'tish kerak: birinchidan, shuni ta'kidlash kerakki, satrdagi barcha elementlarning yig'indisi $2n = 16$; shunga o'xshash, har qanday ustunning elementlari yig'indisi $2n = 16$ ga teng (n-kiruvchi va chiquvchi bitlar soni). Shuningdek, (X',X'') juftlik va (X'',X') juftlik bir xil qiymatga ega bo'lganligi sababli barcha elementlarning qiymatlari juft. Chunki, ularning differensiali ΔX ham bir xil qiymat qabul qiladi: $\Delta X = X' \oplus X'' = X'' \oplus X'$. Bundan tashqaru kirish differensiali

$\Delta X = 0$ bo'lganda S bloklardan $p=1$ ehtimollik ($2n=16$) bilan chiqish differensiali $\Delta Y = 0$ paydo bo'ladi.

Differensial hujumda qo'llaniladigan differensial xarakteristikani olish uchun differensiallarni birlashtirishdan oldin S blok differensialiga kalit bitlarining ta'sirini o'rghanish lozim. Buning uchun 4.2-rasmdan foydalanish mumkin. Ushbu rasmda kalit bilan ikkining moduli bo'yicha qo'shish amali hisobga olinmagan holda S blokka kiruvchi bitlar ketma-ketligi X vektor bilan belgilangan. Shu bilan birgalikda shifrda S blokka kiruvchi bitlar ketma-ketligini raund kalitining mos bitlari bilan ikkining moduli bo'yicha qo'shish amalidan foydalanish nazarda tutilgan. Uchbu holda raund kaliti bilan ikkining moduli bo'yicha qo'shish natijasi W vektori bilan belgilansa, u holda kirish differensiali uchun quyidagiga ega bo'lish mumkin:

$$\Delta W = [W'_1 \oplus W''_1, W'_2 \oplus W''_2, \dots, W'_n \oplus W''_n],$$

bu yerda $[W'_1, W'_2, \dots, W'_n]$ va $[W''_1, W''_2, \dots, W''_n]$ – S blokka kiruvchi ikkita qiymatlar.



4.2-rasm. SP tarmog'iya asosidagi shifrda kalitlarni XOR amali bilan qo'shish.

$[W'_1, W'_2, \dots, W'_n]$, va $[W''_1, W''_2, \dots, W''_n]$ uchun raund kaliti bitlari bir xil hamda $K_i \oplus K_i = 0$ bo'lganligi sababli

$$\Delta W_i = W'_i \oplus W''_i = (X'_i \oplus K_i) \oplus (X''_i \oplus K_i) = X'_i \oplus X''_i = \Delta X_i.$$

Shunday qilib, kirish differensialiga kalit bitlarining ta'siri yo'qligi bois, raund kaliti bilan ikkining moduli bo'yicha qo'shish amalini hisobga olmaslik mumkin. Boshqacha aytganda, kalitni hisobga olganda ham hisobga olmaganda ham S blok differensiallarini tarqalishining bir xil jadvaliga ega bo'ladi.

SP tarmog'idagi shifrning S bloklari uchun differensiallar haqidagi ma'lumotlar yig'ilgandan so'ng, butun shifrning foydali differensial xususiyatlarini aniqlashga kirishish mumkin. Bu jarayonni S bloklar uchun mos keladigan differensial juftliklarni birlashtirish orqali amalga oshirish mumkin.

Buning uchun ochiq matn bitlari va oxirgi raundga kirivchi ma'lumotlar bitlaridan foydalanib, har bir raundda S bloklarning ayrim konkret differensiallari juftliklari uchun differensial xarakteristikalar qurish mumkin. Shu tarzda oxirgi raunddagi raund kaliti bitlarini qayta tiklash orqali shifrga hujum qilish mumkin.

§4.3. SP tarmog'i asosidagi shifr uchun differensial xarakteristikalarini qurish

S_{12} , S_{23} , S_{32} , S_{33} bloklardan tashkil topgan differensial xarakteristikani ko'rib chiqamiz (4.3-rasm). Ushbu rasmida nol bo'limgan differensiallar bitlarining ta'sirini va ular tarmoq orqali qanday o'tishini hamda faol deb qaralishi mumkin bo'lgan S bloklarni ko'rish mumkin. Differensial xarakteristikani qurishda S bloklar uchun ochiq matnlarning quyida keltirilgan juftligidan foydalilanadi:

$$\Delta R = [0000 \ 1011 \ 0000 \ 0000].$$

4.3-rasmdan ko'rinish turibdiku, differensial xarakteristika S_{12} , S_{23} , S_{32} , S_{33} bloklardan tashkil topgan:

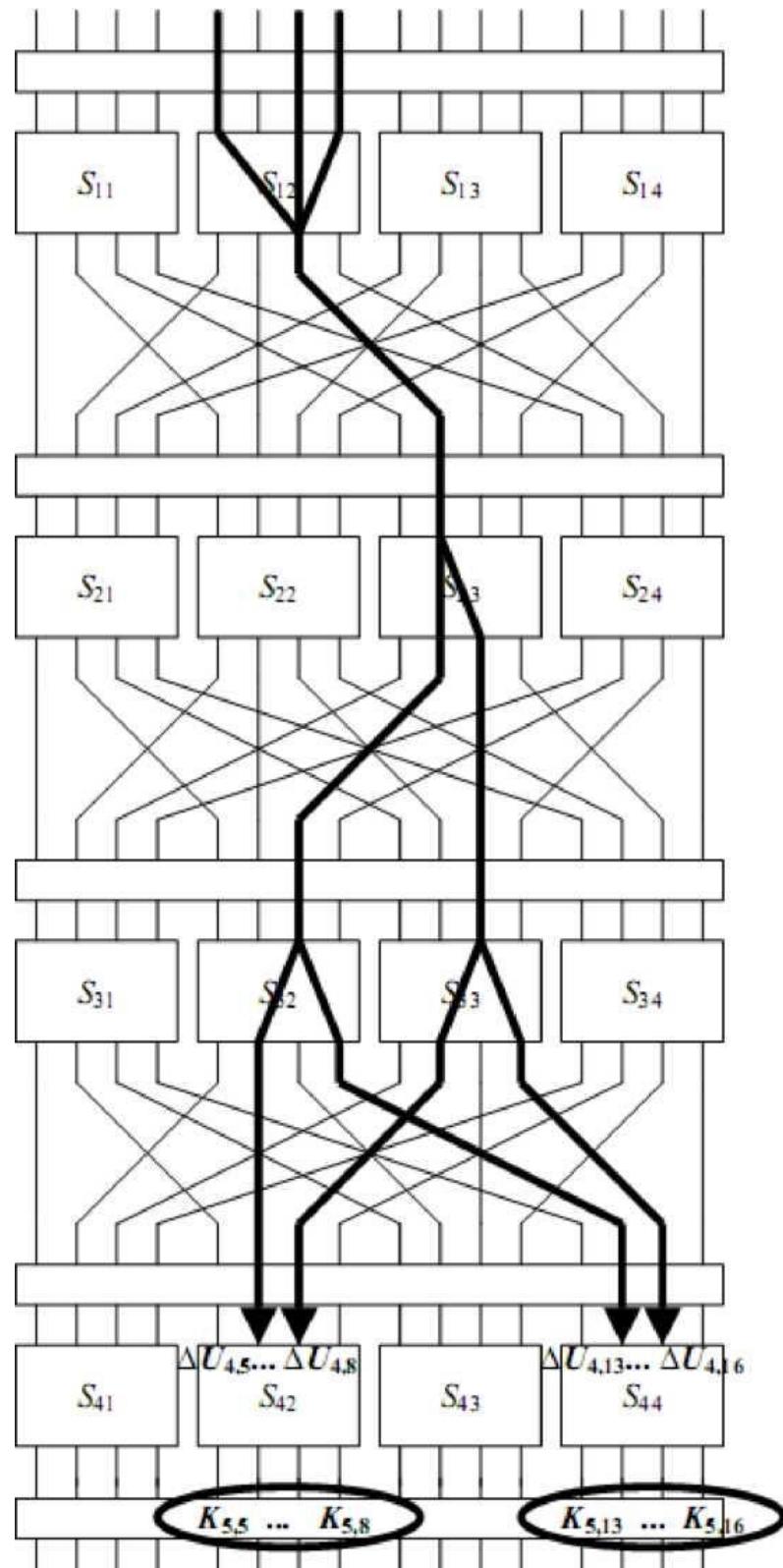
$$S_{12}: \Delta X = B \rightarrow \Delta Y = 2, \text{ paydo bo'lish ehtimoli } 8/16;$$

$$S_{23}: \Delta X = 4 \rightarrow \Delta Y = 6, \text{ paydo bo'lish ehtimoli } 6/16;$$

$$S_{32}: \Delta X = 2 \rightarrow \Delta Y = 5, \text{ paydo bo'lish ehtimoli } 6/16;$$

$$S_{33}: \Delta X = 2 \rightarrow \Delta Y = 5, \text{ paydo bo'lish ehtimoli } 6/16.$$

Boshqa barcha S bloklarga qiymati nol bo'lgan differensiallar kiradi va ulardan bir ehtimollik bilan qiymati nol bo'lgan differensiallar chiqadi.



4.3-rasm. SP tarmog'iga asoslangan shifrga differensial tahlilni qo'llash.

Shifrning kirish differensiali birinchi raundning kirish differensialiga ekvivalent bo'lib, u quyidagicha berilgan:

$$\Delta P = \Delta U_1 = [0000 1011 0000 0000],$$

bu yerda U_i – S blok uchun i -raunddagi kirish va V_i – S-blokdan i -raunddagi chiqishni anglatadi. Demak, ΔU_i va ΔV_i mos keladigan differensiallarni ifodalaydi. Birinchi raundda quyidagi chqish differensialiga ega bo'lish mumkin:

$$\Delta V_1 = [0000 0010 0000 0000].$$

Yuqorida keltirilgan S_{12} uchun bir nechta differensiallar juftliklarini va birinchi raunddagi qayta almashtirishlarni hisobga olib, ΔP ochiq matnning differensiali uchun ehtimolliligi $8/16 = 1/2$ bo'lgan quyidagini kirish differensialini hosil qilish mumkin:

$$\Delta U_2 = [0000 0000 0100 0000].$$

O'z navbatida S_{23} blokdan chiqqan bitlar ketma-ketligi, ya'ni $\Delta V_2 = [0000 0000 0110 0000]$ ikkinchi raunddagi qayta almashtirishdan keyin uchinchi raundda kiruvchi differensialning qiymati

$$\Delta U_3 = [0000 0010 0010 0000]$$

berilgan ΔU_2 ning qiymat uchun $6/16$ va ΔP ochiq matn uchun $8/16 \times 6/16 = 3/16$ ehtimolligi bilan paydo bo'ladi. Berilgan ΔP matni uchun differensial ehtimolini aniqlashda biz birinchi raundning differensiali ikkinchi raundning differensialiga bog'liq emas deb taxmin qilinadi va shuning uchun ularning ikkalasini bajarilish ehtimoli ularning alohida ehtimolliklari ko'paytmasiga teng deb hisoblanadi.

Uchinchi raunddagi S_{32} va S_{33} bloklar differensiallari hamda uchinchi raund almashtirishlaridan foydalanib, uchinchi raundning chiqish differensiali ΔV_3 ning qiymaitni quyidagicha hosil qilish mumkin:

$$\Delta V_3 = [0000 0101 0101 0000].$$

Ushbu differensialga mos holda to'rtinchi raundning kirish differensiali ΔU_3 uchun $(6/16)^2$ va ochiq matnning berilgan ΔP differensiali uchun $8/16 \times 6/16 \times (6/16)^2 = 27/1024$ ehtimollikka ega bo'lib, uning qiymati quyidagiga teng bo'ladi:

$$\Delta U_4 = [0000 0110 0000 0110].$$

§4.4. Kalit bitlarini ajratish

R raundli shifrlash algoritmining R-1 raundigacha qurilgan differensial xarakteristika differensial hujumni amalga oshirish, natijada oxirgi raund kalitining bitlarini tiklash imkonini beradi. Biz bunda oldingi mavzuda bayon qilingan shifr uchun K_5 raund kalitining bitlarini tiklashimiz mumkin. Buning uchun shifrning oxirgi raundida bajarilgan akslantirishlarni qisman tahlil qilish, oxirgi raundga to'g'ri juftlik kirgan yoki kirmaganligini bilish maqsadida oxirgi raundga kirgan ma'lumotlarni tahlil qilish lozim bo'ladi. Oxirgi raund S bloklaridan chiqqan bitlar *qisman maqsadli qismiy kalitlar deb nomlanadi*.

Oxirgi raunddagagi akslantirishlarni qisman tahlil qilish quyidagilardan iborat bo'ladi:

oxirgi raunddagagi S bloklar orqali nolga teng bo'lмаган differensialga ega bo'lgan barcha shifrlangan matn bitlarini teskari yo'nalishda mos S bloklar orqali o'tkazish;

teskari yo'nalishda mos S bloklar orqali o'tkazishda hosil bo'lgan bitlarni qisman maqsadli qismiy kalitning mos bitlari (bo'lishi mumkin bo'lgan barcha qiymatlari) bilan ikkining moduli bo'yicha qo'shish;

Qisman tahlil qilish qisman maqsadli qismiy kalitlarning bo'lishi mumkin bo'lgan barcha qiymatlari uchun kirish differensiali ΔP ni geherasiya qilishda foydalaniladigan ochiq matn juftliklariga mos keluvchi barcha shifr matn juftliklari uchun bajariladi. Har bir qisman maqsadli qismiy kalitlar uchun ularning paydo bo'lishlari soni hisoblagichda saqlab boriladi. Agar oxirgi raunddagagi kirish differensiali differensial xarakteristikadan kutilgan qiymatga to'g'ri kelganda hisoblagichning qiymati bittaga oshiriladi.

Hisoblagich qiymati bo'yicha eng katta qiymatga ega bo'lgan qisman maqsadli qismiy kalit qismiy (raund) kaliti uchun to'g'ri bit qiymatlarini ko'rsatadi. Bu qoida amalda ishlaydi, chunki qisman qisman maqsadli qismiy kalitning to'g'ri qiymati boshqa qismiy kalitlarning qiymatlaridan xarakteristikada kutilgandek

(ya'ni, to'g'ri juftlik paydo bo'lishi bois) oxirgi raundda katta farq qiladi deb taxmin qilinadi.

Noto'g'ri juftlikda hattoki qisman shifrlash va to'g'ri qismiy kalit bilan ham to'g'ri qismiy kalit hisoblagichining qiymati ko'pchilik hollarda oshmaydi, chunki oxirgi raind S blokining kirish bitlari haqida nisbatan tasodifiy taxminlarda noto'g'ri qismiy kalitning ehtimoli juda past bo'ladi.

Biz ko'rayotgan shifrga qilingan hujumda differensial xarakteristika oxirgi raunddagi S_{42} va S_{44} bloklardagi kirishlardan iborat. Har bir shifrlangan matn uchun kalitning $[K_{5,5}, \dots, K_{5,8}, K_{5,13}, \dots, K_{5,16}]$ bitlari uchun barcha 256 qiymatni ko'rib chiqish kerak. Agar qisman tahlil qilish yo'li bilan aniqlanadaigan oxirgi raunddagi kirish differensiali differential xarakteristikadan kutilgan qiymatga mos kelganda qisman maqsadli qismiy kalitning har bir qiymati uchun hisoblagichning qiymati bittaga oshiriladi. Eng katta qiymatga ega hisoblagich maqsadli qismiy kalit bitlari uchun to'g'ri bit qiymati hisoblanadi.

Shuni ham ta'kidlash kerakki, har bir shifrlangan matn juftligi uchun qisman tahlil qilishni amalga oshirish shart emas, chunki oxirgi raunddagi kirish differensiali faqat ikkita S blokka (S_{42} va S_{44} bloklar) ta'sir qiladi, ya'ni S_{41} va S_{43} bloklarda differensiallar nolga teng bo'lishi kerak. Mos S_{41} va S_{43} bloklariga kiruvchi differensiallari nolga teng bo'limgan ko'plab noto'g'ri juftliklarni tashlab yuborish orqali ularni filrlash mumkin. Chunki, shifrlangan matnlarning ushbu juftliklari shifrlangan matnning to'g'ri juftligiga mos kela olmaganligi bois, ular uchun $[\Delta U_{4,5}, \dots, \Delta U_{4,8}, \Delta U_{4,13}, \dots, \Delta U_{4,16}]$ shifrlangan matn differensiallarini o'rganish shart emas.

Tasodifiy yaratilgan qismiy kalitlardan foydalanib, 5000 ta ochiq matn/shifrlangan matn juftliklarini (ya'ni, $\Delta P = [0000101100000000]$) ga mos keladigan 10000 shifrlangan matn juftliklarini tanlab, shifr kalitiga hujum modellashtirildi va undan so'ng yuqorida bayon qilingan jarayon amalga oshirildi.

Maqsadli qismiy kalit kalit uchun to'g'ri qiymat $[K_{5,5} \dots K_{5,8}, K_{5,13} \dots K_{5,16}] = [0010,0100] = [2,4]_{\text{hex}}$ edi. Kutilganidek, hisoblagichning eng katta qiymati $[2,4]_{\text{hex}}$ ga to'g'ri keldi, bu esa hujumning muvaffaqiyatini tasdiqlaydi. 4.5-jadvalda qismiyi kalit hisoblagichlari uchun olingan ma'lumotlar jamlangan (to'liq ma'lumotlar 256 ta

ma'lumot elementini o'z ichiga oladi, maqsadli qismiy kalitning har bir qiymati uchun bittadan).

4.5-jadvalda qismiy kalitga nomzod uchun to'g'ri juftlik paydo bo'lishining taxminiy ehtimoli quyidagi formula bo'yicha hisoblangan

$$prob = count/5000,$$

bu erda *count* – berilgan qisman qismiy kalit necha marta paydo bo'lganligini anglatadi. Jadvaldagi natijalardan ko'rinib turibdiki, qiymatsh $[K_{5,5} \dots K_{5,8}, K_{5,13} \dots K_{5,16}] = [2,4]_{\text{hex}}$ bo'lgan qismiy kalit eng katta ehtimollikka ega.

Biz tahlil qilgan misolda to'g'ri juftlikning paydo bo'lish ehtimoli $P_D = 27/1024 = 0,0264$ ga teng va shuningdek, tajribaviy natijalariga ko'ra $P_D = 0,0244$ bo'lishini ko'rdik. Ba'zida noto'g'ri qismiy kalitlar uchun ham hisoblagichning katta qiymatlari hosil bo'lishi mumkin. Hisoblagichlarning qiymatlariga ta'sir qiluvchi bir nechta omillar mavjud, shuning uchun tajribaviy ma'lumotlar nazariy jihatdan olinganlaridan farq qiladi.

4.5-jadval. Tajribaviy natijalar.

<i>Qisman qismiy kalit [K_{5,5}...K_{5,8}, K_{5,13} ... K_{5,16}]</i>	<i>R_{rob} (Ehtimollik)</i>	<i>Qisman qismiy kalit [K_{5,5}...K_{5,8}, K_{5,13} ... K_{5,16}]</i>	<i>R_{rob} (Ehtimollik)</i>
1 S	0.0000	2 A	0.0032
1 D	0.0000	2 V	0.0022
1 E	0.0000	2 S	0.0000
1 F	0.0000	2 D	0.0000
2 0	0.0000	2 E	0.0000
2 1	0.0136	2 F	0.0000
2 2	0.0068	3 0	0.0004
2 3	0.0068	3 1	0.0000
2 4	0.0244	3 2	0.0004
2 5	0.0000	3 3	0.0004
2 6	0.0068	3 4	0.0000
2 7	0.0068	3 5	0.0004
2 8	0.0030	3 6	0.0000
2 9	0.0024	3 7	0.0008

§4.5. Differensial hujumming murakkabligi

Biz xarakteristikada ishtirok etadigan va nolga teng bo'lмаган kirish differensialiga (va natijada nolga teng bo'lмаган chiqish differensial iga) ega bo'лган S bloklarni *faol deb ataymiz*. Aytish mumkinki, faol S bloklar differensiallarining ehtimoli qanchalik katta bo'lsa, to'liq shifrnini tavsiflash differensial xarakteristikaning ehtimoli shunchalik katta bo'ladi. Bundan tashqari, faol S bloklar soni qanchalik kam bo'lsa, xarakteristikaning ehtimoli shunchalik katta bo'ladi.

Umuman olganda, kerakli tanlangan matn juftliklari sonini aniq aniqlash juda qiyin masala hisoblanadi. Shunga qaramay, qismiy kalit uchun nomzodlarni tanlashda to'g'ri juftliklarni ajratish uchun zarur bo'лган tanlangan matn juftliklari soni N_d quyidagicha aniqlanishi mumkin:

$$N_d \approx c / P_D,$$

bu erda P_D R raundli shifrning R-1 raundi differensial xarakteristikasining ehtimoli, c esa katta bo'lмаган o'згармас. Har bir faol S blokdagi differensial juftliklarning ehtimollikkari bir-biriga bog'liq emas deb deb faraz qilsak, u holda differensial xarakteristikaning ehtimolligi uchun quyidagiga ega bo'lish mumkin:

$$P_D = \prod_{i=1}^{\gamma} \beta_i,$$

bu erda faol S bloklar soni γ bilan ko'rsatilgan va xarakteristikaning i -chi faol S blokida ma'lum bir juft differensialning paydo bo'lish ehtimoli β_i bilan belgilangan. Ushbu formulaning o'rini ekanligini tekshirish oson. Bu shunchaki to'g'ri juftliklarning unchalik katta bo'lмаган sondagi paydo bo'lishi mos holda ularning hisoblagichlari maqsadli qismiy kalitning noto'g'ri qiymatlari hisoblagichlaridan ko'ra ancha katta qiymatga erishishini anglatadi. To'g'ri juftliklar taxminan har bir $1/P_D$ juftlik ehtimoli bilan yuzaga kelganligi sababli, amalda $1/P_D$ juftliklarining uncha katta bo'lмаган karralisidan foydalanish maqsadga muvofiq.

Differensial tahlilga nisbatan bardoshlikni yaratish uchun odatda differensiallarning ehtimolini minimallashtirish va faol S bloklar sonini maksimal

darajada oshiradigan tuzilmalarni topishga e'tibor qaratiladi. Shu nuqtai nazardan, Rijndael shifri differensial kriptotahlilga yuqori bardoshlilik bilan ishlab chiqilgan shifrning yaxshi namunasi hisoblanadi. Chiziqli kriptotahlilda bo'lgani kabi, differensial kriptotahlilga nisbatan "bardoshlilikni isbotlash" uchun ehtiyyot bo'lish kerak. Differensialarning xarakteristikalari ehtimolini hisoblash shifrning sodda modellarida ishtirok etuvchi S bloklarning mustaqilligiga, ya'ni bir-biri bilan bog'lanmaganligiga asoslanadi. Ammo, haqiqiy shifrlarda turli xil S bloklarning kirish ma'lumotlari o'rtasida bog'liqlik mavjud. Shunday qilib, P_D uchun hosil qilingan formula garchi amalda ko'pincha juda aniq bo'lib chiqsa-da, taxminiy ko'rsatkish hisoblanadi.

Nazorat savollari

1. SP tarmog'iga asoslangan shifrning asosiy xarakteristikalarini ayting.
2. SP tarmog'iga asoslangan shifrning har bir raundi qanday kriptografik akslantirish va almashtirishlardan iborat?
3. SP tarmog'iga asoslangan shifrda kalitlarni aralashtirish qanday amalga oshiriladi?
4. SP tarmog'iga asoslangan shifrning S bloklarini tavsiflang.
5. Differensialarning taqsimlanish jadvali deyilganda nima tushiniladi?
6. SP tarmog'iga asoslangan shifrda S blok differensialiga kalit bitlarining ta'siri qanday?
7. Differensial xarakteristikalar qanday quriladi?
8. SP tarmog'iga asoslangan shifrda ochiq matnning berilgan ΔP differensiali uchun ehtimollikning qiymati qanday hisoblanadi?
9. Nima differensial hujumni amalga oshirish imkonini beradi?
10. Qisman maqsadli qismiy kalitlar deb nimaga aytiladi?
11. Oxirgi raunddagi akslantirishlarni qisman tahlil qilish nimalardan iborat bo'ladi?

12. Differensial kriptotahlilda hisoblagichning qiymati qanday shakllantiriladi?

13. Qanday S bloklar faol deb nomlanadi?

14. Differensial kriptotahlilda qismiy kalit uchun nomzodlarni tanlashda to'g'ri juftliklarni ajratish uchun zarur bo'lgan tanlangan matn juftliklari soni N_d qanday aniqlanadi?

15. Differensial kriptotahlilda differensial xarakteristikaning ehtimolligi qanday hisoblanadi?

16. Differensial tahlilga nisbatan bardoshlikni yaratish uchun nimalarga e'tibor qaratiladi?

5-BOB. BLOKLI SHIFRLARNING CHIZIQLI KRIPTOTAHLILI

Kriptotahlilning ushbu turi statistik usul bo'lib, yapon kriptografi Misuru Masui tomonidan 1992 yilda taklif qilingan. M. Masui avval ushbu usulni A.Yamagishi bilan bиргаликда FEAL algoritmi uchun qo'llab ko'rdi. Undan so'ng, ya'ni 1993 yilda DES shifri kriptotahlili uchun tadqiq qildi [6].

Ushbu usul shifr matnga mos keluvchi ochiq matnni bilishga asoslangan bo'lib, unda shifrlash qurilmasidan yoki algoritmidan bitlarning konkret naborini o'tishini tahlil qilishdan foydalaniladi.

Chiziqli tahlil usulini biror bir shifrlash algoritmiga qo'llash uchun shifrlash algoritmi strukturasini bilish, shuningdek, bir necha ochiq matn hamda kriptoanalitikka noma'lum bo'lgan bir xil shifrlash kaliti bilan hosil qilingan shifrmatn hamda ularga mos keluvchi ochiq matnlar juftliklari statistikasiga ega bo'lish talab etiladi.

§5.1. Chiziqli tahlil usulining asosiy g'oyasi

Ushbu usulning mohiyati shifrni chiziqsiz almashtirish ko'rinishida ifodalovchi murakkab bulb funksiyalarini sodda chiziqli funksiya ko'rinishida ifodalashdan iborat. Buning natijasida hosil qilingan shifrni dastlabki shifrga nisbatan tahlil qilish soddalashadi. Shu bois, ayrim hollarda dastlabki shifrni kriptotahlil qilish masalasi uning soddalashtirilgan modifikasiyasini etarlicha aniqlikda kriptotahlil qilish masalasiga keltirish mumkin.

Chiziqli tahlil usulini qo'llashda asosiy qiyinchilik chiziqli yaqinlashishni topishdan iborat. Tahlil qilishda foydalaniladigan ochiq matn–shifr matn juftliklari hajmi topilgan chiziqli funksiya qanday ehtimollik bilan dastlabki shifrga yaqinlashishiga bog'liq. Odatda, tahlil qilishda foydalaniladigan ochiq matn–shifr matn juftliklari hajmi iloji boricha minimal bo'lishi talab etiladi.

Mavzuni bayon qilishda ikkining moduli bo'yicha ikkilik vektorlarni skalyar ko'paytirishda $\langle x, y \rangle = x_1y_1 \otimes \dots \oplus x_ny_n$ belgilashdan foydalaniladi.

Faraz qilaylik, r raundli blokli shifrlash algoritmi o'rganilayotgan bo'lsin. P, C, K - mos holda ochiq matn, shifr matn va shifrlash kaliti bo'lsin.

Shifrnning chiziqli yaqinlashishi deb, $1/2$ ehtimollikdan farqli ravishda $1/2 + \varepsilon$ ehtimollik bilan bajariladigan quyidagi ko'rinishdagi L munosabatga aytildi:

$$\langle P, \alpha \rangle \oplus \langle C, \beta \rangle = \langle K, \gamma \rangle. \quad (5.1)$$

ε miqdor chiziqli munosabatning salmog'i deyiladi. ε miqdor qiymatining qanchalik katta bo'lisi chiziqli tahlilning shunchalik muvaffaqiyatli bajarilishini anglatadi. Ayrim hollarda chiziqli yaqinlashish iborasi o'rniga chiziqli munosabat yoki chiziqli approksimasiya iboralari ham ishlatiladi.

Shunday qilib, chiziqli kriptotahlil usulining asisiy g'oyasi eng katta yoki kichik ehtimollik bilan bajariladigan (boshqacha aytganda, salmog'i yuqori bo'lgan) (5.1) ko'rinishidagi munosabatlarni aniqlashdan iborat.

Amalda bitta raund uchun salmog'i yuqori bo'lgan chiziqli yaqinlashishlarni topish mushkul masala hisoblanadi. To'liq raundli shufr uchun chizqli tahlilni amalga oshirish chiziqli munosabatlarni salmog'ini aniqlashni talab qiladi. Buning uchun Piling-up lemmasidan foydalanib, ehtimollikni yaqinlashtirish mumkin.

Piling-up lemmasi. Faraz qilaylik, turli raundlar uchun $p_i=1/2+\varepsilon_i$ $P = \frac{1}{2} P = \frac{1}{2}$ ehtimolliklar bilan qiymatlari 0 bo'lgan n ta $F_i (1 \leq i \leq n)$ chiziqli yaqinlashishlar topilgan bo'lsin. U holda Piling-up lemmasiga asosan $F_1 \oplus F_2 \oplus \dots \oplus F_n$ umumiyligi chiziqli yaqinlashishning qiymati 0 bo'lish ehtimoli quyidagiga teng bo'ladi:

$$P = 1/2 + \varepsilon, \quad (5.2)$$

bu yerda

$$\varepsilon = 2^{n-1} \prod_{i=1}^n \varepsilon_i.$$

Chiziqli kriptotahlil usuli quyida keltirilgan ikki bosqichda amalga oshiriladi:

1. ochiq matn, shifr matn va kalit bitlari o'rtasida katta ehtimollik bilan bajariladigan chiziqli yaqinlashish o'rnatish;

2. ma'lum bo'lgan ochiq matn-shifrmattn juftliklari va birinchi bosqichda qurilgan chiziqli munosabatdan foydalanib, kalit bitlarini aniqlash.

§5.2. Kalit bitlarini topish uchun chiziqli tahlilda qo'llaniladigan algoritmlar

Chiziqli yaqinlashish qurilgandan so'ng ochiq matn-shifr matn juftliklaridan foydalanib, kalitning ayrim bitlarini topish mumkin bo'ladi. Buning uchun salmog'i yuqori bo'lgan chiziqli yaqinlashishlardan foydalanish lozim. Ushbu paragrafda kalitning ayrim bitlarini topishning ikkita algoritmi keltiriladi.

Shifrlash kalitining bitta bitini aniqlash algoritmi.

Bitta chiziqli yaqinlashishdan foydalanib, shifrlash kalitining bitta bitini aniqlash algoritmi quyida keltirilgan qadamlardan tashkil topgan:

1-qadam. Ochiq matn, shifr matn va shifrlash kaliti bitlari uchun $1/2$ ehtimollikdan sezilarli farqlanuvchi, $p = 1/2 + \varepsilon$ ehtimollik bilan bajariladigan L chiziqli munosabat topilsin.

2-qadam. Ochiq matnlar va fiksirlangan, noma'lum K shifrlash kaliti asosidagi ularga mos keluvchi shifr matnlari N ta juftliklarining statistikasi to'plansin. To'plangan statistika va ε miqdorning ishorasi asosida ushbu noma'lum K shifrlash kaliti uchun L chiziqli munosabatning bajarilishi yoki bajarilmasligi, ya'ni quyidagilar tekshirilsin:

- Statistikating har bir $\langle P, C \rangle$ juftligi uchun L chiziqli munosabatning chap qismi hisoblansin. N_0, N_1 - mos holda L chiziqli munosabatning chap qismi nol va bir bo'lgan statistikadagi juftliklar soni bo'lsin, ya'ni $N_0 + N_1 = N$.

$$\bullet \langle K, \gamma \rangle = \begin{cases} 0, agar(N_0 - N_1) \cdot \varepsilon > 0 bo'lsa; \\ 1 aksinc\u00e1. \end{cases}$$

- Hosil bo'lgan ma'lumotlar asosida shifrlash kaliti tanlanadi.

Natijada K shifrlash kaliti bitlari uchun yangi ehtimolli munosabat o'rnatiladi. Bu munosabatdan bitta bitni aniqlash mumkin. Ochiq matn va shifr matn juftliklarining bitta statistikasi va shifrnning har hil chiziqli yaqinlashishlaridan foydalanib, bir necha shunday munosabatlar o'rnatish mumkin.

Ammo, bitta chiziqli yaqinlashishdan foydalanib, shifrlash kalitining bir necha bitlarini aniqlash imkonini beruvchi chiziqli tahvilning quyida keltirilgan mukammallashtirilgan varianti amaliyatga keng qo'llanilmoqda.

Shifrlash kalitining bir necha bitlarini aniqlash algoritmi.

Faraz qilaylik, $C_i (i = 0, 1, \dots, r)$ oraliq shifrmatnni ifodalasin. U holda $C_0 = P, C_r = C$.

1-qadam. Oraliq C_1, C_{r-1} shifr matnlari va shifrlash kaliti bitlari uchun $1/2$ ehtimollikdan sezilarli farqlanuvchi, $p = 1/2 + \varepsilon'$ ehtimollik bilan bajariladigan L' chiziqli munosabat topilsin. ε' miqdor L' chiziqli munosabatning nazariy salmog'i deyiladi. L' chiziqli munosabat quyidagi ko'rinishda bo'lsin:

$$\langle a, C_1 \rangle \oplus \langle b, C_{r-1} \rangle = \langle d, K \rangle.$$

Ushbu munosabatning chap qismi faqatgina shifr matn bitlariga bog'liq, shifrlash kalitiga bog'liq emas.

2-qadam. Ochiq matnlar va fiksirlangan, noma'lum K shifrlash kaliti asosidagi ularga mos keluvchi shifr matnlarning N ta juftliklari statistikasi to'plansin. Ushbu juftliklar quyidagilar bo'lsin:

$$(P^{(1)}, C^{(1)}), \dots, (P^{(N)}, C^{(N)}).$$

3-qadam. Ma'lum bo'lgan P ochiq matn foydalanib, $\langle a, C_1 \rangle$ chiziqli munosabatni qiymatini aniqlash imkonini beruvchi K shifrlash kalitining minimal qismi K' bilan belgilansin. K' qism K shifrlash kalitining aynan qaysi bitlaridan tashkil topganligini aniqlash uchun shifrlashning birinchi raundini tahlil qilish etarli. Buning uchun koeffisientlari noldan farqli $\langle a, C_1 \rangle$ chiziqli munosabatda ishtirok

etuvchi C_1 shifr matnning bitlari shifrlash kalitining aynan qaysi bitlariga sezilarli darajada bog'liqligini aniqlash lozim bo'ladi.

Xuddi shuningdek, ma'lum bo'lgan C shifr matn foydalanib, $\langle b, C_{r-1} \rangle$ chiziqli munosabatni qiymatini bir qiymatli aniqlash imkonini beruvchi K shifrlash kalitining minimal qismi K'' bo'lsin.

Shifrlash kalitining $K' \cup K''$ qismiga kiruvchi bitlari *faol (ayrim hollarda samarali) bitlari deyiladi*.

4-qadam. Shifrlash kalitining $K' \cup K''$ qismi bo'yicha bo'lishi mumkin bo'lgan variantlarini saralash lozim. Har bir fiksirlangan $K' \cup K''$ qism bo'yicha quyidagilarni amalga oshirish lozim.

- K', K'' qismlardan foydalanib, har bir $(P^{(i)}, C^{(i)})$ juftlik uchun $\langle a, C_1 \rangle \oplus \langle b, C_{r-1} \rangle$ munosabatni qiymati hisoblansin. Faraz qilaylik, ochiq matn va shifr matnlarning N ta juftliklaridan N_0 ta juftliklari uchun ushbu qiymatlar nol, N_1 ta juftliklari uchun ushbu qiymatlar bir bo'lsin, ya'ni $N_0 + N_1 = N$.

- $1/2 + \bar{\varepsilon} = N_0/N_1$ tenglik bilan aniqlanadigan chiziqli munosabatni *tajribaviy salmog'i $\bar{\varepsilon}$ ning qiymati* hisoblansin.

5-qadam. Chiziqli munosabatning tajribaviy salmog'i $\bar{\varepsilon}$ nazariy salmog'i ε' dan keskin farq qiluvchi shifrlash kalitining $K' \cup K''$ qismi noto'g'ri qismlar deb hisoblansin. Shifrlash kalitining qolgan qismi to'g'ri qismlar deb hisoblansin va massiv ko'rinishida saqlansin. Odatda, ushbu algoritm bilan ishslashda chiziqli munosabat salmoqlarining tafovutlari ma'lum bir δ aniqlik bilan hisoblanadi. Agar $|\varepsilon' - \bar{\varepsilon}| \leq \delta$ o'rinali bo'lsa $K' \cup K''$ qism to'g'ri, aks holda noto'g'ri qismlar deb hisoblanadi.

6-qism. K shifrlash kalitining har bir to'g'ri qismlari $K' \cup K''$ uchun K kalitning qolgan bitlarini saralash yo'li bilan tiklash lozim.

2-algoritmnинг асосиј ўтуғ'и шундаки, битта чизиqli munosabatdan foydalanib, K shifrlash kalitining bitlar guruhini tiklash mumkin.

§5.3. «Oddiylikdan murakkablikga» tamoyilini chiziqli tahlilda qo'llanilishi

Chiziqli tahlilning murakkabligi shifrning katta salmoqqa ega bo'lgan chiziqli yaqinlashishi

$$\langle P, \alpha \rangle \oplus \langle C, \beta \rangle = \langle K, \gamma \rangle$$

ni topishning qiyinchiligi bilan izohlanadi. Umuman olganda, α , β , γ vektorlarning bo'lishi mumkin bo'lган barcha qiymatlarini ko'rib chiqish va har bir chiziqli munosabatning bajarilish ehtimolligini alohida aniqlash lozim. Bu esa katta hisoblash resursini talab qiladi. Shuningdek, chiziqli munosabatning bajarilish ehtimolligini hisoblash algoritmi ham noma'lum. Shu sababli amalda shifrning uncha katta bo'lмаган alohida qismlarini, masalan S bloklarini tahlil qilish va bosqichma-bosqich butun shifrni yaqinlashishiga o'tish orqali o'rganilayotgan shifr uchun chiziqli yaqinlashish hosil qilinadi. Ushbu tamoyilni «oddiylikdan murakkablikga» deb atash mumkin.

5.1-jadval. S blokning chiziqli salmoqlilik jadvali.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	+8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	-2	-2	0	0	-2	+6	+2	+2	0	0	+2	+2	0	0
2	0	0	-2	-2	0	0	-2	-2	0	0	+2	+2	0	0	-6	+2
3	0	0	0	0	0	0	0	+2	-6	-2	-2	+2	+2	-2	-2	-2
4	0	+2	0	-2	-2	-4	-2	0	0	-2	0	+2	+2	-4	+2	0
5	0	-2	-2	0	-2	0	+4	+2	-2	0	-4	+2	0	-2	-2	0
6	0	+2	-2	+4	+2	0	0	+2	0	-2	+2	+4	-2	0	0	-2
7	0	-2	0	+2	+2	-4	+2	0	-2	0	+2	0	+4	+2	0	+2
8	0	0	0	0	0	0	0	0	-2	+2	+2	-2	+2	-2	-6	-6
9	0	0	-2	-2	0	0	-2	-2	-4	0	-2	+2	0	+4	+2	-2
a	0	+4	-2	+2	-4	0	+2	-2	+2	+2	0	0	+2	+2	0	0
b	0	+4	0	-4	+4	0	+4	0	0	0	0	0	0	0	0	0
c	0	-2	+4	-2	-2	0	+2	0	+2	0	+2	+4	0	+2	0	-2
d	0	+2	+2	0	-2	+4	0	+2	-4	-2	+2	0	+2	0	0	+2
e	0	+2	+2	0	-2	-4	0	+2	-2	0	0	-2	-4	+2	-2	0
f	0	-2	-4	-2	-2	0	+2	0	0	-2	+4	-2	-2	0	+2	0

Faraz qilaylik, r raundli blokli shifrlash algoritmi berilgan bo'lsin. Raund funksiyalarida o'rniga qo'yish (S bloklar) va o'rinni almashtirish (P bloklar) dan foydalanilsin.

Misol. Faraz qilaylik, shifrda kirishda 4 bitni qabul qilib, 4 bit chiqadigan S-blok foydalanilsin (o'n otilik sanoq tizimida): $[e, 4, d, 1, 2, f, b, 8, 3, a, 6, c, 5, 9, 0, 7]$. Har bir S-blok uchun chiziqli salmoqlilikni ko'rib chiqamiz.

S blokka kirish va chiqish mos holda $x = (x_1, x_2, x_3, x_4)$ va $y = (y_1, y_2, y_3, y_4)$ bilan belgilansin. *S blok uchun chiziqli salmoqlilik jadvali deb shunday jadvalga aytildiki*, bu jadvalning u usatri va v ustuni kesishishida shunday λ soni topiladi, ushbu son uchun $u \cdot x = v \cdot y$ munosabat $(8 + \lambda)/16$ ehtimollik bilan bajariladi. Masalan, $o \cdot x = 0 \cdot y$ munosabat kirish x ning ixtiyoriy qiymatida bajariladi. Shu sababli chiziqli salmoqlilik jadvalida nol satri kesishishida +8 turibdi.

$6 \cdot x = 3 \cdot y$ $6 \cdot x = 3 \cdot y$ munosabatni qaraymiz. Ikkilik sanoq tizimidan foydalanamiz: $6 = (0110)_2$, $3 = (0011)_2$. U holda ushbu munosabat quyidagi ko'rinishga keladi: $x_2 \oplus x_3 = y_3 \oplus y_4$. S blokka kiruvchi va undan chiquvchi 16 ta juftlikda ushbu munosabatni bajarilishini tekshirib, undan 12 ta juftlikda bajarilishini ko'rish mumkin. Demak, salmoqlilik jadvalida mos qiymat $\lambda = +4$ ga teng (5.1-jadval). Xuddi shuningdek, boshqa chiziqli munosabatlar uchun ham chiziqli salmoqlilik jadvalidagi λ sonining qiymatini topish mumkin.

§5.4. DES shifrlash algoritmi uchun chiziqli munosabatlar qurish

DES shifrlash algoritmiga chiziqli kriptotahlini qo'llash uchun S bloklarning eng yaxshi yaqinlashishlarini tanlab, shifr raund funksiyasining yaqinlashishini qurish lozim. Buning uchun DES shifrlash algoritmi 5-chi S-blokinini ko'ramiz. Ushbu blokda

$$x_2 = y_1 \oplus y_2 \oplus y_3 \quad (5.3)$$

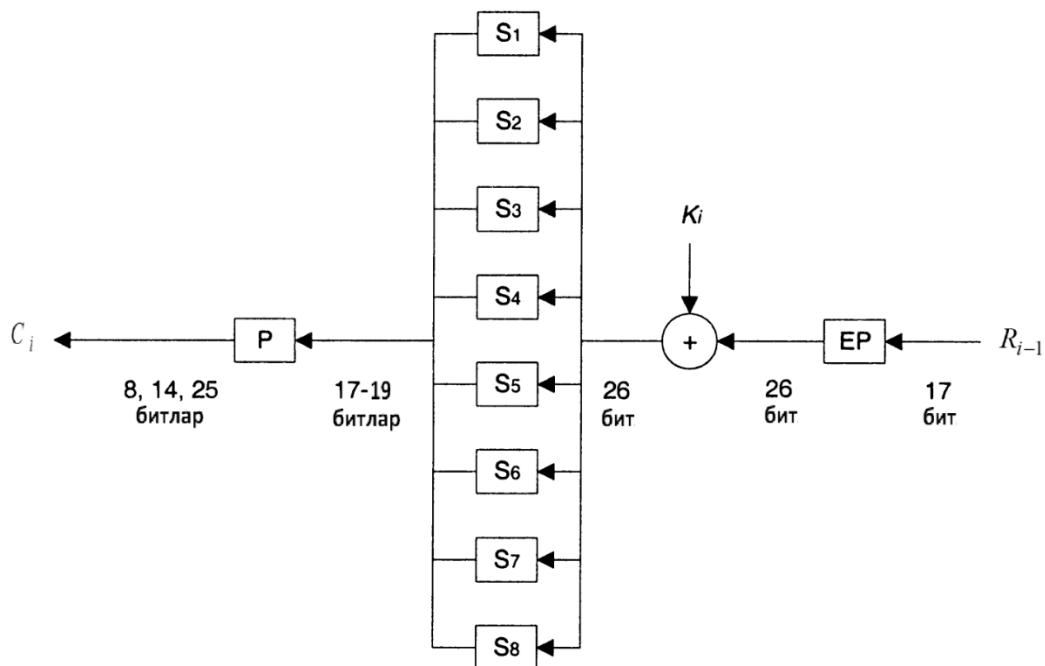
chiziqli munosabat $42/64$ ehtimollik bilan bajariladi. i -chi raundni ko'rib chiqaylik (5.2-jadval). DES shifrlash algoritmi shifrlash funksiyasiga ko'ra (5.3) munosabatni quyidagicha talqin qilish mumkin:

$$w_{26} = z_{17} \oplus z_{18} \oplus z_{19}. \quad (5.4)$$

Bu erda w, z mos holda uzunliklari 48 va 32 bitlardan iborat bo'lgan 5-chi S blokka kiruvchi va undan chiquvchi vektorlardir (5.1-rasm). S blokka kiruvchi w vektor raundga kiruvchi kengaytirilgan (48 bitgacha) R_{i-1} R_{i-1} massivning va raund kaliti K_i ning 2 modul bo'yicha yig'indisi ekanligini e'tiborga olamiz. U holda 5-chi S-blokka kiruvchi x_2 (2-chi), ya'ni (2) tenglikdagi w_{26} -chi bit raundga kiruvchi dastlabki 17-chi bit va raund kaliti 26-chi bitining 2 modul bo'yicha yig'indisidir:

$$w_{26} = R_{i-1}[17] \otimes K_i[26],$$

bu erda kvadrat qavs ichidagi sonlar bitlarning massivlardagi joylashish pozisiyalarini anglatadi. Boshqa tomondan olganda, z_{17}, z_{18}, z_{19} bitlar almashtiruvchi P-blokdan o'tgandan so'ng, $f(R_{i-1}, k_i)$ shifrlash funksiyasining mos holda 8,14,25 bitlariga aylanadi. Shunday qilib, $42/64$ ehtimollik bilan bajariladigan, DES shifrlash algoritmi raund funksiyasining quyidagi chiziqli yaqinlashishini hosil qilish mumkin: $R_{i-1}[17] \oplus K_i[26] = f(R_{i-1}, K_i)$.



5.1-rasm. DES algoritmi uchun nisbatan samarali bo'lgan bir raundli munosabat.

**5.2-jadval. S₅-blok kirish-chiqish juftliklari uchun
 $x_2=y_1 \oplus y_2 \oplus y_3$ chiziqli munosabatni bajarilishi.**

i S(i,j)	Значения j														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
2	36	30	34	30	34	28	32	36	32	34	30	34	30	32	28
3	32	30	38	30	30	36	28	32	32	30	38	30	30	36	28
4	34	30	32	32	34	30	32	32	34	34	36	28	30	30	32
5	34	34	28	32	42	26	28	32	34	22	32	36	30	34	36
6	30	28	26	30	28	34	32	32	30	32	30	26	24	34	32
7	34	32	34	30	40	38	32	28	38	32	26	30	32	26	28
8	32	34	38	32	32	30	26	30	34	36	20	34	38	28	36
9	28	38	30	32	28	26	26	38	30	32	28	34	26	24	28
10	36	32	32	30	26	34	34	34	34	30	34	36	28	28	32
11	36	36	36	38	34	30	30	30	30	30	34	32	24	28	32
12	34	32	30	32	34	36	42	30	36	30	24	30	36	26	28
13	38	32	34	32	30	36	22	30	32	30	36	30	40	26	32
14	30	30	32	30	36	32	34	30	32	36	34	28	38	30	28
15	30	30	40	38	36	32	34	34	36	40	30	40	26	34	32
16	34	30	32	32	30	26	24	32	30	30	28	32	34	42	12
17	34	30	32	36	34	30	28	36	34	34	32	24	26	34	36
18	30	32	30	34	28	30	24	36	38	36	38	30	36	26	32
19	26	32	34	30	36	34	32	36	26	36	34	26	36	30	32
20	35	28	32	32	32	32	32	28	28	36	36	32	36	28	32
21	35	32	28	28	36	24	24	32	32	28	36	40	36	32	36
22	32	38	38	34	30	36	32	36	32	38	34	34	34	32	32
23	36	26	30	38	30	28	36	36	28	26	34	30	34	32	36
24	38	32	34	36	22	28	34	34	32	30	32	34	36	30	28
25	34	36	26	32	30	36	30	38	40	38	36	42	32	34	28
26	34	34	24	30	36	32	34	30	32	36	34	32	30	30	32
27	34	38	28	26	32	32	34	38	40	32	30	28	26	30	32
28	32	30	34	36	32	26	34	30	38	28	32	34	30	32	32
29	36	30	38	24	32	30	34	42	30	24	24	34	34	32	36
30	28	24	32	30	30	30	34	30	34	30	38	36	36	36	32
31	28	40	24	34	26	26	30	30	34	30	30	24	32	32	28
32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
33	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
34	28	30	34	30	34	28	40	28	32	26	38	34	30	16	20

**5.2-jadval (davomi). S₅-blok kirish-chiqish juftliklari uchun
 $x_2 = y_1 \oplus y_2 \oplus y_3$ munosabatni bajarilishi.**

35	32	30	30	38	30	28	36	32	32	30	30	30	38	36	28
36	30	38	36	32	38	30	36	36	26	30	36	32	46	34	32
37	38	34	32	32	38	34	32	28	26	34	24	32	30	38	28
38	34	36	30	30	32	34	28	36	30	28	30	38	32	30	32
39	22	32	30	38	36	38	28	32	38	20	34	34	32	38	28
40	36	30	30	32	36	26	34	34	26	36	32	38	30	28	32
41	32	34	38	32	32	38	34	34	30	24	32	30	26	32	32
42	32	28	24	38	38	38	26	38	34	30	30	24	36	28	36
43	40	32	36	38	30	26	38	34	38	30	38	28	32	36	36
44	34	36	26	32	26	32	38	30	28	34	28	30	36	38	32
45	30	28	30	32	30	24	34	30	32	26	24	30	32	30	36
46	38	34	28	38	36	36	30	22	24	32	30	36	30	34	32
47	38	26	28	38	28	36	30	34	36	36	26	32	34	30	28
48	34	30	32	28	26	30	28	36	34	34	32	32	34	34	36
49	34	30	32	32	30	34	32	32	30	30	28	32	34	34	36
50	38	32	30	30	40	34	36	32	42	32	34	30	36	34	32
51	26	32	42	34	32	30	28	32	38	32	22	34	36	30	32
52	32	20	36	28	32	36	24	28	32	28	32	28	28	32	32
53	24	32	32	40	28	36	32	32	28	28	32	36	36	28	36
54	36	30	26	30	30	40	32	36	28	30	30	38	34	28	32
55	24	26	26	26	38	32	36	44	32	34	30	34	34	36	28
56	34	36	26	32	30	36	30	26	36	26	32	38	36	30	32
57	30	40	34	28	38	28	26	30	28	34	36	30	32	34	32
58	38	22	32	34	36	32	30	38	28	32	34	36	30	30	28
59	30	26	28	22	32	24	30	22	36	36	30	32	34	30	36
60	24	26	30	32	28	34	34	26	34	36	32	42	30	36	36
61	36	34	34	36	36	30	34	30	42	32	32	34	34	36	32
62	28	35	28	34	34	30	34	34	30	30	30	36	28	32	36
63	28	28	28	46	38	26	30	34	30	38	30	32	32	28	32

3-bobning 3.8-jadvalda DES shifrining har bir S bloki uchun kirish va chiqishlarning mosligi keltirilgan. Ushbu jadvaldan foydalanib, $x_4=y_2 \oplus 1$ chiziqli yaqinlashishning S₁ bloki uchun bajarilish ehtimolligi 34/64 ga tenglilgini aniqlaghn mumkin. Natijda yana bitta $x_4=y_2 \oplus 1$ chiziqli munosabat hosil qilindi. Tahlil natijalari 5.3-jadvalda keltirilgan.

**5.3-jadval. DES shifrining S₁ bloki uchun
 $x_4=y_2 \oplus 1$ munosabatning bajarilishi.**

$x_1x_2x_3x_4x_5x_6$	x_4	y_2	$y_1y_2y_3y_4$
0 000 0 00	0	1	1 1 10
1 000 0 01	0	0	0 0 00
2 000 0 10	0	0	0 0 11
3 000 0 11	0	1	1 1 11
4 000 1 00	1	1	1 1 01
5 000 1 01	1	1	0 1 11
6 000 1 10	1	0	0 0 01
7 000 1 11	1	1	0 1 00
8 001 0 00	0	0	0 0 10
9 001 0 01	0	1	1 1 10
10 001 0 10	0	1	1 1 11
11 001 0 11	0	0	0 0 10
12 001 1 00	1	0	1 0 11
13 001 1 01	1	1	1 1 01
14 001 1 10	1	0	1 0 00
15 001 1 11	1	0	0 0 01
16 010 0 00	0	0	0 0 11
17 010 0 01	0	0	1 0 10
18 010 0 10	0	0	1 0 10
19 010 0 11	0	1	0 1 10
20 010 1 00	1	1	0 1 10
21 010 1 01	1	1	1 1 00
22 010 1 10	1	1	1 1 00
23 010 1 11	1	0	1 0 11
24 011 0 00	0	1	0 1 01
25 011 0 01	0	0	1 0 01
26 011 0 10	0	0	1 0 01
27 011 0 11	0	1	0 1 01
28 011 1 00	1	0	0 0 00
29 011 1 01	1	0	0 0 11
30 011 1 10	1	1	0 1 11
31 011 1 11	1	0	1 0 00
32 100 0 00	0	1	0 1 00
33 100 0 01	0	1	1 1 11
34 100 0 10	0	0	0 0 01
35 100 0 11	0	1	1 1 00
36 100 1 00	1	1	1 1 10
37 100 1 01	1	0	1 0 00
38 100 1 10	1	0	1 0 00
39 100 1 11	1	0	0 0 10
40 101 0 00	0	1	1 1 01
41 101 0 01	0	1	0 1 00

42 101 0 10	0	1	0 1 10
43 101 0 11	0	0	1 0 01
44 101 1 00	1	0	0 0 10
45 101 1 01	1	0	0 0 01
46 101 1 10	1	0	1 0 11
47 101 1 11	1	1	0 1 11
48 110 0 00	0	1	1 1 11
49 110 0 01	0	1	0 1 01
50 110 0 10	0	1	1 1 00
51 110 0 11	0	0	1 0 11
52 110 1 00	1	0	1 0 01
53 110 1 01	1	0	0 0 11
54 110 1 10	1	1	0 1 11
55 110 1 11	1	1	1 1 10
56 111 0 00	0	0	0 0 11
57 111 0 01	0	0	1 0 10
58 111 0 10	0	0	1 0 10
59 111 0 11	0	0	0 0 00
60 111 1 00	1	1	0 1 01
61 111 1 01	1	1	0 1 10
62 111 1 10	1	0	0 0 00
63 111 1 11	1	1	1 1 01

Xuddi shunga o'xshash, DES shifrinng S₅ bloki uchun $x_2=y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus 1$ chiziqli munosabat 52/64 ehtimollik o'rini bo'lishini aniqlash mumkin va buning natijasida yuqori ehtimollik bilan bajariladigan yana bitta chiziqli munosabat qurildi. Tahlil natijalari 5.4-jadvalda keltirilgan.

5.4-jadval. DES shifrinning S₅ bloki uchun chiziqli munosabatning bajarilishi.

$x_1x_2x_3x_4x_5x_6$	x_2	$x_2=y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus 1$	$y_1y_2y_3y_4$
0 0 0 0000	0	1	0010
1 0 0 0001	0	1	1110
2 0 0 0010	0	0	1100
3 0 0 0011	0	1	1011
4 0 0 0100	0	1	0100
5 0 0 0101	0	1	0010
6 0 0 0110	0	1	0001
7 0 0 0111	0	0	1100
8 0 0 1000	0	1	0111
9 0 0 1001	0	1	0100
10 0 0 1010	0	0	1010

11 0 0 1011	0		1		0111
12 0 0 1100	0		1		1011
13 0 0 1101	0		1		1101
14 0 0 1110	0		0		0110
15 0 0 1111	0		1		0001
16 0 1 0000	1		1		1000
17 0 1 0001	1		0		0101
18 0 1 0010	1		0		0101
19 0 1 0011	1		0		0000
20 0 1 0100	1		0		0011
21 0 1 0101	1		0		1111
22 0 1 0110	1		0		1111
23 0 1 0111	1		0		1010
24 0 1 1000	1		1		1101
25 0 1 1001	1		0		0011
26 0 1 1010	1		0		0000
27 0 1 1011	1		0		1001
28 0 1 1100	1		1		1110
29 0 1 1101	1		1		1000
30 0 1 1110	1		0		1001
31 0 1 1111	1		0		0110
32 1 0 0000	0		1		0100
33 1 0 0001	0		1		1011
34 1 0 0010	0		1		0010
35 1 0 0011	0		1		1000
36 1 0 0100	0		1		0001
37 1 0 0101	0		0		1100
38 1 0 0110	0		1		1011
39 1 0 0111	0		1		0111
40 1 0 1000	0		0		1010
41 1 0 1001	0		1		0001
42 1 0 1010	0		1		1101
43 1 0 1011	0		1		1110
44 1 0 1100	0		1		0111
45 1 0 1101	0		1		0010
46 1 0 1110	0		1		1000
47 1 0 1111	0		1		1101
48 1 1 0000	1		0		1111
49 1 1 0001	1		0		0110
50 1 1 0010	1		0		1001
51 1 1 0011	1		0		1111
52 1 1 0100	1		0		1100
53 1 1 0101	1		0		0000
54 1 1 0110	1		0		0101
55 1 1 0111	1		0		1001

56 1 1 1000	1	0	0110
57 1 1 1001	1	0	1010
58 1 1 1010	1	0	0011
59 1 1 1011	1	1	0100
60 1 1 1100	1	0	0000
61 1 1 1101	1	0	0101
62 1 1 1110	1	1	1110
63 1 1 1111	1	0	0011

§5.5. DES shifrlash algoritmi chiziqli kriptotahlili

5.4-paragrafda katta ehtimollik bilan yaqinlashuvchi ychta chiziqli munosabat qurildi. Endi bevosita kalitning ayrim bitlarini topishga kirishish mumkin. Misuru Masui chiziqli tahlilni DES shifrlash algoritmiga qo'llashda 2-algoritmdan foydalangan va u quyidagicha ish tutgan [1,6]. DES algoritmining 14 ta raundi (birinchi va oxirgi raunddan tashqari) uchun L' chiziqli yaqinlashish qurgan. Ma'lum bo'lgan ochiq va shifr matn juftliklaridan L' chiziqli munosabatning chap qismini topish imkonini beruvchi 12 ta aktiv bitlar aniqlangan. Undan so'ng chiziqli tahlil parallel ravishda 2^{12} marta bajarilgan va shifrlash kaliti aktiv bitlar guruhining to'g'ri qiymatlari 2-algoritm bo'yicha aniqlanadi. Undan tashqari chiziqli munosabatning o'zidan kalitning 13-chi biti aniqlangan. Ushbu prosedura ochiq va shifrmatnlarni birinchi marta almashtirgandan so'ng hosil bo'ladigan chiziqli munosabatga nisbatan qo'llanilgan. Natijada shifrlash kalitining yana 13-chi biti aniqlangan. Shifrlash kalitining qolgan 30 ta biti to'liq saralash usuli bilan aniqlangan.

DES shifrlash algoritmi uchun chiziqli yaqinlashish. «Oddiylikdan murakkablikga» tamoyili asosida chiziqli yaqinlashishni aniqlash uchun S bloklarining quyidagi chiziqli yaqinlashishlaridan foydalanilgan:

S-blok	Munosabat	Ehtimolligi
S_5	$x_2 = y_1 \oplus y_2 \oplus y_3$	42/64
S_1	$x_4 = y_2 \oplus 1$	34/64
S_5	$x_2 = y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus 1$	52/64

Avval DES shifri raund funksiyalari uchun yaqinlashishlar qurish uchun har bir munosabat «oddiylikdan murakkablikga» tamoyili asosida foydalilanadi. Raund funksiyalarini chuqur tahlil qilib, quyidagi yaqinlashishlarni qurish mumkin.

Chiziqli munosabat	Ehtimolligi
$R_{i-1}[17] \oplus f(R_{i-1}, K_i)[8,14,25] = K_i[26]$	42/64
$R_{i-1}[3] \oplus f(R_{i-1}, K_i)[17] = K_i[4]$	34/64
$R_{i-1}[17] \oplus f(R_{i-1}, K_i)[8,14,25,3] \oplus 1$ $= K_i[26]$	52/64

Ushbu munosabatlar yordamida 14 raundli DES shifri yaqinlashishining maxsus sxemasini quramiz. Jadvaldagi barcha chiziqli munosabatlarni qo'shganimizdan keyin ikkinchi raunddan boshlab, to o'n beshinchi raundgacha chiziqli yaqinlashishni hosil qilamiz.

$$\begin{aligned}
R_1[8,14,25] \oplus L_{15}[17] \oplus R_{15}[8,14,25,3] &= K_3[26] \oplus K_4[4] \oplus K_5[26] \oplus \\
&\oplus K_7[26] \oplus K_8[4] \oplus K_9[26] \oplus K_{11}[26] \oplus K_{12}[4] \oplus K_{13}[26] \oplus K_{15}[26]. \quad (5.5) \\
&\oplus K_7[26] \oplus K_8[4] \oplus K_9[26] \oplus K_{11}[26] \oplus K_{12}[4] \oplus K_{13}[26] \oplus K_{15}[26].
\end{aligned}$$

Bu munosabatlar pilling-up lemmasiga asosan quyidagi ehtimollik bilan bajariladi:

$$\frac{1}{2} + 2^9 \cdot \frac{10}{64} \cdot \frac{2}{64} \cdot \frac{20}{64} \cdot \frac{20}{64} \cdot \frac{2}{64} \cdot \frac{10}{64} \cdot \frac{10}{64} \cdot \frac{2}{64} \cdot \frac{20}{64} \cdot \frac{20}{64} = \frac{1}{2} + \frac{5^7}{2^{37}} \approx 0,50000057.$$

Chiziqli munosabatning salmog'i $\varepsilon' = 0,0000057$.

Chiziqli munosabat	P
$R_1[8, 14, 25] = L_2[8, 14, 25]$	1
$R_2[17] \oplus F(R_2, K_3)[8, 14, 25] = K_3[26]$	42/64
$L_2[8, 14, 25] \oplus F(R_2, K_3)[8, 14, 25] = R_3[8, 14, 25]$	1
$R_2[17] = L_3[17]$	1
$R_3[3] \oplus F(R_3, K_4)[17] \oplus 1 = K_4[4]$	34/64
$L_3[17] \oplus F(R_3, K_4)[17] = R_4[17]$	1
$R_3[8, 14, 25, 3] = L_4[8, 14, 25, 3]$	1
$R_4[17] \oplus F(R_4, K_5)[8, 14, 25, 3] \oplus 1 = K_5[26]$	52/64
$L_4[8, 14, 25, 3] \oplus F(R_4, K_5)[8, 14, 25, 3] = R_5[8, 14, 25, 3]$	1
$R_5[8, 14, 25, 3] = L_6[8, 14, 25, 3]$	1
$R_6[17] \oplus F(R_6, K_7)[8, 14, 25, 3] \oplus 1 = K_7[26]$	52/64
$L_6[8, 14, 25, 3] \oplus F(R_6, K_7)[8, 14, 25, 3] = R_7[8, 14, 25, 3]$	1
$R_6[17] = L_7[17]$	1
$R_7[3] \oplus F(R_7, K_8)[17] \oplus 1 = K_8[4]$	34/64
$L_7[17] \oplus F(R_7, K_8)[17] = R_8[17]$	1
$R_7[8, 14, 25] = L_8[8, 14, 25]$	1
$R_8[17] \oplus F(R_8, K_9)[8, 14, 25] = K_9[26]$	42/64
$L_8[8, 14, 25] \oplus F(R_8, K_9)[8, 14, 25] = R_9[8, 14, 25]$	1
$R_9[8, 14, 25] = L_{10}[8, 14, 25]$	1
$R_{10}[17] \oplus F(R_{10}, K_{11})[8, 14, 25] = K_{11}[26]$	42/64
$L_{10}[8, 14, 25] \oplus F(R_{10}, K_{11})[8, 14, 25] = R_{11}[8, 14, 25]$	1
$R_{10}[17] = L_{11}[17]$	1
$R_{11}[3] \oplus F(R_{11}, K_{12})[17] \oplus 1 = K_{12}[4]$	34/64
$L_{11}[17] \oplus F(R_{11}, K_{12})[17] = R_{12}[17]$	1
$R_{11}[8, 14, 25, 3] = L_{12}[8, 14, 25, 3]$	1
$R_{12}[17] \oplus F(R_{12}, K_{13})[8, 14, 25, 3] \oplus 1 = K_{13}[26]$	52/64
$L_{12}[8, 14, 25, 3] \oplus F(R_{12}, K_{13})[8, 14, 25, 3] = R_{13}[8, 14, 25, 3]$	1
$R_{13}[8, 14, 25, 3] = L_{14}[8, 14, 25, 3]$	1
$R_{14}[17] \oplus F(R_{14}, K_{15})[8, 14, 25, 3] \oplus 1 = K_{15}[26]$	52/64
$L_{14}[8, 14, 25, 3] \oplus F(R_{14}, K_{15})[8, 14, 25, 3] = R_{15}[8, 14, 25, 3]$	1
$R_{14}[17] = L_{15}[17]$	1

5.2-rasm. DES algoritmi uchun 14 raundli yaqinlashish sxemasi.

Ma'lumki, DES shifrining kirishiga C shifr matn berilsa va kalitlardan teskari tartibda (ya'ni, avval k_{16} , so'ng k_{15} va h.k.) foydalanilsa, u holda algoritmning chiqishiga P ochiq matn paydo bo'ladi. DES shifrining ushbu xossasiga ko'ra (5.5) tenglikdan yana bitta munosabat hosil bo'ladi:

$$\begin{aligned}
 L_{15}[8, 14, 25] \oplus R_1[17] \oplus L_1[8, 14, 25, 3] &= K_{14}[26] \oplus K_{13}[4] \oplus K_{12}[26] \oplus \\
 &\oplus K_{10}[26] \oplus K_9[4] \oplus K_8[26] \oplus K_6[26] \oplus K_5[4] \oplus K_4[26] \oplus K_2[26]. \tag{5.6}
 \end{aligned}$$

Ushbu munosabat ham $1/2 + \varepsilon'$ ehtimollik bilan bajariladi.

Hosil qilingan har ikki munosabat ham tahlil qilishda keyinchalik foydalaniladi.

Shifrlash kalitining aktiv bitlari. 2-algoritmga asosan kalitning minimal qismini aniqlaymiz. Kalitning ushbu bitlari asosida ma'lum (P, C) juftlik yordamida (3) munosabatga kiruvchi shifr matnning bitlari kombinasiyasini tiklash mumkin. Bular esa birinchi va oxirgi qismiy kalitlarning quyidagi o'n ikkita bitlaridir:

$$K' = K_1[25], K_1[26], K_1[27], K_1[28], K_1[29], K_1[30],$$

$$K'' = K_{16}[1], K_{16}[2], K_{16}[3], K_{16}[4], K_{16}[5], K_{16}[6].$$

Biz qurgan 14 raundli yaqinlashishda oraliq shifr matnlarning noma'lum $R_1[8,14,25]$ va $L_{15}[17]$ noma'lum bitlari ishtirok etadi. Ularni aniqlash kerak bo'ladi. Shuningdek, yaqinlashishda ishtirok etuvchi $R_{15}[8,14,25,3]$ bitlarning qiymatlari $R_{15} = R_{16}$ tenglikka asosan ma'lum.

$R_1[8,14,25]$ bitlarning qiymatlarini ma'lum bo'lgan L_0R_0 ochiq matnga asosan tiklash mumkin. Buning uchun avval $f(R_0, K_1)[8,14,25]$ qiymatlarni aniqlash lozim bo'ladi. U holda

$$R_1[8,14,25] = L_0[8,14,25] \oplus f(R_0, K_1)[8,14,25]$$

tenglikdan foydalanish mumkin.

Shunday qilib, $f(R_0, K_1)[8,14,25]$ qiymatlarni aniqlash uchun DES shifrini raund funksiyasini tahlil qilamiz. Raund funksiyasining bizga kerakli 8,14,25 chiqish bitlari raund funksiyasini P -blokdan o'tishdan avval mos holda 17,18,19 pozisiyadagi bitlar edi. YA'ni, ushbu bitlar DES shifrini 5-chi S-bloki chiqishidagi birinchi, ikkinchi va uchinchi bitlar edi. Ushbu bitlarni tiklash uchun 5-chi S-blokka kiruvchi kiruvchi bitlarni bilish lozim bo'ladi. Bu bitlarni shartli ravishda $x_1, x_2, x_3, x_4, x_5, x_6$ bilan belgilaymiz. Ushbu bitlar R_0 qismiy blokning alohida bitlarini raund kalitining ayrim bitlari bilan 2 ning moduli bo'yicha qo'shish natijasida hosil qilinganligini payqash mumkin. Haqiqatan ham,

$$x_1 = R_0[16] \oplus K_1[25], \quad x_2 = R_0[17] \oplus K_1[26], \quad x_3 = R_0[18] \oplus K_1[27],$$

$$x_4 = R_0[19] \oplus K_1[28], \quad x_5 = R_0[20] \oplus K_1[29], \quad x_6 = R_0[21] \oplus K_1[30].$$

Shunday qilib, qismiy kalitning yuqorida keltirilgan olti bitlarining qiymatlarini bilish ochiq matn bo'yicha R_1 [8,14,25] bitlarning qiymatlarini tiklash uchun etarli.

Ma'lum bo'lgan shifr matn bo'yicha L_5 [17] bitni tiklash uchun $f(R_{15}, K_{16})$ [17] bitni qiymatini bilish talab etiladi. U holda L_{15} [17] = $f(R_{15}, K_{16})$ [17] $\oplus L_{16}$ [17] tenglik o'rinali bo'ladi. Chunki, $R_{15} = R_{16}$. $f(R_{15}, K_{16})$ ning 17-chi bitini aniqlaymiz. Shuni qayd etish lozimki, P -blokdan o'tishdan avval ushbu bit 1-chi S-blokni chiqishidagi ikkinchi bit edi. Shu bois, ushbu bitni tiklash uchun 1-chi S-blokda ishtirok etuvchi qismiy kalitning bitlaridan foydalanish lozim. Ya'ni, qismiy kalitning ushb bitlari quyidagilar ekanligini osongina aniqlash mumkin: $K_{16}[1], K_{16}[2], K_{16}[3], K_{16}[4], K_{16}[5], K_{16}[6]$.

Xuddi shuningdek, ikkinchi munosabat, ya'ni (5.6) uchun shifrlash kalitining aktiv bitlari quyidagilar ekanligini aniqlash mumkin:

$$K''' = K_{25}[25], K_{25}[26], K_{25}[27], K_{25}[28], K_{25}[29], K_{25}[30],$$

$$K'''' = K_1[1], K_1[2], K_1[3], K_1[4], K_1[5], K_1[6].$$

Kriptotahlil. Chiziqli tahlilning 2-algoritmidan foydalaniladi. Statistika parallel tarzda 2^{12} marta qayta ishlanadi: kalitning aktiv bitlari har bir guruhi $K' \cup K''$ uchun (5.5) munosabatning eksperimental salmog'i hisoblanadi. Uni ε' bilan solishtirib, kalitning aktiv bitlari guruhining to'g'ri qiymatlari aniqlanadi. 2-algoritm ishini tugatgandan so'ng kalitning (5.5) munosabatda ishtirok etgan bitlari uchun chiziqli munosabat hosil bo'ladi. Shu tarzda kalitning 13 ta biti haqida axborotga ega bo'lish mumkin.

Ushbu prosedura (5.5) munosabatda ochiq va shifrmatnlarni o'rinalarini almashtirgandan so'ng hosil bo'ladigan ikkinchi munosabat, ya'ni (5.6) chiziqli munosabatga nisbatan qo'llaniladi. Natijada shifrlash kalitining yana 12 ta bitlari – $K''' \cup K''''$ aniqlanadi va kalit uchun ikkinchi chiziqli munosabat hosil qilinadi.

Shunday qilib, kalitning 26 ta bitlari haqida axborotga ega bo'lish mumkin. Kalitning qolgan 30 ta bitlari qiymatlari to'liq saralash usulidan foydalanib, aniqlanadi.

DES shifrini kalitini aniqlash uchun o’rtacha 2^{43} ta ochiq matn va unga mos keluvchi shifr matn juftliklari kerak bo’ladi. Muvaffaqiyatga erishish 85% ni tashkil qiladi, ya’ni ushbu usul yordamida aniqlangan kalit 0,85 ehtimollik bilan to’g’ri kalit bo’ladi.

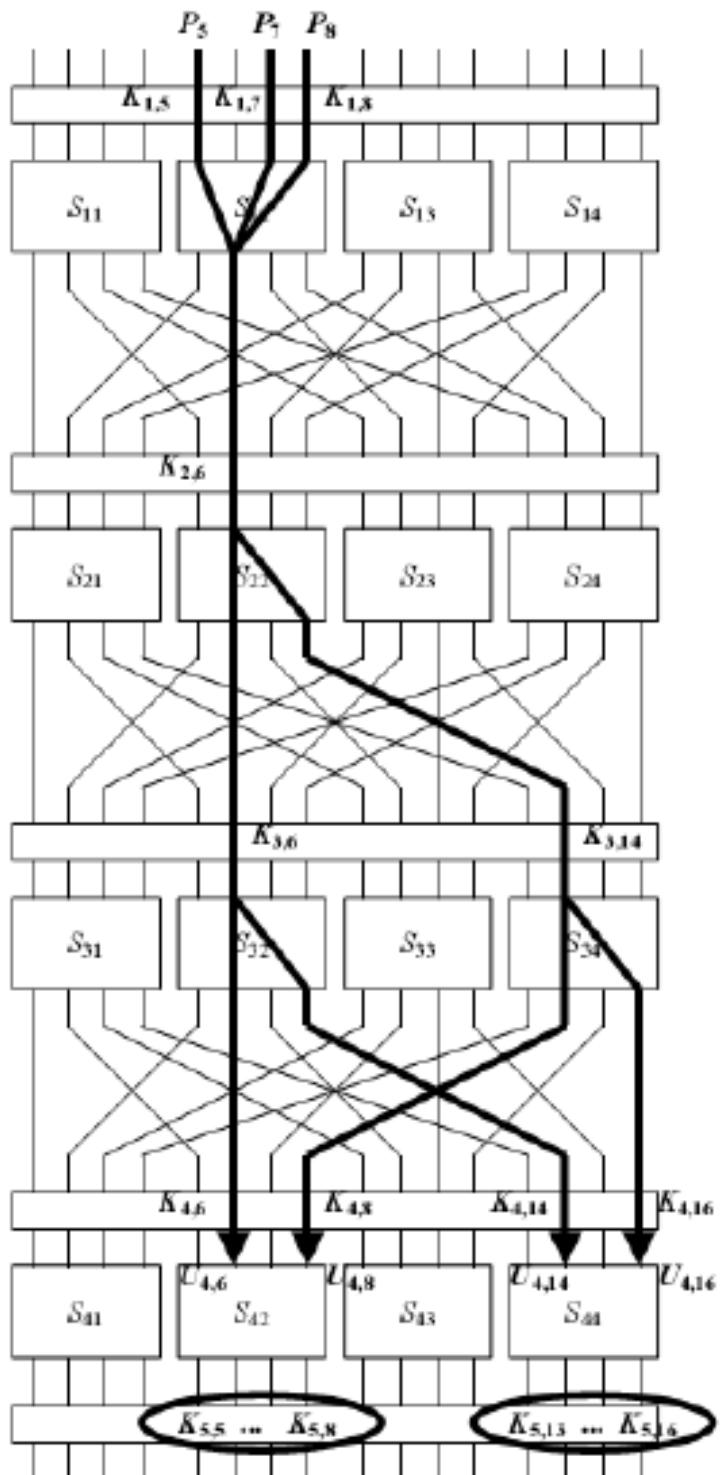
Katta hajmdagi statistikani qayta ishlash kerakligi sababli chiziqli tahlilni amaliyotga qo’llash katta qiyinchiliklar bilan bajariladi.

§5.6. SP tarmog’iga asoslangan shifrning chiziqli kriptotahlili va kalit bitlarini aniqlash

Ushbu shifrning tavsifi va kriptografik akslantirishlari 4-bobda keltirilgan. Shu bois, ishni yuqori ehtimollik bilan bajariladigan chiziqli munosabatlarni topishdan boshlash mumkin.

**5.5-jadval. Shifrning S bloklarining kirish-chiqish juftliklari uchun
(5.7)-(5.10) chiziqli munosabatlarning bajarilishi.**

Kirish	Chiqish															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0001	0	0	6	6	0	0	6	14	10	10	0	0	10	10	0	0
0010	0	0	6	6	0	0	6	6	0	0	10	10	0	0	1	10
0011	0	0	0	0	0	0	0	0	10	2	6	6	10	10	6	6
0100	0	10	0	6	6	4	0	0	0	6	0	10	10	4	10	0
0101	0	6	6	0	6	0	12	10	6	0	4	10	0	6	6	0
0110	0	10	6	12	10	0	0	10	0	6	10	12	6	0	0	6
0111	0	6	0	10	10	4	10	0	6	0	10	0	12	10	0	10
1000	0	0	0	0	0	0	0	6	10	10	6	10	6	6	2	2
1001	0	0	6	6	0	0	6	6	4	0	6	10	0	12	10	6
1010	0	12	6	10	4	0	10	6	10	10	0	0	10	10	0	0
1011	0	12	0	4	12	0	12	0	0	0	0	0	0	0	0	0
1100	0	6	12	6	6	0	10	0	10	0	10	12	0	10	0	6
1101	0	10	10	0	6	12	0	10	4	6	10	0	10	0	0	10
1110	0	10	10	0	6	4	0	10	6	0	0	6	4	10	6	0
1111	0	6	4	6	6	0	10	0	0	6	12	6	6	0	10	0



5.3-rasm. Chiziqli yaqinlashishga misol.

Ochiq matn bitlari va oxirgi raund S bloklaridan chiquvchi bitlardan tashkil topgan samarali chiziqli yaqinlashishlar yoki bog'lanishlar qurish shifrlash algoritmiga hujum qilish va shifrning oxirgi raundi kaliti bitlarini aniqlash imkonini beradi. Buni esa misolda ko'rsatamiz. Shunday chiziqli yaqinlashishlarni qurish kerakki, ushbu yaqinlashishni qurishda ishtirok etuvchi har bir S blokning

yaqinlashish ehtimoli 0,5 dan etarlicha kichik yoki aksincha bo'lsin. Shuningdek, chiziqli yaqinlashish ham mumkin qadar katta ehtimollik bilan bajariladigan bo'lsin.

S_{12} , S_{22} , S_{32} va S_{42} o'rniliga qo'yish bloklaridan tashkil topgan yaqinlashishni o'rganamiz (5.3-rasm). Shuni ham ta'kidlash lozimki, ushbu yaqinlashish haqiqatan ham birinchi uchta raundni qamrab oladi va to'rtinchchi raundni qisman o'zida mujassam etgan. Ushbu holat oxirgi raund kaliti bitlarini aniqlashda qanchalik ahamiyatli bo'llishini keyinroq ko'ramiz.

Biz S bloklarning quyidagi yaqinlashishlarini qaraymiz (5.5-jadval).

$$S_{12}: X_1 \oplus X_3 \oplus X_4 = Y_2 \quad (5.7)$$

(ehtimolligi $p_1=12/16=3/4$, chiziqli mounosabat salmog'i 1/2);

$$S_{22}: X_2 = Y_2 \oplus Y_4 \quad (5.8)$$

(ehtimolligi $p_1=4/16=1/4$, chiziqli mounosabat salmog'i 1/4);

$$S_{32}: X_2 = Y_2 \oplus Y_4 \quad (5.9)$$

(ehtimolligi $p_1=4/16=1/4$, chiziqli mounosabat salmog'i 1/4);

$$S_{34}: X_2 = Y_2 \oplus Y_4 \quad (5.10)$$

(ehtimolligi $p_1=4/16=1/4$, chiziqli mounosabat salmog'i 1/4).

Mavzuni bundan keyingi bayon qilishda quyidagi belgilashlardan foydalananamiz:

P – 16 bitdan iborat ochiq matn bloki;

P_i – 16 bitli ochiq matn blokining i -chi biti;

$U_i(V_i)$ – i -chi S blokga kiruvchi (chiquvchi) qiymat (kirish va chiqish qiymatlari 0000 dan 1111 gacha bo'lган bitlar ketma-ketligini yoki o'nlik sanoq tizimidagi 0 dan 16 gacha bo'lган qiymatlardan birini qabul qilishi mumkin);

$U_{ij}(V_{ij})$ – $U_i(V_i)$ kiruvchi (chiquvchi) ma'lumotlar blokining j -chi biti (bitlar chapdan o'ngga qarab, 1 dan 16 gacha nomerlanadi);

K_i – i -chi raundga kiruvchi ma'lumotlar bloki bilan ikkining moduli bo'yicha qo'shiladigan raund kaliti ($i=1,2,3,4$). K_5 kalit esa to'rtinchchi (oxirgi) raund S bloklaridan chiqqan ma'lumotlar bloki bilan ikkining moduli bo'yicha qo'shiladi.

(5.7)-(5.10) tenglamalarda foydalanilgan indekslar o'ziga xos ma'noga ega. Masalan, X_2 bit aslida ikkinchi raundga kiruvchi umumiy ma'lumotlar blokining oltinchi biti bo'lsada, S_{22} blokka kiruvchi ma'lumotlarning ikkinchi biti ekanligini anglatadi.

5.3-rasm va kiritilgan belgilashlardan foydalanib, birinchi raund uchun

$$U_1 = P \oplus K_1 \quad (5.11)$$

munosabatni hosil qilish mumkin. Natijada birinchi raund chiziqli yaqinlashishi, ya'ni (5.7) tenglikni e'tiborga olib, $p_1 = 3/4$ ehtimollik bilan quyidagiga ega bo'lish mumkin:

$$V_{16} = U_{15} \oplus U_{17} \oplus U_{18} = (P_5 \oplus K_{15}) \oplus (P_7 \oplus K_{17}) \oplus (P_8 \oplus K_{18}). \quad (5.12)$$

Ikkinchi raund chiziqli yaqinlashishi, ya'ni (5.8) tenglikni e'tiborga olib, $p_2 = 1/4$ ehtimollik bilan quyidagini hosil qilish mumkin:

$$V_{26} \oplus V_{28} = U_{26}.$$

Ushbu munosabatni $U_{26} = V_{16} \oplus K_{26}$ tenglikdan foydalanib, $p_2 = 1/4$ ehtimollik bilan bajariluvchi $V_{26} \oplus V_{28} = V_{16} \oplus K_{26}$ ko'rinishga keltirish mumkin. Oxirgi tenglikni (5.12) munosabatdan foydalanib, $p_1 = 3/4$ ehtimollik bilan bajariluvchi quyidagi munosabatga keltirish mumkin:

$$V_{26} \oplus V_{28} \oplus P_5 \oplus P_7 \oplus P_8 \oplus K_{15} \oplus K_{17} \oplus K_{18} \oplus K_{26} = 0. \quad (5.13)$$

(5.13) munosabat Piling-up lemmasiga asosan quyidagi ehtimollik bilan bajariladi

$$p_5 = 1/2 + 2^{n-1}((p_1 - 1/2) \times \dots \times (p_n - 1/2)) = 1/2 + 2 \times (3/4 - 1/2)(1/4 - 1/2) = 3/8,$$

chiziqli munosabat salmog'i quyidagiga teng bo'ladi:

$$\varepsilon_5 = p_5 - 1/2 = 3/8 - 1/2 = -1/8.$$

Xuddi shuningdek, uchinchi raund uchun $p_3 = 1/4$ va $p_4 = 1/4$ ehtimolliklar bilan bajariluvchi mos holda $V_{36} \oplus V_{38} = U_{36}$ hamda $V_{3,14} \oplus V_{3,16} = U_{3,14}$ munosabatlarni aniqlab, ushbu munosabatlarni $U_{36} = V_{26} \oplus K_{36}$ va $U_{3,14} = V_{28} \oplus K_{3,14}$ tengliklarni e'tiborga olib qo'shish natijasida quyidagi tenglikni hosil qilish mumkin:

$$V_{36} \oplus V_{38} \oplus V_{3,14} \oplus V_{3,16} \oplus V_{26} \oplus K_{36} \oplus V_{28} \oplus K_{3,14} = 0. \quad (5.14)$$

Ushbu tenglik

$$p_6 = 1/2 + 2^{n-1}((p_1 - 1/2) \times \dots \times (p_n - 1/2)) = 1/2 + 2 \times (1/4 - 1/2)^2 = 5/8$$

chiziqli munosabat salmog'i quyidagiga teng bo'ladi:

$$\varepsilon_6 = p_6 - 1/2 = 5/8 - 1/2 = 1/8.$$

Endi S bloklarning barcha chiziqli yaqinlashishlarini bir joyga yig'ish uchun (5.13) va (5.14) tengliklarni quyidagicha birlashtiramiz:

$$V_{36} \oplus V_{38} \oplus V_{3,14} \oplus V_{3,16} \oplus P_5 \oplus P_7 \oplus P_8 \oplus K_{15} \oplus K_{17} \oplus K_{18} \oplus K_{26} \oplus K_{36} \oplus K_{3,14} = 0.$$

Ushbu munosabatni $U_{46} = V_{36} \oplus K_{46}$, $U_{48} = V_{3,14} \oplus K_{48}$, $U_{4,14} = V_{3,8} \oplus K_{4,14}$ va $U_{4,16} = V_{3,16} \oplus K_{4,16}$ tengliklarni hisobga olib, quyidagi ko'rinishda ifodalaymiz:

$$U_{46} \oplus U_{48} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 \oplus \sum_K = 0, \quad (5.15)$$

bu erda $\sum_K = K_{15} \oplus K_{17} \oplus K_{18} \oplus K_{26} \oplus K_{36} \oplus K_{3,14} \oplus K_{46} \oplus K_{48} \oplus K_{4,14} \oplus K_{4,16}$, shifrlash algoritmi kalitiga bog'liq holda 0 yoki 1 qiymatni qabul qiladi.

$p_7 = 1/2 + 2^{n-1}((p_1 - 1/2) \times \dots \times (p_n - 1/2)) = 1/2 + 2^3 \times (3/4 - 1/2)(1/4 - 1/2)^3 = 15/32$ ehtimollik va chiziqli munosabat salmog'i

$$\varepsilon_7 = p_7 - 1/2 = 15/32 - 1/2 = -1/8$$

bilan (5.15) tenglikni bajarilishini aniqlash mumkin.

$$U_{46} \oplus U_{48} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 = 0 \quad (5.16)$$

tenglik \sum_K yig'indi 0 yoki 1 qiymat qabul qilishiga ko'ra $15/32$ yoki $(1 - 15/32)$ ehtimollik bilan bajarilishini payqash mumkin. Bu esa dastlabki uchta raund uchun chiziqli yaqinlashishini og'ishi $1/16$ ga tengligini anglatadi. Chiziqli bog'lanish yoki yaqinlashishlarni bajarilish ehtimolligining $1/2$ ehtimollikdan og'ishi yoki chetlashishi qanchalik katta bo'lsa, kriptoanalitik shunchalik chiziqli kriptotahvilni yaxshi qo'llashi mumkin. Kalitning ayrim bitlarini aniqlashda ushbu chetlashishdan foydalanish quyida keltirilgan.

Kalit bitlarini aniqlash

Yuqorida R raundli shifrlash algoritmi uchun R-1 raundli chiziqli yaqinlashish katta ehtimolli og'ish bilan aniqlandi. Shu bois, oxirgi raund kalitlarini aniqlash yordamida shifrlash algoritmiga hujum qilish mumkin. Bizning holimizda dastlabki uch raundning chiziqli yaqinlashishidan foydalanib, raund kaliti K_5 bitlarini aniqlash mumkin. Oxirgi raund kalitidan hosil qilinadigan bitlar *maqsadli qismiy kalitlar deb nomlanadi*. Shu jumladan, maqsadli qismiy kalitlardan birining bitlari oxirgi raund kaliti bitlarini tashkil qilishi mumkin. Oxirgi raund kalitining qidirilayotgan bitlari chiziqli yaqinlashishda ishtirok etadigan ma'lumotlar bitlariga ta'sir qiluvchi oxirgi raund S bloklari bilan bog'liq.

Kalit bitlarini aniqlash bo'yicha ishlar oxirgi raundni qisman deshifrlashdan boshlanadi. Buning uchun oxirgi raunddan so'ng maqsadli qismiy kalitlarning bo'lishi mumkin bo'lgan barcha qiymatlari uchun shifr matn bitlari mos S bloklardan teskari tartibda o'tkaziladi (natijada U_4 hosil qilinadi). Undan so'ng U_4 bitlari maqsadli qismiy kalitning mos bitlari bilan ikkining moduli bo'yicha qo'shib, V_3 hosil qilinadi: $V_3=U_4 \oplus K_4$. Ushbu jarayon kriptoanalitikka ma'lum bo'lgan barcha ochiq matn-shifr matn juftliklari uchun bajariladi hamda maqsadli qismiy kalitlarning barchasi uchun ustma-ust tushishlar (mos kelishlar) soni aniqlanadi. Bu erda mos kelish yoki ustma-ust tushish deyilganda konkret maqsadli qismiy kalit uchun oxirgi raund S bloki bitlari (deshifrlash natijasida aniqlangan) va ochiq matn bitlari uchun chiziqli yaqinlashishning o'rini ekanligi tushuniladi. Agar maqsadli qismiy kalitlarning qandaydir birortasi mos kelsa, ushbu maqsadli qismiy kalitga mos keluvchi hisoblagichning qiymati bittaga oshiriladi. Hisoblagichining qiymati ochiq matn-shifr matn juftliklari sonining yarmidan eng katta chetlashishga ega bo'lgan maqsadli qismiy kalitning qiymati *qidirilaётган мақсадли қисмий калит битларининг тоғ'ри қиymati hisoblanadi*. Bu haqiqatan ham shunday, chunki biz maqsadli qismiy kalit bitlarining to'g'ri qiymati $1/2$ dan sezilarli farq qiladigan ehtimollik bilan bajariladigan chiziqli yaqinlashishlarga ega deb faraz qilgan edik (ushbu ehtimollik $1/2$ dan katta yoki kichik bo'lishidan qat'iy nazar). Noto'g'ri qismiy kalit oxirgi raund S blokiga kiruvchi bitlarni nisbatan tasodifiy faraz qilish

natijasida hosil bo'ladi. Buning natijasida chiziqli bog'lanish 1/2 ga yaqin ehtimollik bilan o'rini bo'ladi.

Endi yuqorida bayon etilgan mulohazalarni konkret misolda qo'llaymiz. Yuqorida biz hosil qilgan

$$U_{46} \oplus U_{48} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 = 0 \quad (5.16)$$

chiziqli bog'lanishda oxirgi raundning (bizning holimizda to'rtinchi) S_{42} va S_{44} bloklariga kiruvchi ma'lumotlar ishtirok etadi. Har bir ochiq matn-shifr matn juftligi uchun maqsadli qismiy kalit $[K_{5,5}, \dots, K_{5,8}, K_{5,13} \dots K_{5,16}]$ larning barcha $2^8=256$ qiymatlarini sinab ko'ramiz. Agar (5.16) chiziqli yaqinlashish maqsadli qismiy kalitning biror bir qiymatida o'rini bo'lsa, u holda maqsadli qismiy kalitning o'sha qiymati uchun hisoblagichning qiymatini bittaga oshiramiz. Ma'lumotlarni maqsadli qismiy kalit va S_{42} va S_{44} bloklaridan teskari tartibda o'tkazish orqali $[U_{4,5} \dots U_{4,8}, U_{4,13} \dots U_{4,16}]$ larning qiymatlarini aniqlaymiz. Qaysi maqsadli qismiy kalit qiymatining hisoblagichi qiymati ochiq matn-shifr matn juftliklari sonining yarmidan eng katta chetlashishga ega bo'lsa, maqsadli qismiy kalitning o'sha qiymatini qidirilayotgan maqsadli qismiy kalit bitlarining to'g'ri qiymati deb hisoblaymiz. Chetlashishning musbat yoki manfiy bo'lishi $\sum_K = K_{15} \oplus K_{17} \oplus K_{18} \oplus K_{26} \oplus K_{36} \oplus K_{3,14} \oplus K_{46} \oplus K_{48} \oplus K_{4,14} \oplus K_{4,16}$ yig'indida ishtirok etuvchi qismiy kalitlar bitlarining qiymatiga bog'liq bo'ladi. \sum_K yig'indi nolga ga teng bo'lsa, (5.15) chiziqli yaqinlashishning ehtimolligi 1/2 dan kichik, agar \sum_K yig'indi birga ga teng bo'lsa, 1/2 dan katta deb hisoblanadi.

Shifrlash algoritmiga hujum qilish uchun 10000 ochiq matn/shifr matn juftligidan foydalanildi. Qismiy kalitlarning $[K_{5,5} \dots K_{5,8}] = [0010]$ (hex 0x02) va $[K_{5,13} \dots K_{5,16}] = [0100]$ (hex 0x04) qiymatlari uchun kriptotahvil natijalari keltiriladi. Kutilganidek, 5000 dan sezilarli farqlanuvchi hisoblagichning qiymati [2,4]hex maqsadli qismiy kalitning qiymatiga mos kelgan. Bu esa ushbu hujum yordamida maqsadli qismiy kalitning bitlari muvaffaqiyatli aniqlanganligini isbotlaydi. Buni 5.6-jadval ham ko'rsatib turibdi. Ushbu jadvalda qismiy kalitlarning mos hisoblagichlaridan hosil qilingan \sum_K yig'indining qiymatlari keltirilgan

(ma'lumotlarning to'liq hajmi 256 ta elementdan iborat bo'lib, maqsadli qismiy kalitlarning har bir qiymatiga bittadan element mos keladi).

5.6-jadval. Chiziqli kriptotahlil asosidagi hujumning tajribaviy natijalari.

Qismiy kalitlar [K_{5,5}, ..., K_{5,8}, K_{5,13}, ..., K_{5,16}]	Chetlashish	Qismiy kalitlar [K_{5,5}, ..., K_{5,8}, K_{5,13}, ..., K_{5,16}]	Chetlashish
1 C	0.0031	2 A	0.0044
1 D	0.0078	2 B	0.0186
1 E	0.0071	2 C	0.0094
1 F	0.0170	2 D	0.0053
2 0	0.0025	2 E	0.0062
2 1	0.0220	2 F	0.0133
2 2	0.0211	3 0	0.0027
2 3	0.0064	3 1	0.0050
2 4	0.0336	3 2	0.0075
2 5	0.0106	3 3	0.0162
2 6	0.0096	3 4	0.0218
2 7	0.0074	3 5	0.0052
2 8	0.0224	3 6	0.0056
2 9	0.0054	3 7	0.0048

$$|Chetlashish|=|Hisoblagich qiymati -5000|/10000$$

formulasi bilan aniqlangan chetlashish miqdorlari ham 5.6-jadvalda keltirilgan. 5.6-jadvaldan ko'rinish turibdiki, eng katta chetlashish [K_{5,5} ... K_{5,8}, K_{5,13} ... K_{5,16}] = [2,4] maqsadli qismiy kalitning qiymatiga mos keladi va ushbu qiymat haqiqatan ham qismiy kalitning haqiqiy bitlariga mos keladi.

Ko'rinish turibdiki, chetlashining hisoblash tajribasi bilan aniqlangan 0,0336 qiymati kutilgan $1/32=0,03125$ qiymatga juda yaqin.

Nazorat savollari

1. Chiziqli kriptotahlil usulining mohiyati nimadan iborat?
2. Chiziqli tahlil usulini qo'llashda asosiy qiyinchilik nimadan iborat?
3. Shifrning chiziqli yaqinlashishi deb nimaga aytildi?
4. Chiziqli munosabat nima?
5. Chiziqli munosabatning salmog'i nima?

6. Chiziqli munosabat salmog'i qiymatining katta yoki kichik bo'lishi nimani anglatadi?
7. Piling-up lemmasi qanday maqsadda qo'llaniladi?
8. Chiziqli kriptotahlil usulini amalga oshirish qanday bosqichlardan iborat?
9. Shifrlash kalitining bitta biti qanday aniqlanadi?
10. Shifrlash kalitining bitlar guruhi qanday aniqlanadi?
11. «Oddiylikdan murakkablikga» tamoyili chiziqli tahlilda qanday qo'llaniladi?
12. Chiziqli salmoqlilik jadvali nima?
13. DES shifrlash algoritmi uchun chiziqli munosabatlar qanday quriladi?
14. Blokli shifrlar uchun chiziqli munosabatning bajarilish ehtimolligi qanday aniqlanadi?
15. Chiziqli munosabatlardan kalit bitlarini aniqlash uchun tenglamalar sistemasi qanday hosil qilinadi?
16. Shifrlash kalitining aktiv bitlari deb qanday bitlarga aytildi?
17. SP tarmog'iga asoslangan shifr uchun chiziqli munosabatlar qanday quriladi?
18. SP tarmog'iga asoslangan shifrning chiziqli kriptotahlili qanday amalga oshiriladi?
19. Maqsadli qismiy kalitlar deb qanday kalitlar nomlanadi?
20. Qidirilayotgan maqsadli qismiy kalit bitlarining to'g'ri qiymati qanday aniqlanadi?

6-BOB. CHIZIQLI-DIFFERENSIAL KRIPTOTAHLIL USULI

Kriptotahlilning ushbu turi ochiq matnni tanlashga asoslangan bo'lib, asosan DESga o'xhash siklik algoritmlarga mo'ljallangan [1]. Ushbu yangi usuldan foydalaniib, S.Langford va M.Xellman 512 ta ochiq matndan foydalaniib, DES shifrlash algoritmi kalitining 10 bitini 80% ehtimollik bilan aniqlashga muvaffaq bo'lishdi. Ochiq matnlar sonini 768 tagacha oshirishda kalit bitlarini aniqlash ehtimolligini 95% ga oshirish mumkin.

Shifrlashning siklik algoritmlari shifrlash funksiyasini bir necha marta takrorlashga asoslangan. Bunda algoritmning har bir raundi o'zidan oldingi raundning chiqishi va kalit bitlarining funksiyasi bo'ladi. DES shunday shifrlash algoritmlari qatoriga kiradi va shu bois, siklik blokli shifrlash algoritmlari kriptobardoshligini o'rganishda ko'pgina tadqiqotlarning predmeti sifatida xizmat qiladi.

Hozirgacha DES shifrlash algoritmiga hujum qilishning uchta samarali usullari mavjud: to'liq saralash usuli, differensial va chiziqli kriptotahlil usullari. Shu bilan birgalikda to'liq saralash usuli to'liq 16 raundli DES shifrlash algoritmiga hujum qilishning eng samarali usuli bo'lib qolmoqda. Ayni vaqtda olimlarning tadqiqotlari nisbatan samaraliroq bo'lган analitik hujumlarga yo'naltirilgan. Masalan, chiziqli tahlil usuli to'liq saralash usuliga nisbatan anchagina tezkor, ammo ushbu usul kriptotahlilni o'tkazish uchun bir xil kalit bilash shifrlangan, bo'lishi mumkin bo'lмаган miqdordagi (masalan, DES uchun uchun 2^{43}) ochiq matnlarni talab qiladi. Aksincha, to'liq saralash usulida bitta ochiq matnni o'zi etarli bo'ladi.

§6.1. Chiziqli-differensial kriptotahlilni qurishning asosiy prinsiplari

Chiziqli-differensial kriptotahlil usuli kriptotahlilning chiziqli va differensial tahlil usullarining kombinasiyasiga asoslangan.

Chiziqli-differensial kriptotahlilni qurishning asosiy prinsiplari bilan tanishamiz. Boshlang'ich IP va yakuniy IP^{-1} almashtirishlar shifrlangan xabarning kriptografik bardoshligiga ta'sir qilmaganliklari sababli ularni tushirib qoldiramiz.

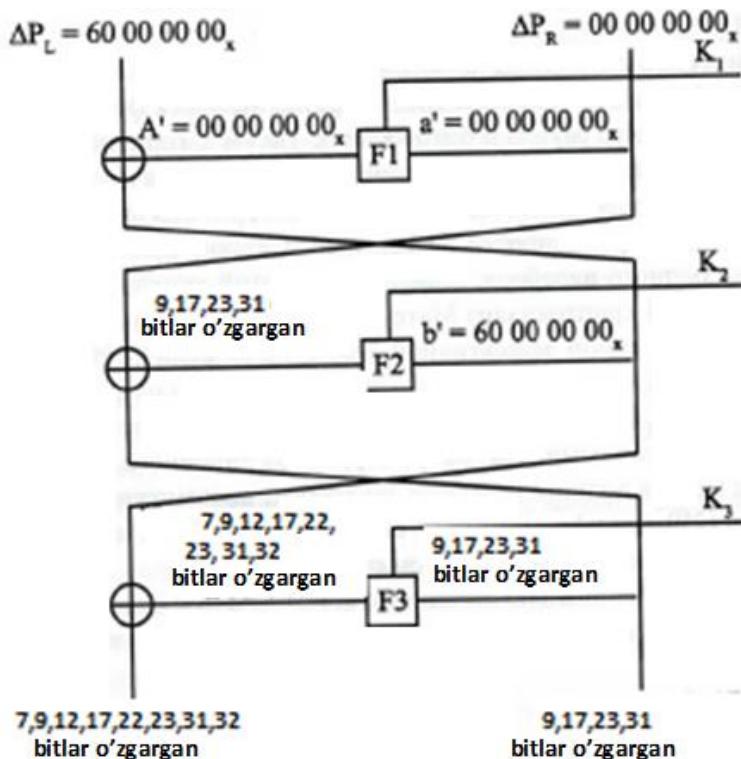
DES shifrlash algoritmining dastlabki uchta raundini differensial tahlilini ko'rib chiqamiz. Bizni o'n qismlari ikkinchi yoki uchinchi biti, yoki ikkinchi va uchinchi bitlaridan boshqa bitlari bir xil bo'lgan kiruvchi xabarlar qiziqtiradi. Bu holat esa faqatgina S_1 blokka noldan farqli, boshqa bloklarga qiymati nol bo'lgan differensial ayirmalar kirishini ta'minlaydi. Ushbu vaziyatda ikkita kiruvchi xabarlarni qanday pozisiyalarda farqlanishiga ko'ra differensial ayirmaning chap qismi ikkinchi va uchinchi pozisiyalardan boshqa pozisiyalarda faqatgina nollardan tashkil topgan bo'ladi. Biz esa aynan ikkinchi va uchinchi bitlarda tafovut bo'lgan variantlarni o'r ganamiz. Kiruvchi xabarlearning o'ng qismlari farqlanmaydi, shu sababli ularning ayirmasi nolga teng bo'ladi (6.1-rasm). Bu yerda shuni eslatish joizki, differensial kriptotahlilda ikkita xabarning ikkining moduli bo'yicha yig'indisi ularning differensial ayirmasi yoki oddiygina ayirmasi deyiladi. Biz mavzuni bayon qilishda ushbu tushunchalarga ko'p marta murojaat qilamiz.

6.1-rasmda birinchi va ikkinchi raund shifrlash funksiyasi F ga kiruvchi ayirmalar mos holda a' va b' bilan, birinchi raund F funksiyasidan chiquvchi ayirma A' bilan belgilangan.

Kiruvchi nolli ayirma hamma vaqt chiqishda nolli ayirmani beradi, shu sababli shifrlashning ikkinchi raundi F funksiyasi kirishiga kiruvchi ayirmaning chap qismi kiradi. F funksiyasiga kiruvchi xabar kengaytirib, o'r in almashtirishga uchragandan so'ng, S_1 blokka qiymati 001100 bo'lgan ayirma kiradi (S_1 blokka kiruvchi ayirmaning birinchi noli kiruvchi ayirmaning 32-chi biti, shuningdek, 2,3,4,5 va 6 bitlari esa kiruvchi ayirmaning mos holda 1,2,3,4 va 5 bitlaridan iborat). Boshqa S bloklarga qiymati nol bo'lgan ayirmalar kiradi.

Natijada S_1 blokdan boshqa barcha S bloklar chiqishida nolli ayirmalar paydo bo'ladi. S_1 blokni chiqishida qanday ayirma paydo bo'lishini biz bilmaymiz, ammo S_1 blok chiqishlari almashtirishdan so'ng 9, 17, 23 va 31 pozisiyalarda bo'lishlarini bilamiz. Shuningdek, S_1 blokka konkret ayirma kirsa, ma'lum bir ayirma qandaydir

ehtimollik bilan S_1 blokdan chiqishini faraz qilishdan foydalanish ham foydali bo'ladi.

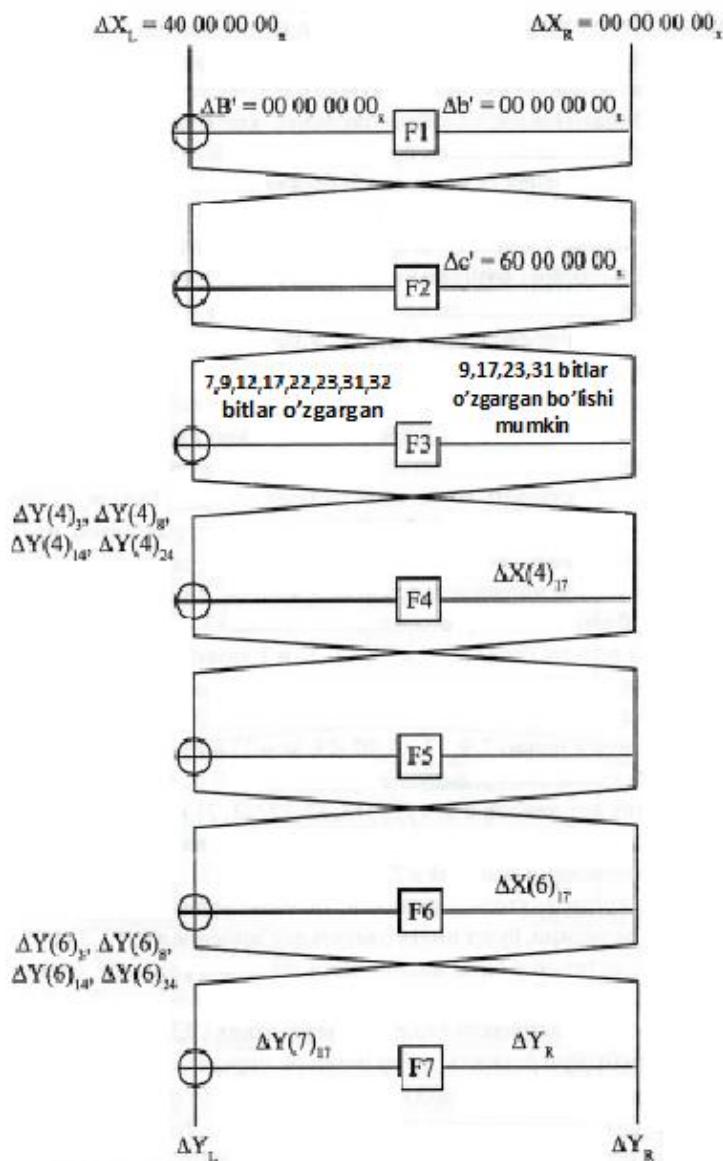


6.1-rasm. DES shifrlash algoritmining uch raundli xarakteristikasi.

Shunday qilib, DES shifrlash algoritmi ikkinchi raundi F funksiyasi chiqishida 9,17,23 va 31 pozisiyalarida o'zgarishlar bo'lgan ayirma paydo bo'ladi. Ushbu ayirmani oldingi raund chiqishi bilan ikkinning moduli bo'yicha yig'indisi ham ayirmaning qiymatiga teng bo'lib qolaveradi va u shifrlashning uchinchi raund F funksiyasiga kiruvchi ayirma vazifasini bajaradi.

Shifrlashning uchinchi raundi F funksiyasiga kiruvchi ayirma kengaytirib, o'rin almashtirishga uchragandan so'ng 9,17,23 va 31 pozisiyalardagi o'zgargan bitlar S_1 va S_7 bloklardan tashqari boshqa S bloklarga kiruvchi ayirmalarda ishtirok etadi. 9-chi bit S_2 va S_3 , 17-chi bit S_4 va S_5 , 23-chi bit S_5 , 31-chi bit S_8 bloklarga kiruvchi ayirmalarda ishtirok etadi. Demak, birinchi va sakkizinch S bloklar chiqishida nolli ayirmalar paydo bo'lishini biz aniq bilamiz. Bundan oldingi raundga o'xhash tarzda S_1 blokning chiqishi 9,17,23 va 31 pozisiyalarda, S_7 blokning chiqishi esa 32, 12, 22 va pozisiyalarda joylashadi.

Shifrlashning uchinchi raundi F funksiyasidan chiquvchi ayirma o'rinn almashtirishga uchragandan so'ng birinchi to'rtta bizga noma'lum qiymatlarga ega bo'ladi (yuqorida biz 7,9,12,17,22,23,31,32 pozisiyalardagi bitlar o'zgarmasdan qolishi haqida fikr yuritgan edik). Shu bois, uning oldingi raund chiqishi $b'=60\ 00\ 00\ 00$ bilan ikkining moduli bo'yicha yig'indisi hech narsani o'zgartirmaydi. Chunki b' da 7,9,12,17,22,23,31,32 pozisiyalardagi bitlar faqat nollardan tashkil topgan.



6.2-rasm. DES shifrlash algoritmining 7 raundiga chiziqli-differensial tahlilni qo'llash.

Shunday qilib, shifrlashning uchinchi raundidan so'ng chiqish ayilmalarining chap qismlari 7,9,12,17,22,23,31,32 pozisiyalarda hamma vaqt o'zgarmas

qiymatlarga ega bo'ladi (ya'ni, bizni holimizda kiruvchi ayirmalarga asosan nollardan iborat bo'ladi). Chiqish ayirmalarining o'ng qismlari 9,17,23 va 31 pozisiyalardagi bitlarning qiymatlari o'zgaradi (ya'ni, chiqish ayirmalarining o'ng qismlarining qolgan bitlari kiruvchi ayirmalarga asosan hamma vaqt nollardan iborat bo'ladi).

Agar 5 raundli DES shifrlash algoritmini o'rgandigan bo'lsak, chiqish ayirmalarini bilgan holda oxirgi beshinchi raund S bloklariga kirishlar, oxirgi raund F shifrlash funksiyasining birinchi va ettinchi S bloklaridan chiqish ayirmalarini osongina aniqlash mumkin bo'lar edi. Bu esa faqatgina kriptotahlilning differensial usulidan foydalanib, kalitning 12 bitini aniqlash imkonini bergan bo'lar edi (ya'ni, shifrlashning oxirgi raundi S_1 blokiga kirishni o'zgartiruvchi kalitning olti biti hamda oxirgi raundi S_7 blokiga kirishni o'zgartiruvchi kalitning olti biti).

Endi 7 raunddan tashkil topgan DES shifrlash algoritmini ko'rib chiqamiz. Dastlabki uchta raundga nisbatan differensial tahlilni yuqorida keltirilganidek qo'llaymiz. Navbatdagi uchta raund uchun (ya'ni, shifrlash algoritmining to'rtinchidan oltinchi raundigacha) chiziqli tahlildan foydalanamiz.

Kriptotahlilning chiziqli tahlil usuli bilan tanishganimizda DES shifrlash algoritmining 3 raundiga nisbatan samarali chiziqli bog'lanishlar qurgan edik. Biz mavzuni bayon qilishda X , X' ochiq matn, xabarlardan foydalanamiz. Birinchi X xabar uchun 4-6 raundlar uchun samarali chiziqli bog'lanish quyidagi ko'rinishda bo'lgan edi:

$$\begin{aligned} X(4)_{17} \oplus Y(4)_3 \oplus Y(4)_8 \oplus Y(4)_{14} \oplus Y(4)_{25} \oplus X(6)_{17} \oplus Y(6)_3 \oplus Y(6)_8 \oplus \\ \oplus Y(6)_{14} \oplus Y(6)_{25} = K(4)_{26} \oplus K(6)_{26}. \end{aligned} \quad (6.1)$$

(6.1) tenglamada qavs ichida raund nomeri, indekslar esa mos keluvchi bitlarni anglatadi. Xuddi shuningdek, ikkinchi X' xabar uchun 4-6 raundlar uchun samarali chiziqli bog'lanish quyidagi ko'rinishda bo'lgan edi:

$$\begin{aligned} X(4)_{17} \oplus Y'(4)_3 \oplus Y'(4)_8 \oplus Y'(4)_{14} \oplus Y'(4)_{25} \oplus X'(6)_{17} \oplus Y'(6)_3 \oplus Y'(6)_8 \oplus \\ \oplus Y'(6)_{14} \oplus Y'(6)_{25} = K(4)_{26} \oplus K(6)_{26}. \end{aligned} \quad (6.2)$$

X va X' xabarlar bir xil kalit bilan shifrlangani uchun (1) va (2) tenglamalarning o'ng qismlari bir xil bo'ladi. Shu sababli bu ikki tenglamani ikkini moduli bo'yicha qo'shib, (6.3) tenglamaga ega bo'lish mumkin. (6.3) tenglamaning chap qismi mos bitlar ayirmalarining ikki moduli bo'yicha yig'indisidan, o'ng qismi esa noldan iborat:

$$\begin{aligned} \Delta X(4)_{17} \oplus \Delta Y(4)_3 \oplus \Delta Y(4)_8 \oplus \Delta Y(4)_{14} \oplus \Delta Y(4)_{25} \oplus \Delta X(6)_{17} \oplus \Delta Y(6)_3 \oplus \\ \oplus \Delta Y(6)_8 \oplus \Delta Y(6)_{14} \oplus \Delta Y(6)_{25} = 0. \end{aligned} \quad (6.3)$$

Ilgari shifrlash algoritmining birinchi uchta raundining differential tahlili yordamida ayirmaning chap qismi 17 pozisiyada o'zgarmasdan qolishini aniqlagan edik. Shifrlash uchinchi raund chiqish ayirmasining chap qismi to'rtinchi raund kirish ayirmasining o'ng qismi bo'lganligi bois, $\Delta Y(4)_3$, $\Delta Y(4)_8$, $\Delta Y(4)_{14}$, $\Delta Y(4)_{25}$ ayirmalarning qiymatlari bizga aniq ma'lum.

Ushbu turdag'i hujumlarning asosiy sharti ochiq matnlarga mos keluvchi shifrmatnlarni kriptoanalitik bilishidir. Shu sababli X, X' ochiq matnlar mos keluvchi Y, Y' shifr matnlar bizga avvaldan ma'lum. Demak, ularning ayirmasi $\Delta Y = Y \oplus Y'$ ham ma'lum. Shifrlashning oltinchi raund chiqish ayirmasining chap qismi ettinchi raund kirish ayirmasining o'ng qismi bo'lganligi sababli, shuningdek, shifr matnlar ayirmasi ΔY ning o'ng qismi bo'lganligi bois, $\Delta Y(6)_3$ va $\Delta Y(6)_{25}$ ayirmalarning qiymatlari bizga aniq ma'lum.

Natijada (6.3) tenglama $\Delta X(6)_{17}$ ga nisbatan bir noma'lumli tenglama va unison hisoblash mumkinligi ko'rinishib qoldi. Shuni ham esda tutish lozimki, (6.3) tenglama (6.1) va (6.2) tenglamalar ehtimolliklari ko'paytmasiga teng ehtimollik bilan bajariladi:

$$p = \frac{39}{128} \times \frac{39}{128} \approx 0,0928.$$

Endi shifrlashning oxirgi ettinchi raundiga kelamiz. Topilgan $\Delta X(6)_{17}$ ni chiqish ayirmasi chap qismi 17-chi biti bilan 2 ning moduli bo'yicha qo'shib, ettinchi raund F shifrlash funksiyasi chiqish ayirmasining 17-chi bitiga ega bo'lamiz. Agar o'rin almashtirish jadvalidan foydalanilsa, F shifrlash funksiyasi chiqishining

17-chi biti S_1 blokning ikkinchi chiqish biti ekanligini ko'rish mumkin. Bizga shifrmatnlar ayirmasining o'ng qismi ma'lum bo'lganligi sababli ettinchi raund F shifrlash funksiyasiga kirish ayirmasi ham ma'lum. Demak, S_1 blokka kiruvchi ayirmani aniq topish mumkin.

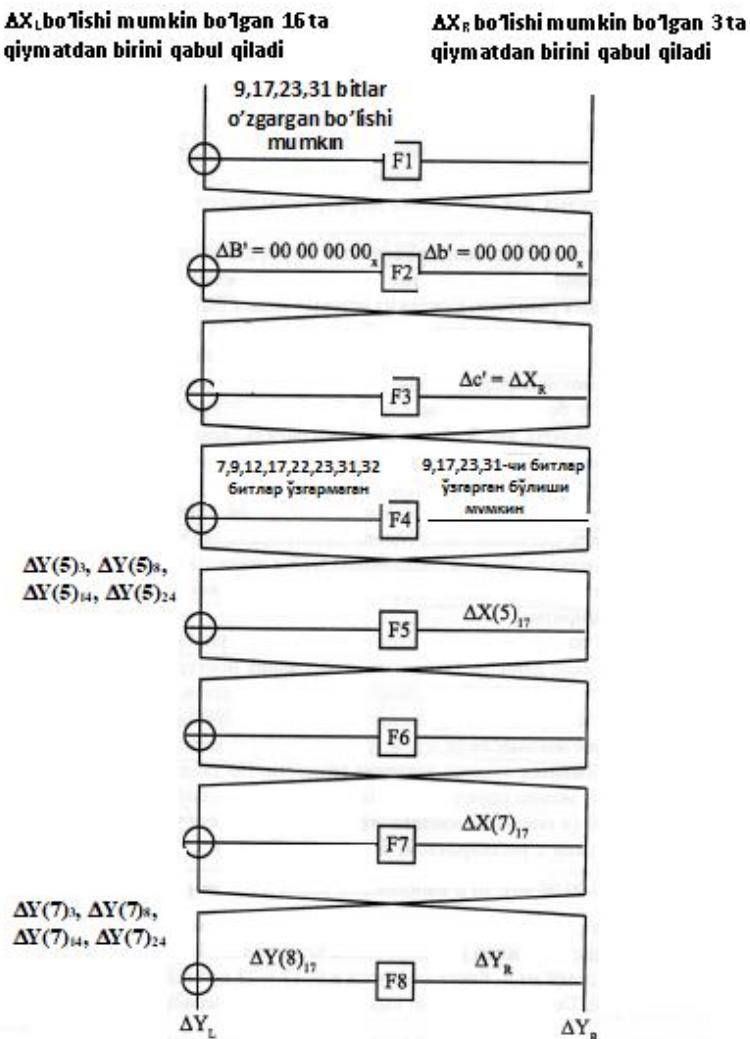
§6.2. DES shifrlash algoritmiga chiziqli-differensial kriptotahlilni qo'llanilishi

S blokka kiruvchi ayirmani va S blokdan chiquvchi ikkinchi bit ayirmasini bilgan holda ikkinchi chiquvchi bitga mos kelmaydigan, S_1 blokdan chiquvchi ayirmaning yarmini aniqlash mumkin. Masalan, agar S_1 blokdan chiquvchi ayirmaning ikkinchi biti 1 ga teng bo'lsa, u holda tahlil uchun bo'lishi mumkin bo'lgan 16 qiymatdan quyidagi 8 ta chiquvchi qiymatlarni qoldiramiz: 0100, 0101, 0110, 0111, 1100, 1101, 1110, 1111. Biroq, kalit bitlarini aniq topishda bu ma'lumotlar etarli emas. Shu sababli S.Langford va M.Xellman sakkiz raundli DES shifrlash algoritmiga hujum qilish variantini taklif qildilar. Bundan oldingi paragrafda ko'rilgan etti raundga ular qo'shimcha birinchi raundni kiritdilar. Ushbu holatda ikkinchi raundga kiruvchi ayirmalarni to'g'ri saqlab qolish uchun kiruvchi xabarlarning o'ng qismlari ikkinchi yoki uchinchi bitda farqlanishi yoki bir vaqtning o'zida ikkinchi va uchinchi bitlarda farqlanishi lozim.

6.1-paragrafda ko'rganimizdek, F shifrlash funksiyasiga shunday ayirma kirishi mumkinki, natijada 9,17,23 va 31-chi bitlarning qiymatlari o'zgarishi mumkin. Shifrlash algoritmining ikkinchi raundiga kiruvchi ayirmaning o'ng qismi nolga teng bo'lishi lozim. Biz birinchi raund F shifrlash funksiyasi chiqishining ayirmasini bilmaymiz, ammo bu ayirma bo'lishi mumkin bo'lgan 16 ta qiymatdan birini qabul qilishini bilamiz.

S.Langford va M.Xellmanlar kiruvchi qiymatlarning bo'lishi mumkin bo'lgan barcha qiymatlarini saralashni taklif qildilar. Natijada har bir kiruvchi juftligi uchun birinchi raund S_1 blokining qismiy kaliti bitlarini saralab, ular dastlabki kalitning 10

bitini qiymatini aniqlashga muvaffaq bo'ldilar. Gap shundaki, birinchi raund S_1 bloki qismiy kaliti 6 ta bitining 2 tasi sakkizinch raund S_1 bloki qismiy kaliti 6 ta bitida ishtirok etar ekan. Ushbu fakti bilish qismiy kalitlarni saralashda o'z natijasini ko'rsatdi. Albatta, kalitning o'n biti ko'p emas, ammo bundan ham nimagadir foydalanish mumkin.



6.3-rasm. 8 raundli DES shifrlash algoritmiga chiziqli-differensial kriptotahlilini qo'llash.

Langford va Xellmanlarning tadqiqotlarini kuzatgan Eli Bixam, Orr Dunkelman i Natai Keller 8 raundli DES shifrlash algoritmini chiziqli-differensial kriptotahlilini o'tkazishda o'zlarining yondoshuvlarini taklif qildilar. Quyida biz ular tomonidan taklif qilingan tahlil qilish usuli bilan tanishamiz (6.4-rasm).

Shifrlash algoritmi kirishiga ($\Delta X_L, \Delta X_R$) = (00 80 82 00, 60 00 00 00) ayirma tushadi. Natijada birinchi raund F shifrlash funksiyasiga qiymati 60 00 00 00 bo'lgan ayirma kiradi. Ilgari bunday holda birinchi S blokdan boshqa barcha S bloklarning chiqishida nol' qiyamatli ayirmalar chiqishini ta'kidlagan edik. Ma'lumki, S_1 blokka 001100 qiyamat kirsa (aynan ushbu qiyamat kiradi, chunki $\Delta X_R = 60 00 00 00$ qiyamat kengaytirib, o'rinni almashtirishga uchragandan so'ng S_0 00 00 00 00 ga o'zgaradi) eng katta $p = 14/64$ ehtimollik bilan chiqishda qiymati 1110 bo'lgan ayirma paydo bo'ladi. F shifrlash funksiyasidan chiqishdan oldin S bloklar chiqishlari o'rinni almashtiishga uchraydi, S_1 blokdan chiqqan ayirmadagi 1 lar ayirmaning 9, 17 va 23 pozisiyalarida joylashadi. SHunday qilib, DES algoritmi birinchi raund F shifrlash funksiyasi chiqishida $p = 14/64$ ehtimollik bilan $\Delta A' = 00 80 82 00$ ayirma paydo bo'ladi.

Birinchi raundni kirish ayirmasini chap qismi bilan chiqish ayirmasining ikkinining moduli bo'yicha yig'indisi ikkinchi raundni F shifrlash funksiyasiga kirganligi sababli ushbu ayirmaning qiymati quyidagicha bo'ladi:

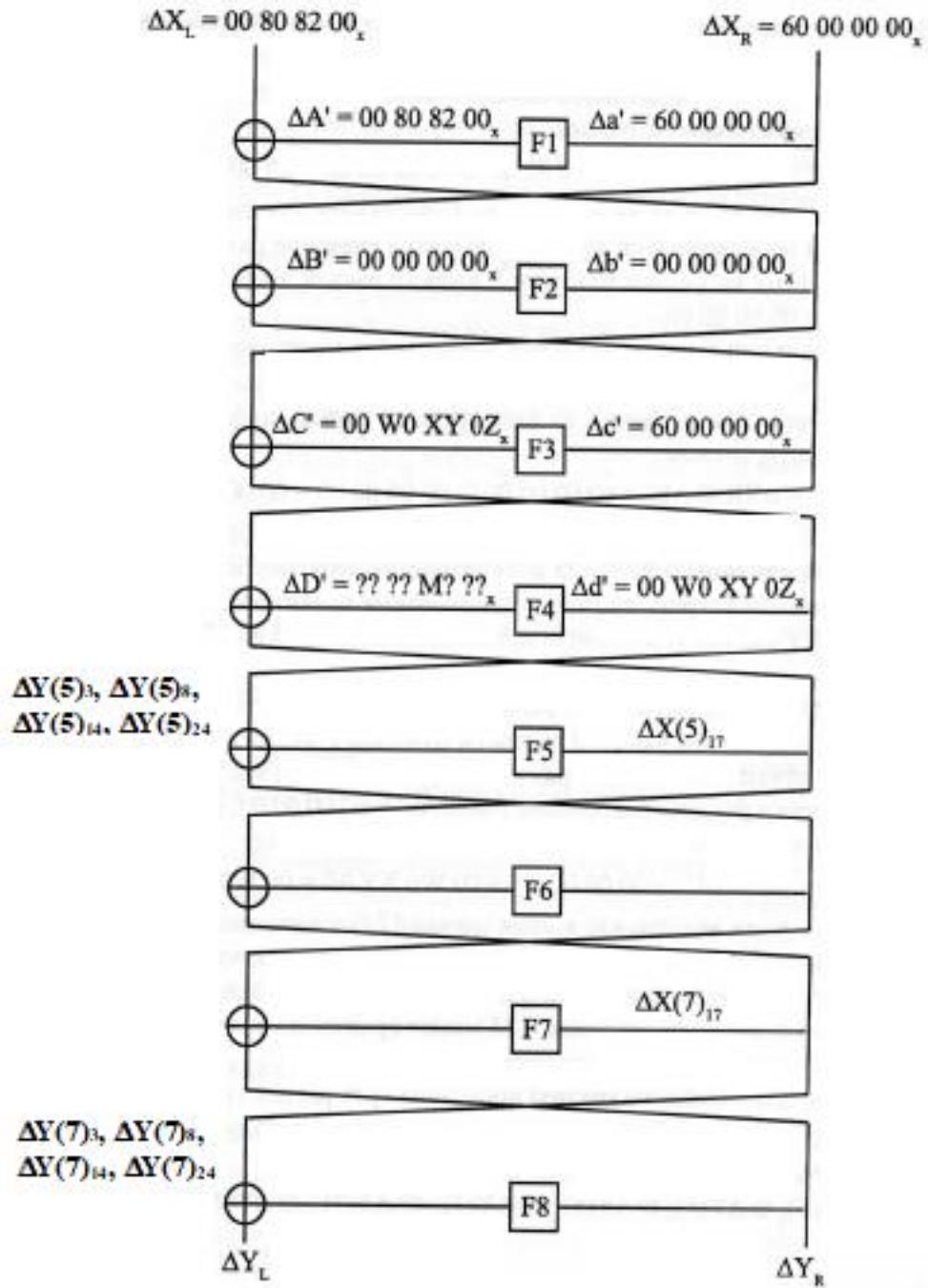
$$\Delta b' = \Delta X_L \oplus \Delta A' = 00 80 82 00 \oplus 00 80 82 00 = 00 00 00 00.$$

Agar F shifrlash funksiyasiga qiymati noldan iborat ayirma kiradigan bo'lsa, ushbu funksiyadan ham qiymati noldan iborat ayirma chiqadi. Shu sababli ikkinchi raund F shifrlash funksiyasidan $\Delta B' = 00 00 00 00$ ayirma chiqadi.

Birinchi raundni kirish ayirmasini o'ng qismi bilan ikkinchi raundni chiqish ayirmasining ikkinining moduli bo'yicha yig'indisi uchinchi raundni F shifrlash funksiyasiga kirganligi sababli ushbu ayirmaning qiymati quyidagicha bo'ladi:

$$\Delta c' = \Delta X_R \oplus \Delta B' = 60 00 00 00 \oplus 00 00 00 00 = 60 00 00 00.$$

Ushbu holda biz bilamizki, F shifrlash funksiyasidan chiquvchi ayirmaning 9, 17, 23 va 31 pozisiyalardagi qiymatlari 1 dan iborat bo'lishi mumkin. Shu bois, shuni aytish mumkinki, uchinchi raund F shifrlash funksiyasidan chiquvchi ayirmaning qiymati $\Delta C' = 00 W_0 X_0 Y_0 Z_0$ bo'ladi. Bu erda W va X lar 0 yoki 8, Y va Z lar 0 yoki 2 qiymatlarni qabul qilishlari mumkin.



**6.4-rasm. 8 raundli DES shifrlash algoritmi uchun Eli Bixam,
 Orr Dunkelman va Natai Keller tomonidan taklif qilingan
 chiziqli-differensial kriptotahsil usuli.**

To’rtinchi raundni F shifrlash funksiyasiga ikkinchi raundni kirish ayirmasini o’ng qismi bilan uchinchi raund F shifrlash funksiyasini chiqish ayirmasining ikkining moduli bo'yicha yig'indisi kiradi. Ikkinchi raundni kirish ayirmasini o'ng qismi $\Delta b' = 00\ 00\ 00\ 00$ bo'lganligi sababli to'rtinchi raundni F shifrlash funksiyasiga qiymati quyidagicha bo'lgan ayirma kiradi:

$$\Delta d' = \Delta b' \oplus \Delta C' = 00\ 00\ 00\ 00 \oplus 00\ W0\ XY\ 0Z = 00\ W0\ XY\ 0Z.$$

Ushbu holda F shifrlash funksiyasidan chiquvchi ayirmaning 17-chi biti doimo o'zgarmasdan qolishini oldinroq ta'kidlagan edik. Shu bois, aytish mumkinki, to'rtinchi raundni F shifrlash funksiyasining chiqishida $\Delta D' = ??\ ??\ M? ??$ ayirma paydo bo'ladi. Bu erda ? bo'lishi mumkin bo'lgan ixtiyoriy qiymatni, M esa 0 dan 7 gacha bo'lgan qiymatlardan birini qabul qiladi, ya'ni 17-chi bit doimo nolga teng qiymatni qabul qiladi.

Shifrlashning oxirgi uchta raundi uchun chiziqli bog'lanish tenglamasi 6.1-paragrafdagi (6.3) tenglamaga o'xshash bo'ladi. Bu erda to'rtinchi va oltinchi raunddagi qiymatlar emas, balki beshinchi va ettinchi raunddagi qiymatlar ishtirok etadi:

$$\begin{aligned} \Delta X(5)_{17} \oplus \Delta Y(5)_3 \oplus \Delta Y(5)_8 \oplus \Delta Y(5)_{14} \oplus \Delta Y(5)_{25} \oplus \Delta X(7)_{17} \oplus \Delta Y(7)_3 \oplus \Delta Y(7)_8 \oplus \\ \oplus \Delta Y(7)_{14} \oplus \Delta Y(7)_{25} = 0. \end{aligned}$$

Endi quyida keltirilgan algoritmga tayanib, tahlilni bajarish mumkin:

1. Ayirmasi ($\Delta X_L, \Delta X_R$) = (00 80 82 00, 60 00 00 00) ga teng bo'lgan $N=2^{13.81}$ sondagi ochiq matnlar juftligini tanlang.

2. Birinchi bandda tanlangan ochiq matnlarni bir xil kalit bilan shifrlab, ularga mos keluvchi shifr matnlarni hosil qiling.

3. 64 ta hisoblagich (schetchik) dan tashkil topgan massivni yarating va ushbu massivni nolb elementlar bilan to'ldiring.

4. Har bir shifr matn juftligi uchun quyidagi amallarni bajaring:

- S_1 blokka kiruvchi ma'lumotlar bilan ikkini moduli bo'yicha qo'shishda ishlatiladigan 6 bitli K_1 qismiy kalitning bo'lishi mumkin bo'ldgan 64 ta qiymatini aniqlang;

- Har bir bo'lishi mumkin bo'lgan qismiy kalit uchun shifrlashni sakkizinch raundi S_1 bloki chiqish juftliklarini hisoblang;

- S_1 blokining chiqishidagi ikkinchi bit F shifrlash funksiyasining chiqishidagi 17-chi bit bo'ladi. Shu sababli $\Delta X(8)_{17}$ ni aniqlash uchun S_1 blokining chiqishidagi ikkinchi bitlarni ikkining moduli bo'yicha qo'shing;

- ΔX_R ni qiymatini (demak, $\Delta Y(7)_3, \Delta Y(7)_8, \Delta Y(7)_{14}, \Delta Y(7)_{25}, \Delta Y(5)_3, \Delta Y(5)_8, \Delta Y(5)_{14}, \Delta Y(5)_{25}$ va $\Delta X(5)_{17}$ larni qiymatlarini ham) bilgan holda $\Delta X(7)_{17}$ ni hisoblang;
- Agar $\Delta X(7)_{17} \oplus \Delta X(8)_{17}$ yig'indi ΔY_L ayirmaning 17-chi bitiga teng bo'lsa, ushbu qismiy kalitga mos keluvchi hisoblagich qiymatini bittaga oshiring.

5. Eng katta qiymatga ega bo'lgan hisoblagich K_1 qismiy kalitni to'g'ri qiymatini aniqlash imkonini beradi.

6. Kalitning qolgan bitlari qo'shimcha tahlillarni bajarish orqali aniqlanishi mumkin.

Algoritm mualliflarini tasdiqlashiga ko'ra, $N=213,81$ ta ochiq matn juftligi mavjud bo'lganda ushbu algoritm bo'yicha hujum qilish 77,27% va undan yuqori hollarda muvaffaqiyatli bo'lishi mumkin.

Chiziqli-differensial kriptotahlil usuli bo'yicha ko'plab olimlar tadqiqotlar olib bormoqda. Ammo, ushbu usulni turli shifrlash algoritmlariga qo'llash etarlicha murakkab bo'lib, shifrlash algoritmi va uning xossalalarini chuqur o'rganishni talab qiladi.

Nazorat savollari

1. Chiziqli-differensial kriptotahlil usuli deb nomlanishini qanday izohlash mumkin?
2. Hozirgi vaqtda DES shifrlash algoritmiga hujum qilishning qanday samarali usullari mavjud?
3. Nima sababdan chiziqli-differensial kriptotahlilda ikkinchi yoki uchinchi bitlarda farq qilgan matn juftliklaridan yoxud ikkinchi yoki uchinchi bitlarda farq qilgan o'n qismlaridan foydalaniladi?
4. Chiziqli-differensial kriptotahlilni amalga oshirishda tenglamalar qanday quriladi?
5. Nimaning hisobiga (6.3) tenglamada $\Delta X(6)_{17}$ ning qiymatini topish mumkin bo'lib qoladi?

7-BOB. SLAYDLI HUJUMGA ASOSLANGAN KRIPTOTAHLIL USULI

XX asrning oxirida zamonaviy kompyuter va hisoblash tizimlarining unumdorligi oshishi bilan shifrlash algoritmlarining kriptobardoshligini yuqori darajada ta'minlash maqsadida raundlar sonini oshishi kuzatildi. Raundlar sonining oshishi bilan algoritmning bardoshligini tahlil qilishda statistik hujumlarga asoslangan chiziqli va differensial tahlil kabi kriptotahlil usullarining qo'llanilishi murakkablashadi. Masalan, 16 raundli DES shifrlash algoritmini buzish ancha murakkab masala hisoblanadi, ushbu algoritmning 32 va 48 raundli (ya'ni, ikkilangan va uchlangan DES) variantlari haqida gapirmasa ham bo'ladi.

AES shifrlash algoritmi tanlovida ishtirok etgan RC6 (20), MARS (32), SERPENT (32), CAST (48) kabi tezligi unchalik past bo'lмаган algoritmlarda ham katta sondagi raundlardan foydalanilganligini payqash mumkin.

Yuqorida keltirilgan sabablarga ko'ra shifrlash algoritmi raundlari soniga bog'liq bo'lмаган, yangi kriptotahlil usulini yaratish masalasi paydo bo'ldi. Ushbu masalani kelib chiqishi rossiyalik bo'lgan Aleks Biryukov va amerikalik taniqli kriptograf Devid Vagnerlar 1999 yilda ijobjiy hal qildilar [1]. Ular tomonidan taklif qilingan kriptotahlil usuli «slaydli hujum» yoki «sirpanuvchi hujum» (Slide Attacks) deb nomланади. Ushbu usul barcha simmetrik blokli shifrlash algoritmlariga qo'llashga mo'ljallangan.

§7.1. Slaydli hujumga asoslangan kriptotahlilning asosiy g'oyasi.

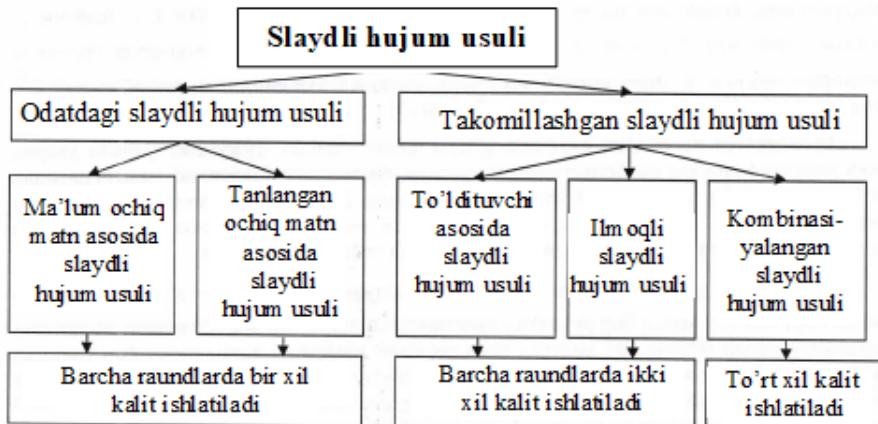
Odatdagи slaydli hujum

Chiziqli va differensial kriptotahlil usullarida asosiy e'tibor shifrlash jarayoni tahliliga qaratilsa, slaydli hujumda esa shifrlashning har bir raundida bitta qismiy kalitga bog'liq bo'lgan kriptografik F-funksiyasidan foydalanishga asoslangan. Shifrlash algoritmini tuzilishiga bog'liq holda slaydli hujum qismiy kalitlarni

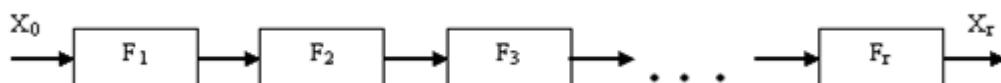
shakllantirish prosedurasining zaifligi hamda algoritmning umumiy tuzilish xossalardan foydalanishi mumkin.

Slaydli hujumning eng oddiy varianti har bir raundi bir xil K kalitga bog'liq bo'lgan F-funksiyalardan tashkil topgan r raundli shifrlash algoritmini tahlil qilishga mo'ljallangan. Bunday turdag'i shifrlash algoritmlari *gomogen shifrlash algoritmlari deb ataladi*.

Hozirgi kunda slaydli hujumning odatdag'i va yaxshilangan (takomillashgan) ko'rinishlari mavjud. Ularning ham o'z navbatida bir necha turlari uchraydi (7.1-rasm).



7.1-rasm. Slaydli hujum usulining turlari.



7.2-rasm. Simmetrik blokli shifrlash algoritmi bo'yicha odatdag'i shifrlash sxemasi.

Simmetrik blokli shifrlash algoritmi bo'yicha odatdag'i shifrlash jarayoni 7.2-rasmida keltirilgan. Ushbu rasmdan ko'rilib turibdiki, n-bitli X_0 ochiq matn r raundli shifrlash algoritmi bo'yicha shifrlanishi natijasida X_r shifr matn hosil qilingan. Agar X_j sifatida shifrlashning j-chi raundidan keyin hosil bo'ladigan oraliq natijani belgilasak, u holda unga nisbatan quyidagi munosabat o'rinli bo'ladi:

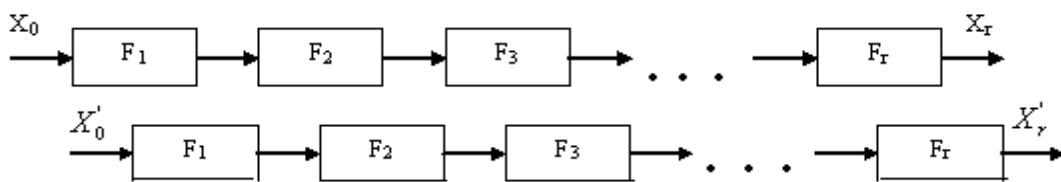
$$X_j = F_j(X_{j-1}, k_j), \quad (j = 1, 2, 3, \dots, r),$$

bu erda k_j – j-chi raund kaliti.

Agar $F(x_1, k) = u_1$ va $F(x_2, k) = u_2$ tengliklarning ma'lumligidan k'kalitni topish oson bo'lsa, u holda shifrlashda qo'llaniladigan *F funksiyasi zaif deyiladi*.

Odatdag'i slaydli hujum usuli

Odatdag'i slaydli hujum usulining asosiy g'oyasi bir vaqtning o'zida ikkita shifrlash jarayoni amalga oshirilib, shifrlash jarayonida jarayonlardan biri ikkinchisidan bir raundga kechiktirilishidan iborat.



7.3 - rasm. Odatdag'i slaydli hujum usuli sxemasi.

Agar 7.3-rasmda X_0 va X'_0 ochiq matnlarni anglatса, u holda shifrlashning j-chi raundidan keyin hosil bo'ladigan oraliq natijalar uchun $X_j = F(X_{j-1})$ va $X'_j = F(X'_{j-1})$ ($j = 1, 2, 3, \dots, r$) ni hosil qilish mumkin. Bu erda F funksiyada kalit tushirib qoldirilgan. Asosiy maqsad shifrlash jarayonida $X_1 = X'_0$ shartdan foydalananishdan iborat, u holda ularga mos keluvchi $X_j = X'_{j-1}$ shifr matnlari qiyamatlar juftligiga ega bo'lish mumkin bo'ladi.

Yuqoridagi fikrlarga asosan, $X_j = X'_{j-1}$ bo'lsa, u holda $X_{j+1} = F(X_j) = F(X'_{j-1}) = X'_j$ o'rini bo'lishini payqash mumkin.

Faraz qilaylik, (R, R') va (S, S') mos holda ochiq matn va shifr matn juftliklari bo'lsin. U holda $F(R) = S$, $F(R') = S'$, $S = R'$, $F(R) = R'$ va $F(S) = S'$ tengliklar o'rini bo'lsa, (R, S) va (R', S') juftliklar slaydjuftligi deyiladi.

Slaydli hujum quyidagi tarzda amalga oshiriladi. $2^{n/2}$ ta sondagi ochiq matn-shifr matn hosil qilinadi va undan slaydli juftlik izlanadi. Tug'ilgan kun parodoksiga asosan, shunday i, i' indekslar topilishi mumkinki, ushbu indekslar

uchun $F(P_i)=P_i$, va $F(C_i)=C_i$ shartlar qandaydir kalit uchun bir vaqtda bajariladi. Slaydli juftlik aniqlangandan so'ng kalitning qandaydir bitlarini topishga kirishish mumkin bo'ladi. Agar raund funksiyasi zaif bo'lsa, unda ushbu raund qismiy kalitining barcha bitlarini topish mumkin. Shifrlash kalitining qolgan bitlarini topish uchun keyingi slaydli juftlikni aniqlash va uning yordamida tahlilni davom ettirish lozim bo'ladi. Shunday qilib, shifrlash kalitining barcha bitlarini topish uchun kriptoanalitik oldida turgan masala bir necha slaydli juftlikni aniqlashdan iborat.

Ma'lum bo'lgan ochiq matn asosidagi hujum. Ma'lumki, Feystel tarmog'iga asoslangan blokli shifrlash algoritmlarida $F(l,r),k=((l \oplus f(r),r),k)$ shifrlash funksiyasi raund funksiyasiga kiruvchi ma'lumotning faqatgina yarmini o'zgartiradi. Shu bois, ma'lumotning x chap kismini ma'lumotning x' o'ng qismi bilan taqqoslash yordamida $F(x)=x'$ shartni osongina tekshirish mumkin. Ushbu shart ma'lum bo'lgan ochiq matn asosidagi xujumning murakkabligini $2^{n/2}$ ta sondagi ma'lum bo'lgan matngacha kamaytirish imkonini beradi.

Agar (R_i,S_i) va (R_j',S_j') juftliklar slayd juftlikni tashkil qilsalar, u holda, $F(R_i)=R_j'$ va $F(S_i)=S_j'$ o'rinli bo'lishi lozim. Feystel tarmog'iga asoslangan blokli shifrlash algoritmlari uchun slayd juftlikni aniqlash uchun (R_i,S_i) ma'lum bo'lgan matnlarni jadvalga kiritish lozim. Undan so'ng har bir j indeks uchun R_i va S_j' matnlarni o'ng yarim qismi R_j' va S_i matnlarni chap yarim qismi bilan teng bo'ladigan matnni topish kerak bo'ladi.

Agar ma'lum bir slaydli juftlik yordamida qismiy kalitning barcha bitlari topilmasa, u holda qolgan bitlarni aniqlash uchun boshqa slaydli juftlikdan foydalanish mumkin.

Tanlangan ochiq matn asosidagi hujum. Agar tanlangan ochiq matnlardan foydalanishning imkonи bo'lsa, Feystel tarmog'iga asoslangan blokli shifrlash algoritmlari uchun slaydli juftlikni aniqlash murakkabligini $2^{n/4}$ ta matngacha kamaytirish mumkin. Buning uchun x ma'lumotning $n/2$ bitli qiymatini ixtiyoriy tarzda tanlash zarur. Undan so'ng bir-birlari bilan faqatgina tasodifiy tanlangan o'ng va chap qismlari bilan farqlanadigan $2^{n/4}$ ta sondagi $P_i=(x,y_i)$ va $P_j'=(y_j',x)$ ochiq matnlardan tashkil topgan massivlarni saralash kerak. Natijada kriptoanalitik

ixtiyorida $2^{n/2}$ ta sondagi ochiq matnlar bo'ladi va ularni ichidan hech bo'lmaganda bitta slaydli juftlikni topish mumkin bo'ladi.

§7.2. Odatdagi slaydli hujumni S-DES-1 shifrlash algoritmiga qo'llanilishi

S-DES-1 shifri bo'yicha ma'lumotlar ikkinchi bobning 2.2-paragrafida to'liq keltirilgan. S-DES-1 shifrlash algoritmi Feystel tarmog'i asosida qurilganligi sababli tanlangan ochiq matn asosidagi hujumni bemalol unga nisbatan qo'llash mumkin. Ushbu algoritmda ochiq matn bloki uzunligi 16 bitni tashkil qiladi. Shifrlash jarayoni uchun algoritmga kiruvchi ochiq matn bloki har birining uzunligi 8 bitdan bo'lgan chap va o'ng qismiy bloklarga bo'linadi. S-DES-1 algoritmida dastlabki shifrlash kaliti uzunligi 10 bit bo'lib, undan ma'lum bir qoida asosida 8 bitli raund kalitlari hosil qilinadi. Mavzuni bayon qilish jarayonini soddalashtirish uchun to'g'ridan to'g'ri 8 bitli K raund kalitdan foydalanamiz (ya'ni, 10 bitli dastlabki shifrlash kalitidan 8 bitli qismiy kalit hosil qilish jarayonidan foydalanmaymiz). Shuningdek, shifrlanuvchi ma'lumotlarni raund kaliti bilan ikkining moduli bo'yicha qo'shish amali F-funksiyadan oldin emas, balki ushbu funksiyaning ichida bo'ladi. Algoritmning kriptografik bardoshligiga ta'sir qilmaganligi uchun boshlang'ich va yakuniy almashtirishlarni ham tushirib qoldiramiz hamda 20 raundan iborat kriptografik almashtirishdan foydalanamiz.

7.1-jadval. $R_i=(x,u_i)$ ochiq matnlar massivini K kalit bilan shifrlash natijalari.

Nº	X_L	X_R	Y_L	Y_R
1	1101	0110	0101	1100
2	1101	0001	1101	1110
3	1101	0010	1001	1010
4	1101	1000	0000	0111

7.2-jadval. $R_j' = (u_j', x)$ ochiq matnlar massivini K kalit bilan shifrlash natijalari.

Nº	X_L'	X_R'	Y_L'	Y_R'
1	1010	1101	1010	1101
2	0010	1101	0101	1111
3	1110	1101	1100	1000
4	1100	1101	0000	0011

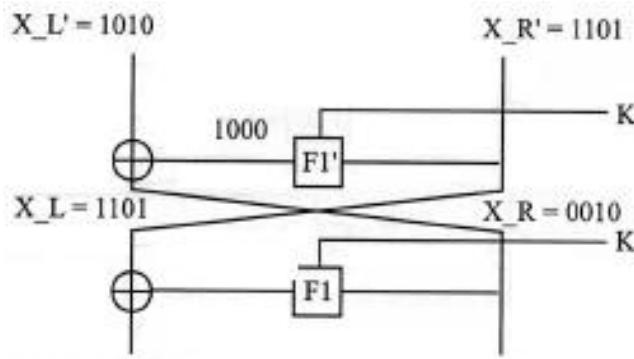
Birinchi navbatda ixtiyoriy ravishda to’rt bitli $x=1101$ matnni tanlaymiz. Undan so’ng bir-birlari bilan faqatgina tasodifiy tanlangan o’ng va chap qismlari bilan farqlanadigan $2^{n/4} = 2^{8/4} = 2^2 = 4$ ta sondagi $R_i = (x=X_L, u_i=X_R)$ va $R_j' = (u_j' = X_L', x = X_R')$ ochiq matnlardan iborat massivlarni shakllantiramiz. Endi tanlangan matnlarni 4 bitli qismlar (ularni har biri S-blok kirishiga ta’sir qiladi) dan iborat, tasodifiy tanlangan 8 bitli $K = (K_1, K_2)$ kalit bilan shifrlaymiz. $R_i = (x, u_i)$ va $R_j' = (u_j', x)$ ochiq matnlardan iborat massivlarni shifrlash natijalari mos holda 7.1- va 7.2-jadvallarda keltirilgan.

Shunday qilib, bizning ixtiyorimizda sakkiz juft matnlar mavjud. 7.1- va 7.2-jadvallarda keltirilgan shifrlash natijalarini tahlil qilib, slayd juftlik shartini ikkita matnlar juftligi qanoatlantirishini aniqlash mumkin.

Aniqlangan juftlikni tahlil qilishda S-DES-1 shifrlash algoritmi o’rniga qo’yish jadvali, ya’ni S bloklaridan foydalanishga to’g’ri keladi. Shu bois, qulaylik uchun ushbu bloklardagi kirish va chiqish mosliklari haqidagi ma’lumotlar 7.3-jadvalda keltirildi.

7.1-jadvaldagagi №1 va 7.2-jadvaldagagi №3 matnlar birinchi slaydli juftlikni tashkil qiladi. 7.1-rasmida keltirilgan shifrlash jarayonining birinchi ikki raundini o’rganib, ushbu juftlikni tahlil qilamiz.

X_R' va X_L matnlarning ma’lumligi F_1' funksiyaga kiruvchining qiymati haqida ma’lumot beradi. Shuningdek, X_R va X_L' matnlarning ham qiymati ma’lum. U holda F-funksiyadan chiquvchining qiymati, ya’ni 1000 ni osongina aniqlash mumkin.



7.4-rasm. Birinchi slaydli juftlik birinchi raundlarini tahlili.

F-funksiyadan chiqishdan oldin ma'lumotlar 7.4-jadvalga asosan o'rinn almashtirishga uchraydi. Bir qadam orqaga qaytib, S blokdan chiqishda 0100 qiymat paydo bo'lishini aniqlash mumkin, ya'ni ushbu vaziyatda 01 va 00 qiymatlar mos holda S_0 va S_1 bloklardan chiqishlar hisoblanadi.

7.3-jadval. S-DES-1 shifrlash algoritmining S bloklariga kirish va chiqish mosliklari.

S-blokka kirish	S_0 blokdan chiqish	S_1 blokdan chiqish
0000	01	01
0001	11	10
0010	00	01
0011	10	00
0100	11	10
0101	01	01
0110	10	11
0111	00	11
1000	00	11
1001	11	10
1010	10	00
1011	01	01
1100	01	01
1101	11	00
1110	11	00
1111	01	11

F-funksiyaga kiruvchi xabar 7.5-jadvalga asosan kengaytirib o'rinn almashtirishga uchraydi. Buning natijasida F-funksiyaga kiruvchi 1101 ma'lumot 11101011 ga almashadi. Kengaytirish natijasi $K=(K_1, K_2)$ kalit bilan qo'shib, ya'ni

S_0 blokka $1110 \oplus K_1$ kirib, S_1 blokka $1011 \oplus K_2$ kirib, ushbu bloklardan mos holda 01 va 00 qiymatlar chiqadi.

7.3-jadvaldan foydalanib, agar 0000, 0101, 1011, 1100 va 1111 qiymatlardan biri S_0 blokka kirsagina, undan chiqishda 01 qiymat paydo bo'lishini aniqlash mumkin. U holda S_0 blokka kiruvchi 0000, 0101, 1011, 1100 yoki 1111 qiymatlarning har birini 1110 bilan ikkining moduli bo'yicha qo'shib, K_1 qismiy kalitning bo'lishi mumkin bo'lgan qiymatlari 1110, 1011, 0101, 0010 yoki 0001 ni hosil qilish mumkin.

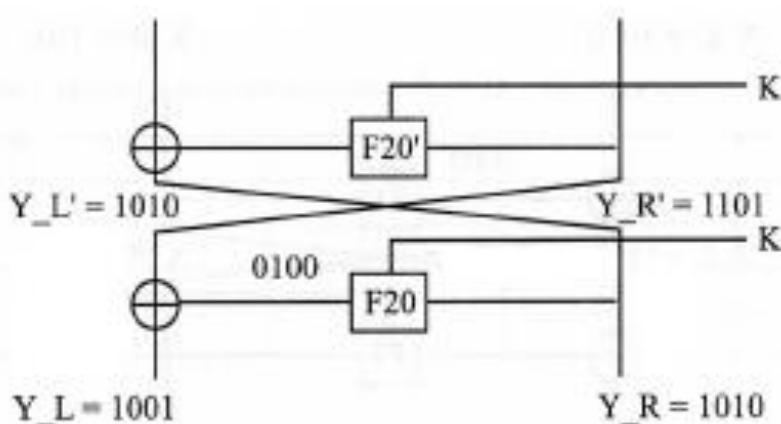
Xuddi shuningdek, 0011, 1010, 1101 yoki 1110 qiymatlardan biri S_1 blokka kirsagina, undan chiqishda 00 qiymat paydo bo'lishini payqash mumkin. U holda S_1 blokka kiruvchi 0011, 1010, 1101 yoki 1110 qiymatlarning har birini 1011 bilan ikkining moduli bo'yicha qo'shib, K_2 qismiy kalitning bo'lishi mumkin bo'lgan qiymatlari 1000, 0001, 0110 yoki 0101 ni hosil qilish mumkin.

7.4-jadval. S-DES-1 shifrlash algoritmi o'rin almashtirish jadvali.

P4			
2	4	3	1

7.5-jadval. E/P kengaytirib almashtirish jadvali.

E/P							
4	1	2	3	2	3	4	1



7.5-rasm. Birinchi slaydli juftlik oxirgi raundlarini tahlili.

Endi ushbu slaydli juftlik uchun shifrlashning oxirgi ikki raundi (bizning holimizda 20-chi raund) ni ko'rib chiqamiz (7.5-rasm).

Y_L' va Y_R matnlarning ma'lumligi F₂₀' funksiyaga kiruvchining qiymati haqida ma'lumot beradi. Shuningdek, Y_R' va Y_L matnlarning ham qiymati ma'lum. U holda F-funksiyadan chiquvchining qiymati, ya'ni 0100 ekanligini osongina aniqlash mumkin.

F-funksiyadan chiqishdan oldin ma'lumotlar 4-jadvalga asosan o'rinn almashtirishga uchraydi. Bir qadam orqaga qaytib, S blokdan chiqishda 0001 qiymat paydo bo'lishini aniqlash mumkin, ya'ni ushbu vaziyatda 00 va 01 qiymatlar mos holda S₀ va S₁ bloklardan chiqishlar hisoblanadi.

F-funksiyaga kiruvchi xabar 7.5-jadvalga asosan kengaytirib o'rinn almashtirishga uchraydi. Buning natijasida F-funksiyaga kiruvchi 1010 ma'lumot 01010101 ga almashadi. Kengaytirish natijasi K=(K₁,K₂) kalit bilan qo'shib, ya'ni S₀ blokka 0101⊕K₁ kirib, S₁ blokka 0101⊕K₂ kirib, ushbu bloklardan mos holda 00 va 01 qiymatlar chiqadi.

7.3-jadvaldan foydalanib, agar 0010, 0111 yoki 1000 qiymatlardan biri S₀ blokka kirsagina, undan chiqishda 00 qiymat paydo bo'lishini aniqlash mumkin. U holda S₀ blokka kiruvchi 0010, 0111 yoki 1000 qiymatlarning har birini 0101 bilan ikkining moduli bo'yicha qo'shib, K₁ qismiy kalitning bo'lishi mumkin bo'lgan qiymatlari 0111, 0010 yoki 1000 ni hosil qilish mumkin.

Xuddi shuningdek, 0000, 0010, 0101, 1011 yoki 1100 qiymatlardan biri S₁ blokka kirsagina, undan chiqishda 01 qiymat paydo bo'lishini payqash mumkin. U holda S₁ blokka kiruvchi 0000, 0010, 0101, 1011 yoki 1100 qiymatlarning har birini 0101 bilan ikkining moduli bo'yicha qo'shib, K₂ qismiy kalitning bo'lishi mumkin bo'lgan qiymatlari 0101, 0111, 0000, 1110 yoki 1001 ni hosil qilish mumkin.

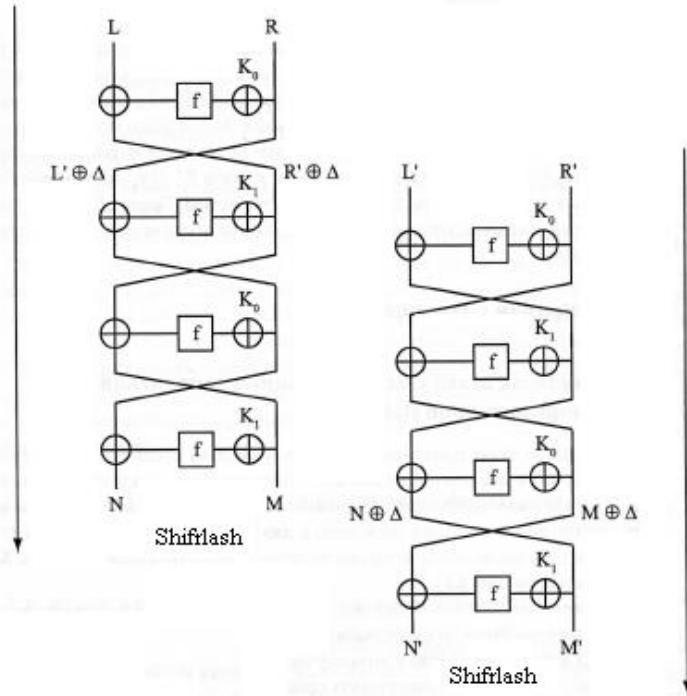
Shifrlashning barcha raundlarida bir xil kalitdan foydalanilgani uchun birinchi va oxirgi raundlarda K₁ va K₂ qismiy kalitlarning qiymatlari o'zgarmasdan qolishi lozim. K₁ va K₂ qismiy kalitlarning bo'lishi mumkin barcha qiymatlarini tekshirib ko'rish orqali faqatgina bitta K₁=0010 va K₂=0101 qiymatlardangina birinchi va oxirgi raundlarda foydalanish mumkinligi aniqlandi. Bu esa qidirilayotgan kalit

aynan K=00100101 ekanligini anglatadi. Yuqorida generasiya qilingan ochiq matnlarni ushbu kalit bilan shifrlab, shifrlash natijalarini taqqoslash orqali shifrlash kaliti to'g'ri topilganligiga ishonch hosil qilish mumkin. 7.1-jadvaldagi №3 va 7.2-jadvaldagi №1 matnlar ikkinchi slaydli juftlikni tashkil qiladi. Ushbu matn juftliklarini tahlil qilish ham yuqoridagi natijaga olib keladi. Buni o'quvchining o'zi mustaqil bajarib, ishonch hosil qilishi mumkin.

§7.3. Yaxshilangan slaydli hujumning asosiy g'oyasi

Qo'shimcha ma'lumotlardan foydalanuvchi slaydli hujum (Comrlemeptiop slide). Ushbu mavzuda ko'plab shifrlash algoritmlariga qo'llash uchun oddiy slaydli hujumni kengaytirishning bir necha usullari keltiriladi. Birinchi navbatda Feystel tarmog'iga asoslangan, ikki raundli o'z-o'ziga o'xhash shifrlash algoritmini tahlil qilishga mo'ljallangan usul bayon etiladi. Bu erda o'z-o'ziga o'xhash shifrlash algoritmi deyilganda 7.6-rasmda ko'rsatilgani kabi shifrlash jarayonida ikkita doimo almashinuvchi K_0 va K_1 qismiy kalitlardan foydalanuvchi algoritm nazarda tutiladi.

Odatdagi slaydli hujumni ikki raundli o'z-o'ziga o'xhash shifrlash algoritmi qo'llashda ikki raundga «kechikuvchi» ikkita shifrlash jarayonini taqqoslash mantiqan to'g'ri bo'lar edi, ammo ushbu holda hujum samarasiz bo'lar edi. Agar har bir raundda ikkita shifrlash jarayoni o'rtasida $\Delta = K_0 \oplus K_1$ ayirmadan foydalanilsa, bir raundga «kechikuvchi» shifrlash jarayonlarini taqqoslash imkonи mavjud. Ushbu holda ikki raundli o'z-o'ziga o'xhashlikdan bir raundli o'z-o'ziga o'xhashlikka o'tish mumkin. Shu bilan birgalikda slaydli juftliklarda shifrlash raundlari o'rtasida ayirmaga ega bo'lish mumkin.



7.6-rasm. O'z-o'ziga o'xhash shifrlash algoritmi.

Hujum qilish uchun shunday slaydli juftlikni tanlash kerakki, natijada ochiq matnlar ayirmasi kalitlar ayirmasini kompensasiya qilsin. Buning uchun slaydli ayirmasi (Δ , Δ) bo'lgan ochiq matnlarni topish lozim bo'ladi. Ma'lumki, agar $F(P) \oplus R' = \Delta$ bo'lsa, u holda R va R' ochiq matnlar juftligi Δ slaydli ayirmaga ega bo'ladi. Bunday slaydli ayirma $p=1$ ehtimollik bilan raunddan raundga o'tadi va natijada shifr matnlarni shu ayirmaga olib keladi. 7.6-rasmida ushbu kriptotahli usuli ochiq ko'rsatilgan.

Xuddi oldingi mavzularga o'xshab, $2^{n/2}$ ta ochiq matndan tashkil topgan massivdan slaydli juftlik ajratib olinishi mumkin. Agar ochiq va shifr matnlarni mos holda $R = (L, R)$ va $S = (N, M)$ bilan belgilasak, u holda quyidagi tengliklarga ega bo'lish mumkin:

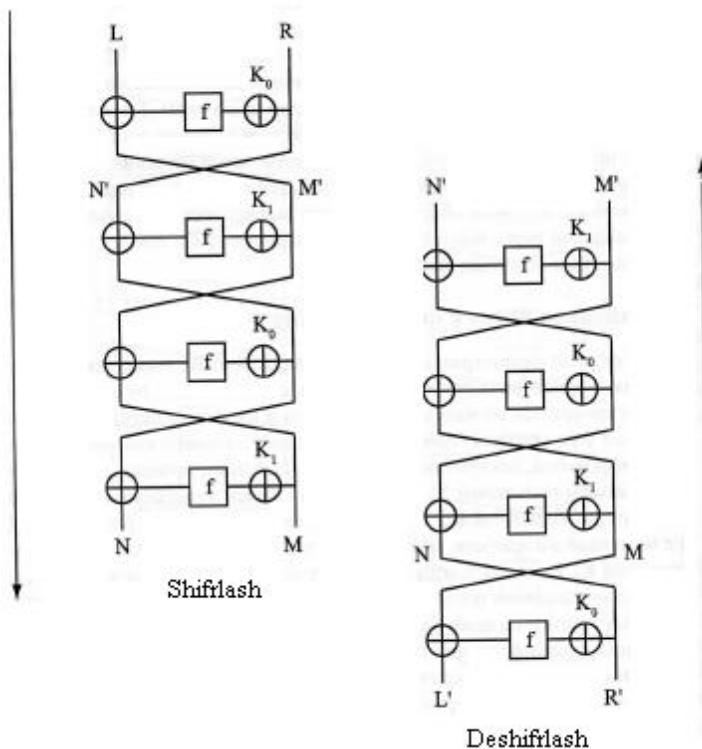
$$(L', R') = (R, L \oplus f(K_0 \oplus R)) \oplus (\Delta, \Delta), \quad (7.1)$$

$$(N', M') = (M \oplus f(K_1 \oplus N \oplus \Delta), N) \oplus (\Delta, \Delta). \quad (7.2)$$

Keltirilgan tenglamalardan ko'rinish turibdiki, $L' = R \oplus \Delta$ va $M' = N \oplus \Delta$. Natijada $L' \oplus M' = R \oplus \Delta \oplus N \oplus \Delta = R \oplus N$ ni hosil qilish mumkin. Bu esa slaydli juftlikni aniqlashning $n/2$ bitli shartidir. Topilgan slaydli juftlik L, R, M, N ,

L' , R' , M' va N' larning qiymatlarini beradi.

Ma'lumki, $R=L\oplus\Delta$ (7.6-rasm), demak, $\Delta=R\oplus L$. Ikkining moduli bo'yicha ikkita qiymat $L\oplus\Delta\oplus R'$ ni qo'shib, shifrlash raundining F funksiyasi chiqishida slaydli juftlikni hosil qilish mumkin. Bizga F funksiyaning almashtirishlari ma'lum va ular kalitga bog'liq emas. U holda slaydli juftlik shifrlashining birinchi raundi F funksiyasi kirishiga qanday qiymat kelib tushganligi haqida faraz qilish mumkin. Chunki ushbu funksiyaning kirishiga $R\oplus K_0$ yig'indi kelib tushadi, bu esa K_0 ning qiymati haqida faraz qilish imkonini beradi. Xuddi shunday mulohazalarni ikkinchi slaydli juftlikning oxirgi raundi haqida ham yuritib, F funksiyaning chiqishida $M\oplus\Delta\oplus N'$ yig'indi paydo bo'lislashi aniqlash mumkin. Ushbu funksiyaning kirishiga $M'\oplus K_1$ yig'indi kelib tushadi. Demak, K_1 ning qiymati haqida faraz qilish mumkin bo'ladi. K_0 va K_1 qismiy kalitlarning ilgari faraz qilingan qiymatlaridan ikkining moduli bo'yicha Δ qiymatni beradigan qiymatlarigina haqiqiy bo'ladi. Ko'rinish turibdiki, tahlildagi asosiy qiyinchilik to'g'ri slaydli juftliklarni topish bilan bog'liq bo'lib qolmoqda.



7.7-rasm. Ilmoqli slaydli hujum.

Ilmoqli slaydli hujum (Sliding with a Twist). Ushbu mavzuda Feystel tarmog’iga asoslangan, ikki raundli o’z-o’ziga o’xhash shifrlash algoritmini tahlil qilish uchun yana bitta slaydli hujum usuli keltiriladi.

Agar blokli shifrlash algoritmlariga ko’pchilik hollarda qo’llaniladigan boshlang’ich va yakuniy almashtirishlar e’tiborga olinmasa, Feystel tarmog’iga asosida qurilgan shifrlash algoritmlari uchun K_0 va K_1 qismiy kalitlardan foydalanuvchi deshifrlash jarayoni K_1 va K_0 qismiy kalitlardan foydalanuvchi shifrlash jarayoniga o’xhash bo’ladi. Shuni ham aytish mumkinki, Feystel tarmog’i asosidagi algoritmlar yordamida K_0 va K_1 qismiy kalitlardan foydalanuvchi shifrlash jarayoni ushbu algoritm bilan K_1 , K_0 qismiy kalitlardan foydalanib, shifrlash jarayoniga juda yaqin, ya’ni bunda jarayonlardan biri ikkinchisiga nisbatan bitta raundga «kechiktirilib» bajariladi. Shu boisdan, shifrlash va deshifrlash jarayonlaridan biri ikkinchisiga nisbatan bitta raundga «kechiktirilib», taqqoslanadi. Ushbu holda shifrlashning birinchi va deshifrlashning oxirgi raundlaridan boshqa barcha raundlarda slaydli juftliklar qisman ustma-ust tushadi. 7.7-rasmda qanday qilib, ushbu ikki jarayonni taqqoslash ko’rsatilgan.

Kriptotahlil hech bo’lmaganda bitta slaydli juftlikni topish uchun $2^{n/2}$ ta ochiq matndan iborat massivni yaratishdan boshlanadi. Izlanayotgan slaydli juftlik uchun quyidagi tengliklar o’rinli bo’lishi lozim:

$$(N', M') = (R, L \oplus f(K_0 \oplus R)). \quad (7.3)$$

$$(L', R') = (M \oplus f(K_0 \oplus N), N), \quad (7.4)$$

(7.3), (7.4) tenglamalar slaydli juftlik (ya’ni, $N' = R$ va $R' = N$) ni ajratish uchun n-bitli shartni beradi. Slaydli juftlikni aniqlab, bundan oldingi mavzuda bayon qilingan usul bilan K_0 qismiy kalitni bitlarini topish mumkin. Shifrlashning ikki raundiga «kechiktirilib», slaydli hujum qilish natijasida K_1 qismiy kalitni aniqlash mumkin. Bunda tahlil uchun ilgari yaratilgan matnlar massividan foydalanish mumkin.

Shuningdek, tanlangan ochiq matn–shifr matn asosida hujum qilish mumkin.

Ushbu holda talab qilinadigan matnlar soni $2^{n/4}$ tagacha kamayadi. Buning uchun faqatgina chap yarim qismi bilangina farqlanadigan $2^{n/4}$ sondagi (L_i , R) ochiq matnlardan tashkil topgan massivni yaratish va ularga mos keluvchi shifr matnlar qiymatini hosil qilish lozim bo'ladi. Shuningdek, faqatgina chap yarim qismi bilangina farqlanadigan $2^{n/4}$ sondagi (M_j' , N') (bu erda $N' = R$) shifr matnlardan tashkil topgan massivni yaratish va ularga mos keluvchi ochiq matnlar qiymatini hisoblash kerak. Bunday sondagi ochiq va shifr matnlarga ega bo'lgandan keyin hech bo'limganda bitta slaydli juftlikni topish mumkin bo'ladi. Keyingi bo'ladigan tahlillar oldingilariga o'xhash tarzda olib boriladi.

§7.4. To'rt raundli o'z-o'ziga o'xhash shifrlash algoritmiga slaydli hujumni qo'llash

Amaliyotda nafaqat bitta tahlil qilish usuli, balki maqsadga erishish uchun minimal xarajatlar sarf qilish imkonini beruvchi tahlil qilishning bir necha usullaridan birlagikda qo'llash, bir necha usullarning kombinasiyasidan foydalanish ko'p hollarda yaxshi natijalar beradi. Ushbu mavzuda Feystel tarmog'i asosida qurilgan, to'rt raundli o'z-o'ziga o'xhash shifrlash algoritmi (ayrim hollarda bunday algoritmlar (4K-Feystel shifr deb nomlanadi) ga to'ldiruvchi asosida va ilmoqli slaydli hujum usullari kombinasiyasiga asoslangan tahlilni o'rganamiz.

Albatta, shifrlash jarayonlaridan birini ikkinchisiga nisbatan ikki raundga «kechiktirib»,

$$K_0 \ K_1 \ K_2 \ K_3 \ K_0 \ K_1 \dots$$

$$K_0 \ K_1 \ K_2 \ K_3 \ K_0 \ K_1 \dots$$

oddiygina taqqoslash varianti ham mavjud. Undan so'ng ($K_1 \oplus K_3$, $K_0 \oplus K_2$) to'ldiruvchidan foydalanib, slaydli hujumni qo'llash mumkin. Ammo, bunday tahlilni o'tkazish uchun $2^{n/2}$ dan kam bo'limgan matn talab qilinadi va tahlil jarayonini o'zi ham ancha murakkab bo'ladi.

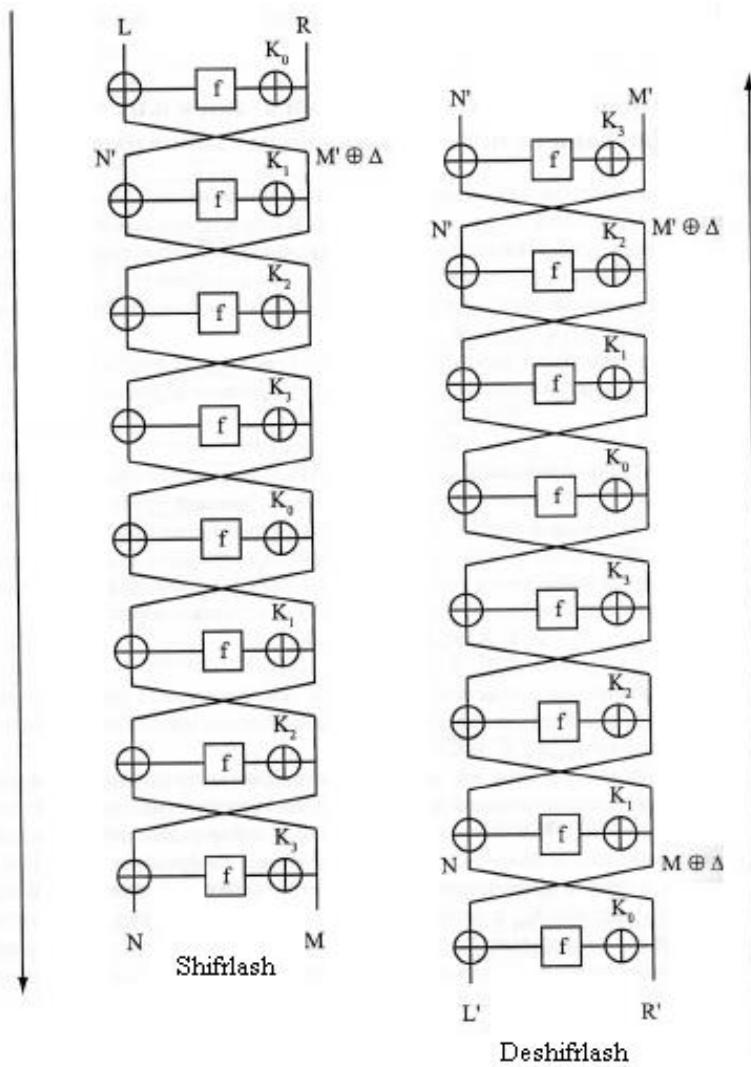
Ilmoqli slaydli hujumdan foydalanish eng yaxshi natijalarni beradi. Ammo,

ushbu usulni to'ldiruvchi asosidagi slaydli hujum bilan birlashtirib, quyidagicha qo'llash mumkin:

$$K_0 K_1 K_2 K_3 K_0 K_1 K_2 K_3 K_0 \dots$$

$$K_3 K_2 K_1 K_0 K_3 K_2 K_1 K_0 K_3 \dots$$

Bu erda yuqori qator shifrlash, pastki qator deshifrlash jarayoni (yoki K_3, K_2, K_1 va K_0 qismiy kalitlardan ketma-ket foydalanuvchi shifrlash jarayoni) ga mos keladi.



7.8-rasm. Slaydli hujumlarni kombinasiysi.

$(0, K_1 \oplus K_3)$ slaydli ayirmaga ega bo'lgan matnlar uchun to'ldiruvchidan foydalanuvchi slaydli hujumni qo'llash imkoniyati paydo bo'lganligini payqash mumkin. 7.8-rasmdan ko'rinish turibdiki, slaydli juftliklar orasida bunday ayirmaning tanlanishi ikkinchi slaydli juftlikning birinchi va birinchi slaydli

juftlikning oxirgi raundlarida K_3 qismiy kalitdan foydalanilgan bir vaqtda birinchi slaydli juftlikning ikkinchi va ikkinchi slaydli juftlikning oxiridan bitta oldingi raundlarida K_1 qismiy kalitdan foydalanilganligi bilan izohlanadi. Undan to'ldiruvchidan foydalanuvchi slaydli hujum hamda 7.8-rasmdan foydalanib, tahlilni o'tkazish mumkin.

Shifrlash algoritmini tahlil qilishning bunday yondoshuvi K_0 qismiy kalitni qiymatini aniqlash hamda K_1 va K_3 qismiy kalitlar qiymatlarini faraz qilish imkonini beruvchi Δ ning ham qiymatini topish imkonini beradi.

Nazorat savollari

1. Slaydli hujum deb nimaga aytildi?
2. Slaydli hujumning chiziqli va differensial kriptotahlil usullaridan asosiy farqi nimada?
3. Slaydli hujumni amalga oshirish uchun qanday shratlar bajatilishi lozim?
4. Hozirgi kunda slaydli hujumning qanday turlari mavjud?
5. F funksiyasi qachon zaif deyiladi?
6. Odatdagi slaydli hujum usulining asosiy g'oyasi nimadan iborat?
7. Slayd juftligi deb nimaga aytildi?
8. Feystel tarmog'iga asoslangan shifrga tahlil qlishda slaydli juftliklar qanday mezon asosida tanlanadi?
9. Slaydli hujum qanday tarzda amalga oshiriladi?
10. Ma'lum bo'lgan va tanlangan ochiq matn asosidagi slaydli hujumlarning mohiyati nimadan iborat?
11. Odatdagi slaydli hujumni S-DES-1 shifrlash algoritmiga qanday qo'llaniladi?
12. O'z-o'ziga o'xhash shifrlash algoritmi deyilganda qanday algoritm nazarda tutiladi?
13. Ilmoqli slaydli hujumning mohiyati nimadan iborat?
14. To'rt raundli o'z-o'ziga o'xhash shifrlash algoritmiga slaydli hujum qanday qo'llaniladi?

8-BOB. OCHIQ KALITLI RSA KRIPTOTIZIMIGA HUJUMLAR

TASHKILLASHTIRISH

RSA kriptotizimi ommaviyashgan ochiq kalitli kriptotizim hisoblanadi. Ushbu kriptotizim hozirgi kunda amaliyatga eng ko'p qo'llanilayotgan, dasturiy amalga oshirish eng samarali bo'lган ochiq kalitli kriptotizimdir [3,4,7-9]. Shu bois, ushbu kriptotizimni zaif tomonlarini o'rganish, kriptotizim xavfsizligini ta'minlovchi parametrlardan to'g'ri foydalanish ilmiy va amaliy ahamiyat kasb etadi.

Hozirgi kungacha RSA kriptotizimini buzuvchi jiddiy hujumlar bo'lмаган. Ushbu kriptotizimga nisbatan bir necha hujumlar bo'lishi mumkinligi bashorat qilingan. Ushbu hujumlar zaif ochiq matnlar, parametrlarni zaif tanlash yoki RSA kriptotizimiini noto'g'ri amalga oshirishga asoslangan.

Ushbu bobda hozirgi kundagi ma'lumotlarni shifrlash va raqamli imzolashda eng ommaviyashgan ochiq kalitli RSA kriptotizimiga bir necha turdag'i hujumlar tashkil qilishga bag'ishlangan. Ushbu hujumlar RSA kriptotizimini amalga oshirishdagi mavjud matematik zaifliklarga asoslanadi.

§8.1. RSA kriptotizimining xavfsizligi va uni buzish

RSA kriptotizimining xavfsizligi umumiyligi modul sifatida foydalaniladigan n sonining qiymati kattaligi, ya'ni bu sonni ko'paytuvchilarga yoyish masalasi amalda imkon yo'qligiga asoslanadi. Agar buzg'unchi n sonini ko'paytuvchilarga yoyib, p va q tub sonlarini qiymatlarini aniqlasa, u holda u $\varphi(n) = (p-1)(q-1)$ Eyler funksiyasini hisoblashi mumkin bo'ladi. Buning natijasida $d = e^{-1} \bmod \varphi(n)$ tenglik orqali yopiq kalit d ni hisoblashi mumkin bo'lar edi. Chunki, ochiq kalit e barcha foydalanuvchilarga ma'lum. Shu bois, RSA kriptotizimining xavfsizligini ta'minlash maqsadida modul n soni o'nlik sanoq tizimidagi raqamlardan tashkil topgan 300 xonali sondan katta bo'lishi lozim. Bu degani modul n sonining

uzunligi kamida 1024 bit bo'lishi kerak. Hozirgi kundagi mavjud eng tezkor kompyuterdan foydalanilganda ham bu uzunlikdagi butun sonni tub sonlar ko'paytmasi ko'rinishida yoyish amalga oshirib bo'lmaydigan katta vaqtni talab qiladi. Shu sababli butun sonni tub sonlar ko'paytmasi ko'rinishida yoyishning samarali algoritmi paydo bo'limguncha, RSA kriptotizimi xavfsiz bo'lib qolaveradi.

RSA kriptotizimini buzish usullari. RSA kriptotizimini buzishning bir necha usullari mavjud. Eng samarali usul: ochiq kalitga mos keluvchi maxfiy, yopiq kalitni topish usuli. Ushbu usul hujum qiluvchiga ochiq kalit bilan shifrlangan barcha xabarlarni o'qish va raqamli imzoni qalbakilashtirish imkonini beradi. Bunday hujumni tashkil qilish mumkin. Buning uchun hujum qiluvchi kriptotizimni moduli sifatida foydalaniladigan n sonini ko'paytuvchilari p va q sonlarini bilishi kerak bo'ladi. Ushbu sonlarni bilgan holda yopiq kalit d ni hujum qiluvchi osongina hisoblashi mumkin. Asosiy qiyinchilik n sonini ko'paytuvchilarga yoyishdir. Ushbu masala hozirgi kunda samarali echimi mavjud bo'limgan, murakkab matematik masalalar qatoriga kiradi.

Amalda yopiq kalit d ni tiklash masalasi kriptotizimni umumiyligi moduli n sonini ko'paytuvchilarga yoyish bilan ekvivalentdir. Xuddi shuningdek, umumiyligi modul n sonini ko'paytuvchilarga yoyish masalasi yopiq kalit d dan foydalanishni taqoza qiladi.

Shuni alohida qayd qilish lozimki, agar RSA kriptotizimida foydalaniladigan kalitlar etarlicha uzunlikga ega bo'lsa, hisoblash qurilmalarini takomillashtirish ushbu tizimni kriptobardoshligini kamaytirish uchun etarli bo'lmaydi. Aksincha, hisoblash qurilmalarini takomillashtirish RSA kriptotizimini kriptobardoshligini oshirishda juda katta imkoniyatlar yaratadi.

RSA kriptotizimida shifrmatn $C = M^e \pmod{n}$ formula bilan hisoblanganligi sababli, ochiq matn M ni tiklash masalasi M^e sonidan $\text{mod } n$ bo'yicha ildiz chiqarishni talab qiladi. Shu sababli RSA kriptotizimini buzishning boshqa usuli modul n bo'yicha e darajaga ko'tarishdan hosil bo'lgan sondan ildiz chiqarish usuliga asoslangan. Ildizni hisoblab, yopiq kalit d ni bilmagan holda shifrlangan xabarni ochish yoki raqamli imzoni qalbakilashtirish mumkin. Ushbu ko'rinishdagi

hujum faktorlash masalasiga ekvivalent bo'lmasa-da, ammo hozirgi kunda uning amaldagi echimi mavdjud emas.

RSA kriptotizimiga hujum uyushtirishning boshqa turlari ham mavdud. Masalan, hujum qiluvchiga boshqa shifrmatnlarni ochish imkonini bermaydigan, faqatgina bitta shifrmatnni ochish mumkin bo'lgan hujum. Bunday turdag'i bitta shifrmatnga qilinadigan eng oddiy hujum bu bo'lishi mumkin bo'lgan ochiq matnga qilinadigan hujumdir. Ushbu holda hujum qiluvchi o'zidagi shifrmatnda qandaydir ma'lum bir ochiq matnning shifrlangan qismi ham mavjud deb faraz qiladi. Ushbu farazga asosan hujum qiluvchi xabarni qabul qiluvchining ochiq kaliti bilan ochiq matnni shifrlaydi hamda hosil bo'lgan shifrmatn bilan o'zidagi haqiqiy shifrmatnni solishtiradi. Bunday turdag'i hujumni shifrlanishi lozim bo'lgan xabarni oxirida bir necha tasodifiy bitlarni qo'shish yo'li bilan bartaraf qilish mumkin.

Bitta xabarga asoslangan boshqa bir hujum kimdir bitta M xabarni o'zini bir necha kishiga shifrlangan holda jo'natishga asoslangan. Bu vaziyatda xabarni jo'natuvchi xabarni qabul qiluvchilarining har birining ochiq kalitlari yordamida M xabarni shifrlaydi. Ushbu holni bilgan hujum qiluvchi har xabarni tutib olib, ulardan foydalangan holda shifrmatnlardan ochiq M xabarni tiklashi mumkin. Bunday turdag'i hujumga qarshi turish uchun xabarni har safar shifrlashdan oldin xabarni oxirida bir necha tasodifiy bitlar ketma-ketligini qo'shish lozim.

Shuningdek, shifrmatnga asosan hujum qilishning bir necha usullari (raqamli imzoni soxtalashtirish maqsadida alohida shifrmatnlarga hujum) mavjud. Bunda hujum qiluvchi qandaydir shifrmatnni hosil qiladi va uning mos ochiq matniga ega bo'ladi. Masalan, ro'yxatdan o'tgan foydalanuvchi aldash yo'li bilan soxta xabarni ochishga majburlash orqali erishishi mumkin.

Xuddi shuningdek, bevosita RSA kritotizimining o'ziga emas, balki butun kommunikasiya tizimining zaifligiga yo'naltirilgan hujumlar ham mavjud. Bunday hujumlar RSA kritotizimini buzish sifatida qaralmasdan, balki uni konkret amalga oshirishdagi zaiflik sifatida qaralishi lozim. Masalan, agar yopiq kalit etarlichcha ehtiyyot choralarini asosida saqlanmasa, hujum qiluvchi ushbu kalitga ega bo'lishi mumkin.

§8.2. RSA kriptotizimiga hujumlar tashkil qilish

RSA kriptotizimi ëpiq shifrlash kalitini bilmasdan, shifrlangan matndan ochiq matnni tiklash (shifrmatnni siklik shifrlashga asoslangan hujum). Faraz qilaylik, buzg'unchiga (e, n) ochiq kalit juftligi va C shifrmatni ma'lum bo'lsin.

Masala: C shifrmatdan M ochiq matnni tiklash talab etilsin.

Ushbu masalani yechish uchun buzg'unchi $C^{e \cdot j} \pmod{n} = C$ munosabat o'rinli bo'ladigan j sonini saralash asosida tanlab oadi. Buning uchun buzg'unchi tutib olingan C shifrmatnni e ochiq kalit yordamida ketma-ket shifrlaydi. Buzg'unchi ochiq qaysi ekanligini bilmaydi. SHu sababli ketma-ket shifrlash jarayoni qandaydir j soni uchun dastlabki C shifrmatn hosil bo'lguncha, ya'ni quyidagi tenglik bajarilguncha davom etadi:

$$\left(\left(\left((C^e \pmod{n})^e \pmod{n} \right)^e \pmod{n} \dots \right)^e \pmod{n} \right) = C^{e \cdot j} \pmod{n} = C.$$

j soni topilgandan keyin buzg'unchi e ochiq kalit yordamida C shifrmatnni $j - 1$ marta ketma-ket shifrlaydi. $j - 1$ marta shifrlash natijasi ochiq matn M ni ifodalaydi. Bu esa quyidagi munosabatdan kelib chiqadi:

$$C^{e \cdot j} \pmod{n} = (C^{e \cdot (j-1)} \pmod{n})^e \pmod{n} = M^e \pmod{n}.$$

Ya'ni, $C^{e \cdot (j-1)} \pmod{n} = M$ ochiq matnga teng.

Ushbu hujum RSA kriptotizimi uchun jiddiy bo'lishi mumkinmi? Buzg'unchi tomonidan tutib olingan C shifrmatnni e ochiq kalit yordamida ketma-ket shifrlash jarayonining murakkabligi n sonini ko'paytuvchilarga yoyish masalasining murakkabligi bilan bir xil ekanligi tasdiqlangan. Shu sababli talab qilingan darajada yetarlicha katta tanlansa, ushbu turdag'i hujumni tashkil qilish hech qanday natija bermaydi.

Misol. $p=983$, $q=563$, $e=49$ bo'lsin. U holda $n=983 \cdot 563 = 553429$ modulga ega bo'lish mumkin. Ochiq matn $M=123456$ bo'lsin. Ushbu ochiq matnga mos keluvchi shifrmatn quyidagicha:

$$C = M^{49} \pmod{553429} = 1603.$$

Endi ushbu shifrmatndan ochiq matn M ni topish bilan shug'ullanamiz. Buning uchun shifrmatnni ochiq matn hosil bo'lguncha e ochiq kalit yordamida ketma-ket shifrlanadi. Shifrmatn 498 marta ($j=499$) shifrlangandan so'ng shifrlash natijasi sifatida dastlabki shifrmatn hosil bo'ldi:

$$C^{499} \pmod{553429} = 1603^{499} \pmod{553429} = C = 1603.$$

Endi C shifrmatnni $j-1=499-1=498$ marta e ochiq kalit yordamida ketma-ket shifrlab, ochiq matn M hosil qilinadi:

$$C^{498} \pmod{553429} = 1603^{498} \pmod{553429} = M = 123456.$$

Shifrmatnni tanlashga asoslangan hujum. RSA kriptotizimining mul'tiplikativ xossasidan foydalanib, unga nisbatan potensial hujum tashkil qilish mumkin. Faraz qilaylik, P matnni shifrlab, shifrmatn $C = P^e \pmod{n}$ ni Bobga jo'natdi. Eva ushbu shifrmatnni tutib oldi. Undan P matnni o'qish uchun quyidagicha ayyorona yo'l tutadi:

1. Eva Z_n gruppadan tasodifiy x sonini tanlaydi.
2. Eva $y = C \cdot x^e \pmod{n}$ ni hisoblaydi.
3. Eva y ni deshifrlash uchun Bobga jo'natadi.
4. Bob $z = y^d \pmod{n}$ ni hisoblab, uni Evaga jo'natadi.

Quyidagi hisoblashlarni bajarib, Eva osongina P ochiq matnga ega bo'ladi:

$$z = y^d \pmod{n} = (C \cdot x^e)^d \pmod{n} = (C^d \cdot x^{e \cdot d}) \pmod{n} = C^d \cdot x \pmod{n},$$

$$P = z \cdot x^{-1} \pmod{n}.$$

Ushbu hisoblashlarda x sonini teskarisini topish uchun Eva kengaytirilgan evklid algoritmidan foydalanadi.

§8.3. RSA kriptotizimiga Viner hujumi

RSA algoritmida ochiq kalit bilan bajariladigan amallarni tezlashtirish uchun ushbu ochiq kalitlar kichik tanlanadi. Ayrim hollarda ushbu kriptotizimdan foydalanilganda shifrlash jarayonini emas, balki dastlabki matnga o'girish jarayonini tezlashtirish kerak bo'ladi. Bunday hollarda ochiq kalit sifatida foydalaniladigan e soniga mos keluvchi yopiq kalit d ni kichik tanlash lozim. Bu esa ochiq kalit e ni qiymatini katta tanlashni talab qiladi.

Yopiq kalit d ni juda kichik tanlash ham maqsadga muvofiq emas. Chunki bunday hollarda yopiq kalit d ning qiymatini hujum qiluvchi saralash yo'li bilan aniqlab olishi mumkin.

Uzluksiz kasrlarga asoslangan Viner hujumini hisobga olgan holda yopiq kalit d ni qiymatini $\frac{1}{3}n^{\frac{1}{4}}$ dan (bu erda n – RSA kriptotizimi moduli) kichik bo'lgan sonlar orasidan tanlash kerak bo'ladi.

Bu erda esa uzluksiz kasrlar nazariyasidan quyidagi ma'lumotni keltirish o'rinni. Buning uchun haqiqiy $\alpha \in R$ soni bo'yicha quyidagi ketma-ketlikni hosil qilamiz:

$$\alpha_0 = \alpha, \quad p_0 = q_0 = 1, \quad p_1 = a_0 a_1 + 1, \quad q_1 = a_1,$$

$$a_i = [\alpha_i], \quad \alpha_{i+1} = \frac{1}{\alpha_i - a_i},$$

$$p_i = a_i p_{i-1} + p_{i-2} \quad \text{agar} \quad i \geq 2,$$

$$q_i = a_i q_{i-1} + q_{i-2} \quad \text{agar} \quad i \geq 2.$$

α sonlarini ifodalovchi a_0, a_1, a_2, \dots butun *sonlari uzluksiz kasr deyiladi*, $\frac{p_i}{q_i}$ rasional sonlari *mos keluvchi kasrlar deb nomlanadi*. Har bir mos keluvchi kasrlar qisqartirilmaydigan rasional sonlar bo'lib, ular maxrajlarining o'sish tezligini darajali funksiya bilan taqqoslash mumkin.

Agar qisqartirilmaydigan kasr $\frac{p}{q}$ quyidagi tengsizlikni qanoatlantirsa,

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{2q^2}$$

u holda $\frac{p}{q}$ kasr α sonlarini uzluksiz kasrga yoyishda mos keluvchi kasrlardan biri bo'ladi. Bu esa uzluksiz kasrlar nazariyasining yutuqlaridan biri hisoblanadi.

Viner RSA kriptotizimiga hujum qilishda uzluksiz kasrlardan foydalanishni taklif qilgan. Modul $n = pq$ bo'lib, $q < p < 2q$ bo'lsin. Faraz qilaylik, yopiq kalit d quyidagi tengsizlikni qanoatlantirsin:

$$d < \frac{1}{3}n^{\frac{1}{4}}.$$

Ushbu tengsizlik hujum qiluvchiga ham ma'lum bo'lsin. Shuningdek, RSA kriptotizimi qurilishiga ko'ra quyidagi tenglik o'rini:

$$e \cdot d = 1 \pmod{\varphi}. \quad (*)$$

Bu erda $\varphi = \varphi(N) = (p-1)(q-1)$. $e < \varphi$ deb hisoblaymiz, chunki ko'pchilik hollarda ushbu tengsizlik bajariladi.

(*) tenglikdan shunday k butun soni mavjudki, ushbu son uchun quyidagi tenglik o'rini bo'ladi:

$$e \cdot d - k \cdot \varphi = 1.$$

Demak,

$$\left| \frac{e}{\varphi} - \frac{k}{d} \right| = \frac{1}{d \cdot \varphi}.$$

$\varphi \approx n$ ekanligini hisobga olinsa, quyidagiga ega bo'lish mumkin:

$$|n - \varphi| = |p + q - 1| < 3\sqrt{n}.$$

Bu erdan shunday qilish mumkinki, $\frac{e}{n}$ kasr $\frac{k}{d}$ ga yaxshi yaqinlashadi. Haqiqatan ham

$$\begin{aligned} \left| \frac{e}{n} - \frac{k}{d} \right| &= \left| \frac{e \cdot d - k \cdot n}{d \cdot n} \right| = \left| \frac{e \cdot d - k \cdot \varphi - k \cdot n + k \cdot \varphi}{d \cdot n} \right| = \\ &= \left| \frac{1 - k \cdot (n - \varphi)}{d \cdot n} \right| \leq \left| \frac{3k\sqrt{n}}{d \cdot n} \right| = \frac{3k}{d\sqrt{n}}. \end{aligned}$$

$e < \varphi$ ekanligidan $k < d$ ekanligini payqash mumkin. Bundan tashqari farazga ko'ra

$$d < \frac{1}{3}n^{\frac{1}{4}}.$$

Demak,

$$\left| \frac{e}{n} - \frac{k}{d} \right| < \frac{1}{2d^2}.$$

$EKUB(k, d) = 1$ ekanligi hisobga olinsa, $\frac{e}{n}$ kasrni uzlusiz kasrga yoyishda $\frac{k}{d}$ mos keluvchi kasr bo'ladi. Shunday qilib, $\frac{e}{n}$ kasrni uzlusiz kasrga yoyib, mos keluvchi kasrlarni maxrajini qandaydir tasodifiy M soni uchun navbat bilan quyidagi

$$(M^e)^d = M \pmod{n} \quad (**)$$

ifodaga qo'yib, yopiq kalit d ni topish mumkin, ya'ni $(**)$ tenglik o'rinali bo'ladigan yopiq kalitni qiymatini aniqlash mumkin.

Tekshirish uchun kerak bo'ladigan mos keluvchi kasrlarni umumiyl sonini $O(\ln n)$ bilan baholash mumkin. Shunday qilib, yopiq kalit d uchun

$$d < \frac{1}{3} n^{\frac{1}{4}}$$

tengsizlik o’rinli bo’lsa, ushbu bayon qilingan usul bo’yicha RSA kriptotizimi yopiq kaliti d ni aniqlash chiziqli murakkablikka ega ekan.

Misol. RSA kriptotizimi moduli

$$n = 9449 \ 868410449$$

bo’lsin. Ochiq kalit $e=6792 \ 605 \ 526025$ ko’rinishda tanlangan bo’lsin.
Kriptotizimning yopiq kaliti

$$d < \frac{1}{3} n^{\frac{1}{4}} \approx 584$$

tengsizlikni qanoatlantirsin. $\alpha = \frac{e}{n}$ sonini uzlusiz kasrga yoyib, har bir mos keluvchi kasr maxrajini yopiq kalit d bo’lishi yoki bo’lmasligini tekshirib ko’ramiz.
 α sonini mos keluvchi kasrlari

$$1, \ \frac{2}{3}, \ \frac{3}{4}, \ \frac{5}{7}, \ \frac{18}{25}, \ \frac{23}{32}, \ \frac{409}{569}, \ \frac{1659}{2308}, \dots$$

ko’rinishda ekanligini aniqlash mumkin. Navbat bilan tekshirib, ettinchi mos keluvchi kasr maxraji $d = 569$ izlanayotgan yopiq kalit ekanligiga ishonch hosil qilish mumkin.

§8.4. Bir necha foydalanuvchilarga bir xil xabarni jo’natishga asoslangan hujum

Faraz qilaylik, Alisa bir xil m xabarni bir necha foydalanuvchilarga shifrlab jo’natishni xohlaydi. Ushbu foydalanuvchilarning modullari mos holda n_1, n_2, n_3 bo’lsin. Foydalanuvchilarning barchasining ochiq kaliti, bir xil, masalan $e = 3$ bo’lsin. U holda Alisa yuboradigan xabarlar quyidagicha bo’ladi:

$c_1 = m^3 \text{ mod } n_1$ 1-chi foydalanuvchi uchun,

$c_2 = m^3 \text{ mod } n_2$ 2-chi foydalanuvchi uchun,

$c_3 = m^3 \text{ mod } n_3$ 3-chi foydalanuvchi uchun.

Deyarli barcha n_1, n_2, n_3 modullar jufti-jufti bilan o'zaro tub bo'ladi.

Buzg'unchi Eva c_1, c_2, c_3 xabarlarni tutib olib, $m^3 \text{ mod } n_1 n_2 n_3$ ni topish uchun qoldiq had haqidagi xitoy teoremasidan foydalanishi mumkin. Chunki, $m < \min\{n_1, n_2, n_3\}$ bo'lganligi bois, $m^3 < n_1 n_2 n_3$ o'rinni bo'ladi. Bu esa Eva m butun sonini aniqlashini anglatadi. Bu sondan m butun sonini aniqlash murakkablik tug'dirmaydi.

Misol. Faraz qilaylik, foydalanuvchilarning modullari

$$n_1 = 137703491, n_2 = 144660611, n_3 = 149897933$$

hamda Eva tutib olgan shifrlangan xabarlar mos holda

$$c_1 = 124100785, c_2 = 85594143, c_3 = 148609330 \text{ bo'lsin.}$$

Quyidagi chiziqli taqqoslamalar sistemasining

$$m^3 \equiv c_1 \text{ mod } n_1, m^3 \equiv c_2 \text{ mod } n_2, m^3 \equiv c_3 \text{ mod } n_3$$

o'ng tomonlari va modullari ma'lum bo'lgan holda yechish uchun «*Mathematica*» tizimining *ChineseRemainderTheorem* funksiyasidan foydalanamiz. Buning uchun avvalo *NumberTheory'Functions'* paketini yuklaymiz:

```
<< NumberTheory'Functions'
```

```
n1 = 137703491; n2 = 144660661; n3 = 149897933;
```

```
c1 = 124100785; c2 = 85594143; c3 = 148609330;
```

```
mCybed = ChineseRemainderTheorem[{c1, c2, c3}, {n1, n2, n3}]
```

```
|| 1881563525396008211918161
```

Natijada $m^3 \equiv 18815635253960082119118161 \pmod{n_1 n_2 n_3}$ ni hosil qilish mumkin. $m^3 < n_1 n_2 n_3$ bo'lganligi sababli $m^3 \equiv 18815635253960082119118161$ ga ega bo'lish mumkin. Bundan m ni qiymatini osongina topish mumkin:

$$m = (\text{mCubed})^{1/3}$$

|| 123454321

Ushbu natijaning to'g'riliqini Mod funksiyasidan foydalanib, tekshirib ko'rish mumkin:

$$\text{Mod}[m^3, n1] == c1$$

$$\text{Mod}[m^3, n2] == c2$$

$$\text{Mod}[m^3, n3] == c3$$

|| True

|| True

|| True

§8.5. Ochiq kalit kichik bo'lganda bir-biriga bog'langan xabarlarga asoslangan hujum

Alisa ikkita xabarni Bobga shifrlab jo'natmoqchi. Faraz qilaylik, shifrlashda foydalaniladigan Bobning ochiq kaliti e_B kichik va moduli n_B bo'lsin. Shifrlanishi lozim bo'lgan m_1 va m_2 xabarlar bir-biri bilan chiziqli bog'langan, ya'ni $m_2 = a \cdot m_1 + b$ bo'lsin. Bu erda a va b sonlari Z_{nB} gruppaga tegishli bo'lib, chiziqli bog'lanish

buzg'unchi Evaga ma'lum bo'lsin.bo'lsin. Koppersmit va boshqalar Eva ochiq m_1 xabarni tiklashning quyidagi ikkita usulini bayon qilishgan [16].

Aniq usul. Avval ushbu usulni $e = e_B = 3$ holi uchun bayon qilamiz. m_1 va m_2 xabarlarga mos keluvchi shifrmatnlar mos holda c_1 va c_2 bo'lsin. U holda $c_1 = m_1^3 \text{ mod } n_B$ va $c_2 = (a \cdot m_1 + b)^3 \text{ mod } n_B$ bo'lib,

$$\frac{b(c_2 + 2a^3c_1 - b^3)}{a(c_2 - a^3c_1 + 2b^3)} \equiv \frac{3a^3bm_1^3 + 3a^2b^2m_1^2 + 3ab^3m_1}{3a^3bm_1^2 + 3a^2b^2m_1 + 3ab^3} \equiv m_1 \text{ (mod } n_B).$$

Ushbu tenglikni «*Mathematica*» paketini *Simplify* funksiyasi orqali tekshirib ko'rish mumkin.

```
Clear[a, b, c1, c2, m1, m2];
```

```
Simplify[
```

```
b (c2 + 2 a3 c1 - b3) / (a (c2 - a3 c1 + 2 b3) ) //.{c1 -> m13,  
c2 -> (a * m1 + b)3 }]
```

```
|| m1
```

$m_1 = m$ va $m_2 = m+1$, ya'ni $a = b = 1$ bo'lgan holni alohida qayd qilish lozim.

Ushbu holda yuqoridaagi munosabat quyidagi taqqoslamaga keladi:

$$\frac{(m+1)^3 + 2m^3 - 1}{(m+1)^3 - m^3 + 2} \equiv \frac{3m^3 + 3m^2 + 3m}{3m^2 + 3m + 3} \equiv m \text{ (mod } n_B).$$

Misol. Faraz qilaylik, $n_B = 477310661$, m_1 va m_2 xabarlar $m_2 \equiv 3m_1 + 5 \text{ (mod } n_B)$ taqqoslama bilan bog'langan bo'lsin. Ya'ni, $a = 3$ va $b = 5$. Shifrmatnlar $c_1 = 5908795$, $c_2 = 374480016$ bo'lsin. U holda «*Mathematica*» paketini *Mod* va *Solve* funksiyalaridan foydalanib, m_1 ni qiymatini quyidagicha hisoblash mumkin:

```
Clear[c1, c2, f, g, m1, m2, a, b];
```

```

n = 477310661;
c1 = 5908795; c2 = 374480016;
a = 3; b = 5;
f = Mod [b (c2 + 2 a3 c1 - b3), n];
g = Mod [a (c2 - a3 c1 + 2 b2), n];
Solve [{f == g * m1, Modulis == n}, m1]
|| {{Modulis -> 477310661; m1 -> 321321321}}

```

Shunday qilib, $m_1 = 321321321$ aniqlandi. Bu haqiqatan ham izlangan echim ekanligini quyidagicha tekshirib, ishonch hosil qilish mumkin:

```

m1 = 321321321;
m2 = Mod[3 * m1 + 5, n]
PowerMod [m1, 3, n] == c1
PowerMod [m2, 3, n] == c2
|| 9342646
|| True
|| True

```

Agar $a = b = 1$ va $e = e_B > 3$ bo'lganda ham ushbu usul ishlaydi. $c_1 = m^e \text{ mod } n_B$ va $c_2 = (m+1)^e \text{ mod } n_B$ shifrmatnlar bilan ifodalanadigan $P(m)$ va $Q(m)$ ko'phadlar mavjud. Ushbu ko'phadlar o'rtaida $Q(m) = m \cdot P(m)$ chiziqli munosabat mavjud. $e = e_B = 5$ hol uchun ushbu ko'phadlar quyidagi ko'rinishga ega:

$$P(m) = c_2^3 + 2c_1c_2^2 - 4c_1^2c_2 + c_1^3 - 2c_2^2 + 9c_1c_2 + 8c_1^2 + c_2 - 2c_1,$$

$$Q(m) = 9c_1c_2^2 - 9c_1^2.$$

Buni ham «*Mathematica*» paketidan foydalanib, quyidagicha tekshirib ko'rish mumkin:

```
Clear [c1, c2, m];
```

$$P = c2^3 + 2 c1 c2^2 - 4 c1^2 c2 + c1^3 - 2 c2^2 + 9 c1 c2 + 8 c1^2 + c2 - 2 c1;$$

$$Q = 9 c1 c2^2 - 9 c1^2;$$

$$\text{Expand } [P // \{c1 \rightarrow m^3, c2 \rightarrow (m+1)^3\}]$$

$$\text{Expand } [Q // \{c1 \rightarrow m^3, c2 \rightarrow (m+1)^3\}]$$

$$\text{Simplify } [Q/P // \{c1 \rightarrow m^3, c2 \rightarrow (m+1)^3\}]$$

$$\begin{aligned} &|| \quad 9m^2 + 54m^3 + 135m^4 + 171m^5 + 135m^6 + 54m^7 + 9m^8 \\ &|| \quad 9m^3 + 54m^4 + 135m^5 + 171m^6 + 135m^7 + 54m^8 + 9m^9 \\ &|| \quad m \end{aligned}$$

e ning katta qiymatlari uchun bu usulni qo'llash amalda katta qiyinchiliklar bilan amalgalash oshadi.

§8.6. Eng katta umumiy bo'lувчи (EKUB)ni hisoblash orqali buzish usuli

Buzg'unchiga xabar qanoatlantiradigan polinomial taqqoslama ma'lum bo'lganda ochiq kalit e ning ixtiyoriy qiymati uchun c_1 va c_2 shifrmatnlardan m_1 va m_2 ochiq matnlarni to'g'ridan to'g'ri aniqlashning usuli mavjud.

Faraz qilaylik, $m_2 = f(m_1) \bmod n_B$ bo'lsin. Ushbu usulning asosiy g'oyasi $EKUB(z^e - c_1, (f(z))^e - c_2)$ ni hisoblashdan iborat. m_1 ikkala ko'phadning echimi bo'lganligi sababli, ushbu ko'phadlar $z - m_1$ ga bo'linadi. Bundan kelib chiqadiki, EKUB ham ushbu bo'lувchiga bo'linadi hamda EKUBning boshqa bo'lувchilari deyarli yo'q. Ushbu g'oyani quyidagi misolda ko'rsatamiz.

Misol. Faraz qilaylik, $e = 5$, $n_B = 466883$ bo'lsin. Shuningdek, m_1 va m_2 xabarlar $m_2 = 2m_1 + 3$ tenglik bilan bog'langan, mos keluvchi shifrmatnlar mos holda c_1 va c_2 bo'lsin. Biz $EKUB(z^5 - 66575, (2z + 3)^5 - 387933)$ ni hisoblashni xohlaymiz. n_B murakkab son bo'lganligi sababli «*Mathematica*» paketi ushbu hisoblashni to'g'ridan-to'g'ri amalga oshira olmaydi. Shu sababli Evklid algoritmining polynominal variantini qadamma-qadam amalga oshiramiz. Ayrim hollarda $n = n_B$ bilan o'zaro tub bo'limgan sonlar paydo bo'lganda muammolar paydo bo'lishi mumkin.

Avvalo $f_1 = (2z + 3)^5 - 387933$ $f_2 = z^5 - 66575$ funksiyalarni hisoblab, undan so'ng f_1 ni f_2 ga bo'lamiz. Buning uchun «*Mathematica*» paketining *Expand* va *PolynomialMod* funksiyalaridan foydalaniladi:

```

n = 466883;
c1 = 66575; c2 = 387933;
f1 = Expand [2 z + 3]^5 - c2]
f2 = z^5 - c1
f3 = PolynomialMod [f1 - 32 f2, n]
|| -387690 + 810z + 1080z^2 + 720z^3 + 240z^4 + 32z^5
|| - 66575 + z^5
|| 342061 ++ 810z + 1080z^2 + 720z^3 + 240z^4

```

Bo'lish jarayoni qulayroq bo'lishi uchun f_3 ni normallashtiramiz. Buning uchun f_3 ni n_B moduli bo'yicha teskarisini «*Mathematica*» paketining *PowerMod* funksiyasi yordamida katta koeffisientiga ko'paytiramiz:

```

InverseLeadCoeff = PowerMod [240, -1, n]
f3 = PolynomialMod [InverseLeadCoeff * f3, n]
|| 258731

```

$$|| \quad 376877 + 408526z + 233446z^2 + 3z^3 + z^4$$

Ushbu bo'lish jarayoni qandaydir k soni uchun $f_k = 0$ bo'limguncha davom ettiriladi. Natijada f_{k-1} izlanayotgan EKUB sifatida aniqlanadi.

$$f4 = \text{PolynomialMod}[f2 - f3 * (z + 466880), n]$$

$$|| \quad 130290 + 381818z + 291812z^2 + 233446z^3$$

$$\text{InverseLeadCoeff} = \text{PowerMod}[233446, -1, n]$$

$$f4 = \text{PolynomialMod}[\text{InverseLeadCoeff} * f4, n]$$

$$|| \quad 103752$$

$$|| \quad 184581 + 292352z + 116723z^2 + z^3$$

$$f5 = \text{PolynomialMod}[f3 - f4 * (z + 350163), n]$$

$$|| \quad 355162 + 4681z + 203714z^2$$

$$\text{InverseLeadCoeff} = \text{PowerMod}[203714, -1, n]$$

$$f5 = \text{PolynomialMod}[\text{InverseLeadCoeff} * f5, n]$$

$$|| \quad 349909$$

$$|| \quad 397084 + 98465z + z^2$$

$$f6 = \text{PolynomialMod}[f4 - f5 * (z + 18258), n]$$

$$|| \quad 451016 + 87731z$$

$$\text{InverseLeadCoeff} = \text{PowerMod}[87731, -1, n]$$

$$f6 = \text{PolynomialMod}[\text{InverseLeadCoeff} * f6, n]$$

$$|| \quad 132235$$

$$|| \quad 466340 + z$$

$$f7 = \text{PolynomialMod}[f5 - f6 * (z + 99008), n]$$

$$|| \quad 0$$

$k = 7$ hosil qilindi. Demak, $EKUB(z^5 - 66575, (2z + 3)^5 - 387933) \equiv EKUB(z^5 - 66575, (2z + 3)^5 - 387933) \equiv z + 466340 \equiv z - 543 \pmod{466883}$.

Shu sababli maxfiy xabar $m = 543$ dan iborat. Buni «*Mathematica*» paketining *PowerMod* funksiyasidan foydalanib, quyidagicha tekshirib ko’rish mumkin:

$m = 543$;

```
PowerMod [m, 5, n] == c1
PowerMod [2 m + 3, 5, n] == c2
|| True
|| True
```

Ochiq matn m ni izlash uchun EKUB ni hisoblashga asoslangan ushbu yondoshuvdan 32 bit uzunlikdagi *e* ochiq kalitlar uchun foydalanish mumkin.

Nazorat savollari

1. RSA kriptotizimiga hujumlar qanday zaifliklardan foydalanishga asoslangan?
2. RSA kriptotizimining xavfsizligi nimaga asoslangan?
3. RSA kriptotizimini buzishning qanday usullari mavjud?
4. RSA kriptotizimining yopiq kalitini topish masalasi qanday masalaga keltiriladi?
5. RSA kriptotizimida shifrmatr $C = M^e \pmod{n}$ dan ochiq matn M ni tiklash masalasi qanday masalaga keltiriladi?
6. RSA kriptotizimi yopiq shifrlash kalitini bilmasdan, shifrlangan matndan ochiq matnni tiklash nimaga asoslanadi?
7. RSA kriptotizimi yopiq shifrlash kalitini bilmasdan, shifrlangan matndan ochiq matnni tiklash imkonini qanday bartaraf qilish mumkin?

8. Shifrmatnni tanlashga asoslangan hujum RSA kriptotizimining qanday xossasidan foydalanishga asoslangan?
9. Viner hujumi nimaga asoslangan?
10. Uzluksiz kasr nima?
11. Viner hujumining mohiyatini tushuntirib bering.
12. Bir necha foydalanuvchilarga bir xil xabarni jo'natishga asoslangan hujumning mohiyati nimadan iborat?
13. Ochiq kalit kichik bo'lganda bir-biriga bog'langan xabarlarga asoslangan hujumning mohiyati nimadan iborat?
14. Eng katta umumiy bo'luvchi (EKUB)ni hisoblash orqali buzish usulida c_1 va c_2 shifrmatnlardan m_1 va m_2 ochiq matnlarni to'g'ridan to'g'ri aniqlash qanday amalga oshiriladi?

9-BOB. RSA RAQAMLI IMZOGA HUJUMLAR TASHKIL QILISH

Raqib RSA algoritmidagi n nodulni ikkita tub sonlarni ko'paytmasi ko'rinishida ifodalasa, u holda u maxfiy d parametrni aniqlashi va RSA kriptotizimini buzishi mumkin [3,9,12,13]. Ammo, hozirgi kunda katta tub solarni ko'paytmasidan tashkil topgan n nodulni tub ko'paytuvchilarga yoyish amalda imkonsiz masala hisoblanadi. Ushbu bobda n nodulni tub ko'paytuvchilarga yoyishdan foydalanmasdan, RSA raqamli imzoga bir necha hujumlar uyushtirish masalalari o'rganiladi. Ushbu hujumlar RSA algoritmidan noto'g'ri foydalanish bilan bog'liq.

§9.1. Notarius sxemasi bo'yicha RSA raqamli imzosiga hujum uyushtirish

Faraz qilaylik, hujjatlarni elektron imzolaydigan notariusga buzg'unchi qandaydir N soni ko'rinishidagi hujjatni elektron ko'rinishda tasdiqlatishni istaydi. Ammo, notarius ushbu hujjatni imzolashni istamaydi. Buzg'unchiga notariusning (e, n) ochiq kalit juftligi ma'lum bo'lsin.

Masala: N hujjatni notariusga imzolatish talab etiladi.

Buzg'unchi N soni bilan o'zaro tub bo'lgan qandaydir x sonini tanlaydi. Ushbu x sonidan foydalanib, quyidagi sonni hisoblaydi:

$$y = x^e \pmod{n}.$$

Hisoblangan y soni va N hujjatdan foydalanib, yangi M hujjatni shakllantiradi:

$$M = y \cdot N \pmod{n}.$$

Endi M hujjatni imzolatish uchun notariusga jo'natadi. Hujjatni qabul qilgan notarius ushbu hujjat N emasligini ko'rib, uni imzolaydi va imzolangan hujjat

$$s = M^d \pmod{n} = (y \cdot N)^d = (x^e)^d N^d = x \cdot N^d \pmod{n}.$$

ni buzg'unchiga jo'natadi.

Imzolangan hujjatni qabul qilgan buzg'unchi x soniga modul n bo'yicha teskari bo'lган x^{-1} sonini M hujjatni imzosi s soniga ko'paytirib, o'ziga kerakli N hujjatga mos keluvchi notariusning S imzosini hosil qiladi:

$$S = x^{-1} \cdot s = x^{-1} \cdot x \cdot N^d \pmod{n} = N^d \pmod{n}.$$

Ushbu turdag'i hujumdan himoyalanish uchun notarius imzolashdan oldin imzolanadigan hujjatga qandaydir son (masalan vaqt, sana) ni qo'shib imzolash lozim.

§9.2. Tanlangan shifrmattn bo'yicha RSA raqamli imzosiga hujum uyushtirish

Faraz qilaylik, buzg'unchiga C shifrmattn hamda xabarni jo'natuvchisining (e, n) ochiq kalit juftligi ma'lum bo'lsin.

Masala. M ochiq matnni topish talab qilinadi.

Ushbu masalani yechish uchun buzg'unchi n soni bilan o'zaro tub bo'lган qandaydir r ($r < n$) sonini tanlab, $x = r^e \pmod{n}$ ni hisoblaydi. Undan so'ng ushbu sondan foydalanib, $y = x \cdot C \pmod{n}$ sonini hisoblab, ushbu sonni buzg'unchi imzolatish uchun xabar jo'natuvchiga yuboradi.

Xabar jo'natuvchi hech narsadan shubhalanmasdan qabul qilingan y xabarni $s = y^d \pmod{n}$ ko'rinishda imzolaydi va ushbu imzoni buzg'unchiga jo'natadi.

Buzg'unchi s imzodan foydalanib, M ochiq matnni tiklaydi. Buning uchun s imzoni r soniga modul n bo'yicha teskari bo'lган r^{-1} soniga ko'paytirib, hosil bo'lган ko'paytmada y va x sonlarini qiymatlarini qo'yib hisoblashni davom ettiradi:

$$\begin{aligned} r^{-1} \cdot s(\text{mod } n) &= r^{-1} \cdot y^d (\text{mod } n) = r^{-1} \cdot x^d \cdot C^d (\text{mod } n) = \\ &= r^{-1} \cdot r^{e \cdot d} \cdot C^d (\text{mod } n) = C^d (\text{mod } n) = M . \end{aligned}$$

Ko'rinib turibdiki, buzg'unchi C shifrmatnni o'zini xabar jo'natuvchiga jo'natmaydi. Chunki xabar jo'natuvchi buni payqab qolishi mumkin. Shu sababli buzg'unchi C shifrmatnni xabar jo'natuvchiga niqoblab jo'natadi.

Ushbu turdag'i hujumdan himoyalanish uchun xabarni jo'natuvchi qandaydir tasodify vektor yoki xesh-funksiyadan imzolashda foydalanishi lozim.

§9.3. RSA kriptotizimi va raqamli imzosi xavfsizligini ta'minlash uchun taklif qilingan tavsiyalar

RSA kriptotizimini xavfsizligi quyidagi g'oyaga asoslangan: modul shunday katta sonki, uni «qisqa» vaqtda ko'paytuvchilarga yoyish imkonsiz.

Faraz qilaylik, haqiqiy foydalanuvchi Bob p va q tub sonlarini tanlab, $n = p \cdot q$ ni hisoblaydi. Bu erda n soni axborot almashinuvida ishtirok etuvchi barcha foydalanuvchilarga ma'lum, ammo p va q tub sonlari maxfiy.

Agar buzg'unchi Eva n sonini ko'paytuvchilarga yoyishni uddalay olsa, p va q tub sonlari qiymatlarini aniqlay oladi. Natijada $\varphi(n) = (p-1)(q-1)$ hisoblab, e' ochiq kalit orqali $d = e^{-1} \text{ mod } \varphi(n)$ yopiq kalitni qiymatini aniqlaydi. Buning natijasida Bob tomonidan shifrlangan barcha ma'lumotlarni dastlabki matnga o'girish imkoniga ega bo'ladi.

Ko'paytuvchilarga yoyishni ko'pgina algoritmlari mavjud. Ammo, ularning birortasi vaqtning polinomial murakkabligi bilan katta butun sonni ko'paytuvchilarini amalda topish imkonini bermaydi.

RSA kriptotizimini xavfsizligi ta'minlash uchun n soni 300 xonali sondan katta bo'lishi talab etiladi. Bu degani modul kamida 1024 bit bo'lishini anglatadi. Hozirgi kundagi mavjud eng tezkor kompyuterdan foydalanilganda ham bunday

katta sonni ko'paytuvchilarga yoyish amalga oishirib bo'lmaydigan katta vaqt ni talab qiladi. Bu esa ko'paytuvchilarga yoyishning samarali algoritmi topilmaguncha RSA kriptotizimi xavfsiz bo'lib qolishini bildiradi.

Nazariy va eksperimentlar natijasida hozirgi kunda RSA kriptotizimini xavfsizligini ta'minlash bo'yicha quyidagi tavsiyalar mavjud:

1. Modul sifatida foydalaniladigan n sonidagi bitlar soni kamida 1024 bo'lishi lozim. Bu n soni taxminan 2^{1024} ga teng yoki o'nlik sanoq tizimidagi 309 xonali son bo'lishini anglatadi;

2. p va q tub sonlari har birining uzunligi kamida 512 bitdan kam bo'lmasligi kerak. Bu p va q tub sonlari har biri 2^{512} ga teng yoki o'nlik sanoq tizimidagi 154 xonali son bo'lishini anglatadi;

3. p va q tub sonlarining qiymatlari bir-biriga yaqin bo'lmasligi kerak;

4. p/q nisbat kichik surat yoki maxrajga ega bo'lgan rasional songa yaqin bo'lmasligi lozim;

5. Ochiq kalit sifatida foydalaniladigan e sonining qiymati $2^{16} + 1$ ga teng yoki unga yaqin bo'lishi lozim;

6. Agar yopiq kalit d oshkor bo'lsa, tezda n, e, d parametrlarni qiymatlarini o'zgartirish kerak.

Nazorat savollari

1. Notarius sxemasi bo'yicha RSA raqamli imzosiga hujum uyushtirish nimaga asoslangan?

2. n nodulni tub ko'paytuvchilarga yoyishdan foydalanmasdan, RSA raqamli imzoga hujumlar uyushtirish mumkinmi?

3. Notarius sxemasi bo'yicha RSA raqamli imzosiga hujumdan qanday himoyalanish mumkin?

4. Tanlangan shifrmattn bo'yicha RSA raqamli imzosiga hujumning mohiyati nimadan iborat?

5. Tanlangan shifrmatn bo'yicha RSA raqamli imzosiga hujumdan qanday himoyalanish mumkin?
6. RSA kriptotizimini xavfsizligi qanday g'oyaga asoslangan?
7. RSA kriptotizimini xavfsizligi ta'minlash uchun n sonining razriyadi qanaqa bo'lishi lozim?
8. Hozirgi kunda RSA kriptotizimini xavfsizligini ta'minlash bo'yicha qanday tavsiyalar mavjud?

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Бабенко Л.К., Ишукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. – М., «Гелиос АРВ», 2006. – 376 с.
2. Курьязов Д.М., Саттаров А.Б., Ахмедов Б.Б. Блокли симметрик шифрлаш алгоритмлари бардошлилигини замонавий криптотаҳлил усуллари билан баҳолаш. –Т., 2017. –224 б.
3. Jo'rayev G.U. Kriptografik protokollar. –Т., Fan va texnologiyalar. 2016. -142 b.
4. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. -М.: Издательский центр «Академия», 2009. -272 с.
5. Biham E., Shamir A. Differential Cryptanalysis of the Full 16-round DES //Crypto'92, Springer-Verlag, 1998, p. 487.
6. Matsui M. Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology // EUROCRYPT'93, Springer-Verlag, 1998, p. 38.
7. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши. –Т., Ўзбекистон маркаси. 2009. - 432 б.
8. Акбаров D.E., Xasanov P.F., Xasanov X.P., Ahmedova O.P. Криптографиянинг математик асослари. -Т., 2010. –210 бет.
9. Молдавян А.А., Молдавян Н.А. Введение в крипtosистемы с открытым ключом. Санкт -Петербург «БХВ-Петербург» 2005г. –288 с.
10. Фаниев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлар хавфсизлиги. -Т., Алоқачи, 2008. –282 б.
11. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. –СПб.: БХВ-Петербург, 2009. – 576 с: ил.
12. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие / Под ред. М.А. Иванова. М.: НИЯУ МИФИ, 2012. – 400 с.: ил.
13. Новиков Е.А., Шитов Ю.А. Криптографические методы защиты информации. Красноярск, 2008. – 178 с.

14. Токарева Н.Н. Симметрическая криптография. Краткий курс: учебное пособие / Новосиб. гос. ун-т. Новосибирск, 2012. –234 с.
15. Juraev G.U., Djabborov A.Kh. To A Differential Attack for Symmetric Block Cipher. OSR Journal of Computer Engineering (IOSR-JCE). Volume 22, Issue 5, Ser. I (Sep. – Oct. 2020), PP. 55-58. DOI: 10.9790/0661-2205015558.
16. Ищукова Е.А. Разработка и исследование алгоритмов анализа стойкости блочных шифров методом дифференциального криптоанализа. Диссертация кандидата технических наук: - М.: РГБ, 2007. – 210 с.