ACADEMIC RESEARCH IN EDUCATIONAL SCIENCES VOLUME 2 | ISSUE 5 | 2021
ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00938

O‘QUVCHILARNI MA’LUMOTLARNI DESHIFRLASH ALGORITMINI QO‘LLASHGA O‘RGATISHNI SODDALASHGAN USULI

Shokir Bobobekov
Jizzax davlat pedagogika instituti
sh.r.bobobekov@mail.ru

Feruz Raxmonkulov
Jizzax davlat pedagogika instituti
feruz0123@jspi.uz

ANNOTATSIYA

Maqolada ma’lumotlarni deshifrlash uchun Feystel tarmog‘iga asoslangan simmetrik blokli shifrlash algoritmining soddalashtirilgan varianti taklif etilgan va ushbu algoritm yordamida hosil qilingan shifrmatnlarga mos keluvchi ochiq matnlar ikkita juftligining bitta kalit bilan shifrlash sikllari orqali o‘tish jarayonida o‘zgarishlarining o‘xshash emasligi tahliliga asoslanib, differentsial kriptotahlilni bir va to‘rt raunddan iborat bo‘lgan blokli shifrlash algoritmlariga qo‘llash va katta ehtimollikka ega bo‘lgan differentsiallarni aniqlash usuli tadbiqi keltirildi.
Kalit so‘zlar: Feystel shifri, kriptografiya, kriptotahlil, shifrlash, deshifrlash, shifrmatn, kalit.

ABSTRACT

The article proposes a simplified version of the Feistel network-based symmetric block encryption algorithm for data decryption, and analyzes the similarity of changes in the transition of two pairs of plaintext encryption cycles using one algorithm through one-key encryption cycles. based on the application of differential cryptanalysis to block encryption algorithms consisting of one and four rounds and the application of the method of detecting high-probability differentials.
Keywords: Feistel’s cipher, cryptography, cryptanalysis cipher, decryption, ciphertext, key.

KIRISH

Hozirgi paytda axborotlarni himoyalashda ma’lumotlarni shifrlash algoritmlaridan keng foydalanilmoqda. Ushbu ishda esa differentsial kriptotahlilni bir

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00938

va to‘rt raunddan iborat bo‘lgan ba’zi blokli shifrlash algoritmlariga qo‘llash va katta ehtimollikka ega bo‘lgan differentsiallarni aniqlash usuli keltirilgan.

ADABIYOTLAR TAHLILI VA METODOLOGIYA

Differensial kriptotahlil tushunchasi ilk bora 1990 yil Eli Bixam va Adi Shamir tomonidan kiritilgan [1]. Ular “to‘g‘ridan-to‘g‘ri” hujum usulidan ko‘ra, DES algoritmi hujum usulini samarali deb hisoblagan.

Usulning asosini tanlangan ochiq matn asosidagi hujum tashkil qiladi. Differensial kriptotahlil g‘oyasi dastlabki aniq tafovutlarga ega bo‘lgan ochiq matnlar ikkita juftligining bitta kalit bilan shifrlash sikllari orqali o‘tish jarayonida o‘zgarishlarining o‘xshash emasligi tahlilidan iborat. Ochiq matnlarni tanlashga hech qanday cheklov yo‘q. Ayrim pozisiyalarda tafovut bo‘lishi kifoya.

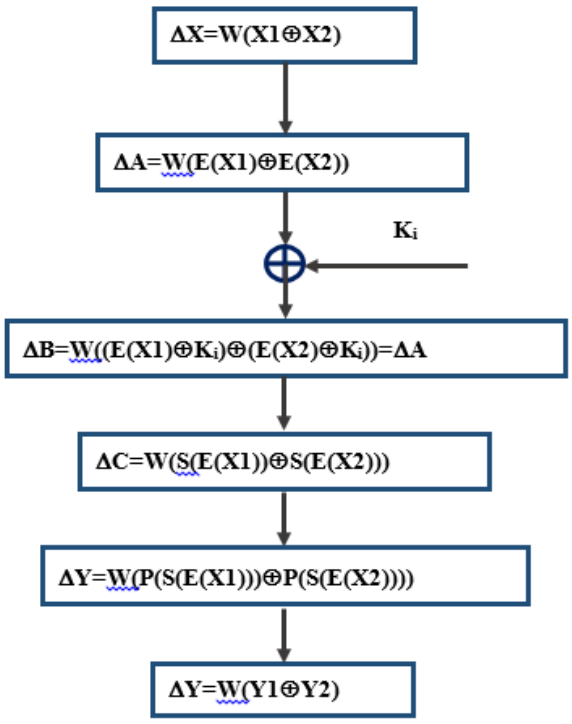
Shifrmatnlardan hosil bo‘lgan tafovutlardan kelib chiqib, kalitlarga turli ehtimolliklar beriladi. Haqiqiy kalit shifrmatnlar juftliklarini keyinchalik tahlil qilish jarayonida aniqlanadi – bu ko‘plab da’vogar kalitlar orasida ehtimoli eng yuqori bo‘lgan kalitdir. Differensial kriptotahlilni izohlash uchun DES kriptografik almashtirishining sikllaridan birini ko‘rib chiqamiz (1-rasm).

ΔX o‘xshash emasligidan iborat bo‘lgan X va X' kirish juftliklari berilgan bo‘lsin [1]. Mos holda Y va Y' chiqishlar, hamda, ΔY o‘xshash emaslik ham ma’lum. Shuningdek, P o‘rin almashtirish va E kengaytirish funksiyasi ham ma’lum, demak, ΔA va ΔC lar ham ma’lum. 2 ning moduli bo‘yicha (Xor bo‘yicha qo‘shish) chiqishdagi qiymatlar noma’lum, ammo ularning o‘xshash emasligi ΔB ma’lum va ΔA ga teng. Isbot qilinganki, har qanday berilgan ΔA uchun ΔS ning hamma qiymatlari ham bir xilda ehtimollikka ega emas. ΔA va ΔS 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.

Almashtirishning har bir siklida boshlang‘ich 56 bitli maxfiy kalitning 48 bitli qismiy kaliti ishtirok etadi. Shunday qilib, oxirgi raunddagi K_{16} kalitni ochib berish 56 bitli maxfiy kalitning 48 bitini tiklashga imkon beradi. Qolgan sakkiz bitni kuchli hujum orqali 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 bloki uchun jadval tuzish orqali, aniqlash mumkin bo‘ladi. Jadvallar quyidagi tamoyil bo‘yicha tuziladi: vertikal bo‘ylab ΔA ning, gorizontal bo‘ylab – barcha ΔC ning mumkin bo‘lgan kombinasiyalari, ularning kesishuvida esa – ΔC ning ΔA ga mos kelishlar soni joylashtiriladi.

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00938

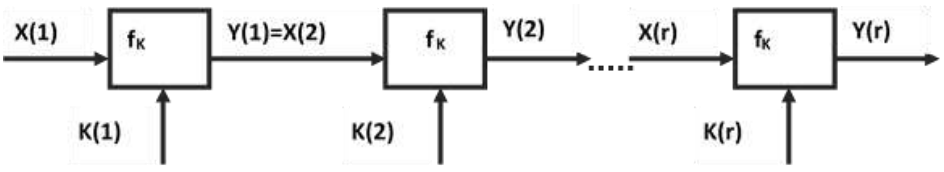


1-rasm.

Eng katta mos kelishlar soni ular yordamida maxfiy kalitni aniqlash mumkin bo‘lgan (ΔA; ΔC) juftlikini beradi. Ushbu juftlikga mos keladigan ochiq matnlar juftligi to‘g‘ri juftlik va aksincha, mos kelmaydigan ochiq matnlar juftligi esa noto‘g‘ri juftlik deb ataladi. To‘g‘ri juftlik siklning to‘g‘ri, noto‘g‘ri juftlik esa tasodifiy kalitini aniqlashga imkon beradi.

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‘rinib turibdiki, maxfiy kalitni muvaffaqiyatli ochib berish uchun katta miqdordagi ma’lumotlar kerak bo‘ladi.

Blok uzunligi N bo‘lgan ma’lum bir blokli shifrator 2-rasmda keltirilgan sxema bo‘yicha tuzilsin [1]. Bu yerda K = (K(1), K(2), ..., K(g)) ma’lum bir sxema bo‘yicha K_0 dan olinadi yoki mustaqil va teng ehtimollik bilan har bir sikl uchun tanlab olinadi. X(1) va X'(1) – ochiq matnlar juftligi bo‘lsin. Quyidagi har xilliklarni ko‘rib chiqamiz:



2-rasm.

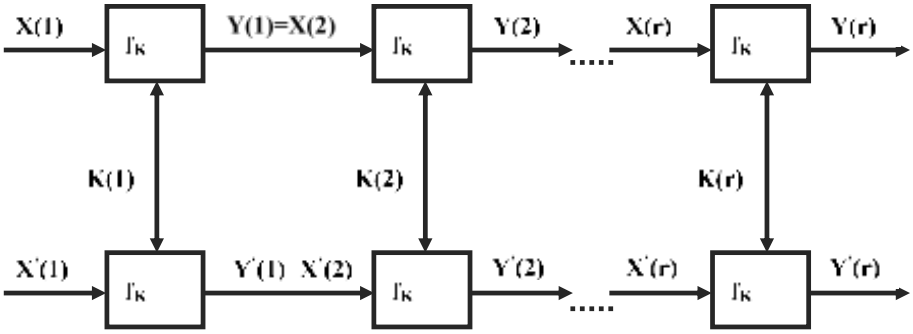
ΔX(1) = X(1)-X'(1);

ΔY(i) = Y(i)-Y'(i).

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00938

Differentsial kriptotahlil g‘oyasi shundan iboratki, tasodifiy teng ehtimolli X(1), K(1), K(2), ..., K(g-1) tanlashda $1/(2^N)$ dan katta ehtimol bilan ΔY(r-l) paydo bo‘ladigan ΔX(1) topish lozim.

Shunda differentsial tahlil quyidagi model bilan tavsiflanadi (3-rasm).



3-rasm.

Oxirgi shifrlash siklining quyikalitini quyidagi algoritmdan foydalanib topish mumkin:

1. Ehtimoliy R(ΔX(1) = α, ΔY(r-l) = β) katta bo‘lgan (r-1)-sikl (α, β) uchun differentsial tanlaymiz.
2. Tasodifiy ravishda X(1) tanlaymiz va X'(1) shunday tanlaymizki, ΔX(1) = α bo‘lsin. Y(r) va Y'(r) ma’lum bo‘lsin.
3. ΔY(r-l) = β deb taxmin qilamiz va Y(r) va Y'(r)ni bilgan holda K(r) topamiz.
4. 2 va 3 punktlarni to quyikalitlardan biri boshqalardan ko‘proq uchray boshlamagunga qadar takrorlaymiz.

Yuqorida keltirilgan algoritm bir qarashda sodda bo‘lib ko‘rinishiga qaramay, bir qator sezilarli muammolar mavjud. Birinchidan, yetarli hajmda ma’lumot to‘planmagunga qadar to‘g‘ri quyikalitni ajratishnning imkoni yo‘q. DES ga hujumda bo‘lishi mumkin bo‘lgan 2^{48} kalitlar ehtimolini saqlash uchun hisoblagichlardan foydalanish zarur, buning ustiga, ochish uchun ham juda ko‘plab ma’lumotlar talab qilinadi. Bixam va Shamir o‘zlarining hujum usulini taklif etdilar. 16-ranudli DES ning 15-raundli differentsialidan foydalanish o‘rniga ular 13- raundli differentsialdan va keyingi bir nechta raunddan o‘tish uchun qator usullardan foydalandilar. Ular shuningdek, bir onda testdan o‘tkazish mumkin bo‘lgan potensial 56-bitli kalitlar olish uchun ayrim ayyorona matematik usullardan foydalandilar. Shunday qilib, hisoblagichlarga ehtiyoj bartaraf etiladi. Bunday hujum to‘g‘ri juftlik topilishi bilan muvaffaqiyatga erishadi. Biroq to‘liqroq axborot keltirilmaydi, Bixam va Shamir differentsial kriptotahlilni qanday qilib amalga oshirgani haqida esa faqat aql yugurtirib bilish mumkin bo‘ladi.

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00938

NATIJALAR

Endi “ACADEMICIA MAY 2020 FULL JOURNAL” jurnalida e’lon qilingan maqolaga differentsial kriptotahlilni bir va to‘rt raunddan iborat bo‘lgan ayrim blokli shifrlash algoritmlariga qo‘llash va katta ehtimollikka ega bo‘lgan differentsiallarni aniqlash usuli tadbiqini ko‘rib chiqamiz [2].

Biz ishni $F(R_{i-1},K_i)$ - blok ΔX (ΔX=000000, 000001,…,111111) kirishining shu blokka ΔY (ΔY=000000, 000001,…,111111) chiqishiga bog‘liqligini, ya’ni optimal juftligini (ΔX, ΔY) aniqlashdan boshlaymiz [1]. Biz ΔX =000001 teng bo‘lgan barcha kirish juftliga mos ΔY chiqish natijalarini aniqlaymiz. Hisoblash qulay bo‘lishi uchun oldin almashtirish bloklari chiqishlarining kiruvchi ma’lumotlarga bog‘liqligini aks ettiradigan 1-jadvalni tashkil etamiz.

S_1 blokiga kirish	**S_1 blokdan chiqish**	**S_2, S_3 bloklariga kirish**	**S_2 blokdan chiqish**	**S_3 blokdan chiqish**
0000	10	000	10	01
0001	11	001	01	10
0010	11	010	11	10
0011	01	011	10	01
0100	10	100	11	10
0101	11	101	10	11
0110	01	110	01	11
0111	10	111	11	10
1000	01			
1001	11			
1010	10			
1011	01			
1100	01			
1101	10			
1110	11			
1111	01			

1-jadval.

Jadvalni hosil qilganimizdan so‘ng kalitsiz holatda $F(R_{i-1},K_i)$ ga kiruvchi barcha X larning unga mos Y chiquvchilarni hisoblaymiz (2-jadval). Ushbu hosil qilingan jadval optimal juftliklarni aniqlashda qo‘l keladi.

№	X kirish	Y chiqish	№	X kirish	Y chiqish	№	X kirish	Y chiqish	№	X kirish	Y chiqish
1	000000	011010	17	010000	110001	33	100000	110011	49	110000	011011
2	000001	110011	18	010001	111011	34	100001	111000	50	110001	110001
3	000010	011110	1	010010	110101	3	100010	110111	5	110010	011111

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00938

			9			5			1		
4	000011	110111	20	010011	111111	36	100011	111100	52	110011	110101
5	000100	001110	21	010100	100101	37	100100	100101	53	110100	101111
6	000101	100111	22	010101	001111	38	100101	001110	54	110101	100101
7	000110	011010	23	010110	110001	39	100110	110001	55	110110	111011
8	000111	110011	24	010111	011011	40	100111	011010	56	110111	110001
9	001000	011110	25	011000	110101	41	101000	110111	57	111000	011111
10	001001	110111	26	011001	111111	42	101001	111100	58	111001	110101
11	001010	001110	27	011010	100101	43	101010	100111	59	111010	001111
12	001011	100111	28	011011	101111	44	101011	101100	60	111011	100101
13	001100	011010	29	011100	110001	45	101100	110001	61	111100	111011
14	001101	110011	30	011101	011011	46	101101	011010	62	111101	110001
15	001110	011110	31	011110	110101	47	101110	110101	63	111110	111111
16	001111	110111	32	011111	011111	48	101111	011110	64	111111	110101

2-jadval.

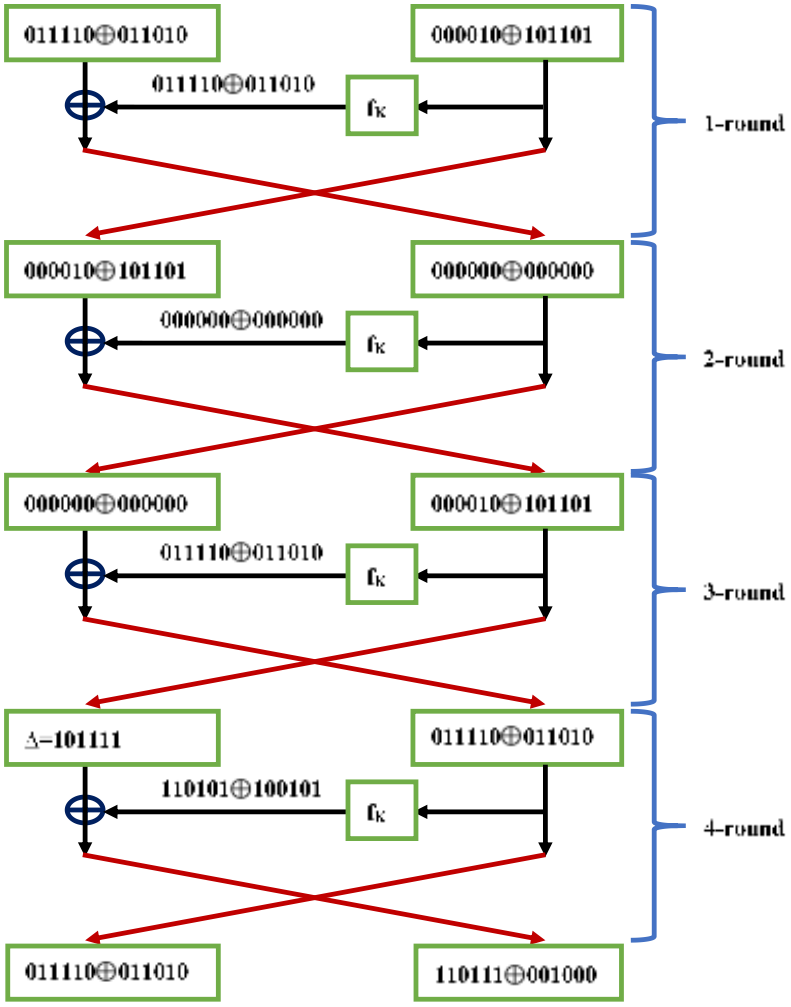
Keyingi ish, yuqoridagi jadvaldan foydalangan holda barcha ΔX farqlarni hisoblashga o‘tamiz. Kirish farqi ΔX=000000 bo‘lganda unga mos barcha chiqish farqlari ΔY=000000 teng bo‘ladi. Qolgan 62 ta Δ**X** farqlar ham shunday aniqlanadi. Natijada, Δ**X** ustun va Δ**Y** qatorlardan iborat umumlashgan jadval hosil bo‘ladi.

Endi matn juftliklari ichida boshqalaridan ko‘proq uchraydigan qismkalitlarini misollar orqali topishga harakat qilamiz [1]. Buning uchun ochiq matn juftliklari bilan ishlashni boshlaymiz. Masalan:

1-matn juftligi: X1=011110000010, X2=011010101101 ochiq matn juftligini tanlaymiz va unga mos yopiq matn juftligi 4-rasmda ko‘rishimiz mumkinki Y1=011110110111 va Y2=011010001000 bo‘ladi.

Ushbu holatda ΔY=000100111111. Ushbu tahlilda ko‘rishimiz mumkinki, to‘rtinchi raund chap qismiga Δ=101111 o‘ng qismiga Δ=100100 kelib tushadi. Shu sababli, faqat chap qismi 2 modul bo‘yicha Δ=000001 beradigan 64 ta har xil usul bilan olinadigan variantlar yig‘indisini ikkita Y1 va Y2 sxemalarga ajratgan holda ko‘rib chiqamiz:

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00938



4-rasm.

1. 000000 ⊕ 101111
2. 000001 ⊕ 101110
3. 000010 ⊕ 101101
. . .
. . .
. . .
64. 111111 ⊕ 010000

Endi ushbu 64 ta variantlarni tahlil qilib chiqamiz:

1) 000000⊕101111;

Y1 uchun to‘rtinchi raundning f_K-bloki kirishidagi 011110 qiymat kengaytmali o‘rin almashtirishda 1100111100 ga o‘zgartiriladi. f_K-blok chiquvchi 110111 qiymati ham o‘rin almashtirishga duch keladi, o‘rin almashtirish bilgan holda

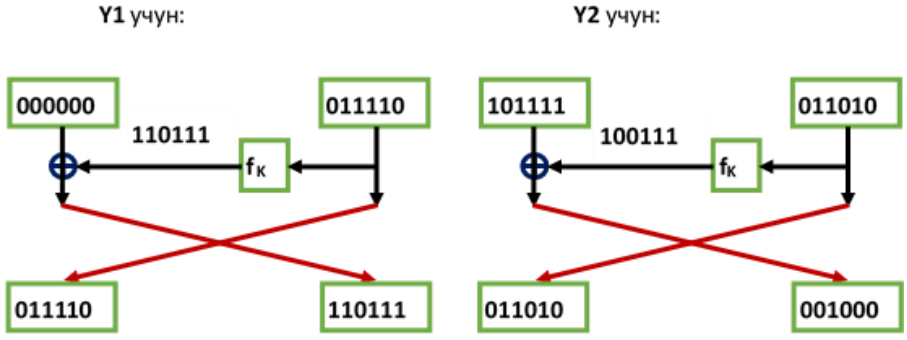
ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00938

bu qiymat 111110 ga teng bo‘ladi (4-rasm). Shunday qilib, uchala blokda uchrashi mumkin bo‘lgan qismkalitlarni aniqlaymiz:

- Almashtirish S_1- bloki chiqishiga 2-modul bo‘yicha ushbu raund qismkaliti bilan qo‘shilgan 1100 qiymat kelib tushadi va almashtirish natijasida chiqishda 11 qiymat hosil bo‘ladi. Bundan kelib chiqib, 1-jadvaldan foydalangan holda quyidagiga ega bo‘lamiz: $1100 \oplus K1 = 11$, bu yerda K1 quyikalitning dastlabki 4 bitini ifodalaydi. Almashtirish S_1- bloki chiqishida 11 qiymat ushbu blok kirishiga quyidagi qiymatlardan biri berilgan holda olinishi mumkin: 0001, 0010, 0101, 1001 va 1110. Bundan kelib chiqib, K1 quyidagi qiymatlardan birini qabul qilishi mumkin: 1101, 1110, 1001, 0101, 0010.

- Almashtirish S_2- blok chiqishiga 2-modul bo‘yicha ushbu raund qismkaliti bilan qo‘shilgan 111 qiymat kelib tushadi va almashtirish natijasida chiqishda 11 qiymat hosil bo‘ladi. Bundan kelib chiqib, shuningdek, 1-jadvaldan foydalanib, quyidagiga ega bo‘lamiz: $111 \oplus K2 = 11$, bu yerda K2 quyikalit keyingi 3 bitini ifodalaydi. Almashtirish S_2- blok chiqishida 11 qiymat ushbu blok kirishiga quyidagi qiymatlardan biri berilgan holda olinishi mumkin: 010, 100 va 111. Bundan kelib chiqib, K2 quyidagi qiymatlardan birini qabul qilishi mumkin: 101, 011, 000.

- Almashtirish S_3- bloki chiqishiga 2-modul bo‘yicha ushbu raund qismkaliti bilan qo‘shilgan 100 qiymat kelib tushadi va almashtirish natijasida chiqishda 10 qiymat hosil bo‘ladi. Bundan kelib chiqib, 1-jadvaldan foydalanib, quyidagiga ega bo‘lamiz: $100 \oplus K3 = 10$, bu yerda K3 qismkalitning oxirgi 3 bitini ifodalaydi. Almashtirish S_3- bloki chiqishida 10 qiymat ushbu blok kirishiga quyidagi qiymatlardan biri berilgan holda olinishi mumkin: 001, 010, 100 va 111. Bundan kelib chiqib, K3 quyidagi qiymatlardan birini qabul qilishi mumkin: 101, 110, 000, 011.



5-rasm.

Y2 uchun to‘rtinchi raundning f_K-bloki kirishidagi 011010 qiymat kengaytmali o‘rin almashtirishda 1000110100 ga o‘zgartiriladi. f_K-blok chiquvchi 100111 qiymati

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00938

ham o‘rin almashtirishga duch keladi, o‘rin almashtirish bilgan holda bu qiymat 110110 ga teng bo‘ladi (5-rasm).

Shunday qilib, uchala blokda uchrashi mumkin bo‘lgan qismkalitlarni aniqlaymiz:

- Almashtirish S_1- bloki chiqishiga 2-modul bo‘yicha ushbu raund qismkaliti bilan qo‘shilgan 1000 qiymat kelib tushadi va almashtirish natijasida chiqishda 11 qiymat hosil bo‘ladi. Bundan kelib chiqib, 1-jadvaldan foydalangan holda quyidagiga ega bo‘lamiz: $1000 \oplus K1 = 11$, bu yerda K1 quyikalitning dastlabki 4 bitini ifodalaydi. Almashtirish S_1- bloki chiqishida 11 qiymat ushbu blok kirishiga quyidagi qiymatlardan biri berilgan holda olinishi mumkin: 0001, 0010, 0101, 1001 va 1110. Bundan kelib chiqib, K1 quyidagi qiymatlardan birini qabul qilishi mumkin: 1001, 1010, 1101, 0001, 0110.
- Almashtirish S_2- blok chiqishiga 2-modul bo‘yicha ushbu raun qismkaliti bilan qo‘shilgan 110 qiymat kelib tushadi va almashtirish natijasida chiqishda 01 qiymat hosil bo‘ladi. Bundan kelib chiqib, shuningdek, 1-jadvaldan foydalanib, quyidagiga ega bo‘lamiz: $110 \oplus K2 = 01$, bu yerda K2 quyikalit keyingi 3 bitini ifodalaydi. Almashtirish S_2- blok chiqishida 01 qiymat ushbu blok kirishiga quyidagi qiymatlardan biri berilgan holda olinishi mumkin: 001 va 110. Bundan kelib chiqib, K2 quyidagi qiymatlardan birini qabul qilishi mumkin: 111, 000.
- Almashtirish S_3- bloki chiqishiga 2-modul bo‘yicha ushbu raund qismkaliti bilan qo‘shilgan 100 qiymat kelib tushadi va almashtirish natijasida chiqishda 10 qiymat hosil bo‘ladi. Bundan kelib chiqib, 1-jadvaldan foydalanib, quyidagiga ega bo‘lamiz: $100 \oplus K3 = 10$, bu yerda K3 qismkalitning oxirgi 3 bitini ifodalaydi. Almashtirish S_3- bloki chiqishida 10 qiymat ushbu blok kirishiga quyidagi qiymatlardan biri berilgan holda olinishi mumkin: 001, 010, 100 va 111. Bundan kelib chiqib, K3 quyidagi qiymatlardan birini qabul qilishi mumkin: 101, 110, 000, 011.

Keyingi juftliklar, masalan $000001 \oplus 101110$ juftlikda Y1 va Y2 uchun to‘rtinchi raundning f_K-bloki chiqish qiymati 111100 va 110100 teng bo‘lishi lozim, lekin shifrlash algortmining S akslantirish bloklarida 00 teng bo‘ladigan chiqish qiymatlarilari mavjud emas. Shu sababli, faqat qiymati mavjud bo‘lgan juftliklarni tanlaymiz.

Qolgan barcha juftliklar uchun, xuddi shunday tahlil o‘tkazamiz.

Tahlil natijasida, kalitni aniqlash uchun tanlangan birinchi matn juftligi $\Delta=101111$ da 64 ta variantdan faqat 12 tasi qanoatlantirdi, qolgan 52 tasi yuqorida

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00938

aytilgandek qiymati mavjud emas. Qolgan matn juftliklarini ham birinchi matn juftligi kabi aniqlanadi.

Matn juftliklarini tahlil qilganimizdan so‘ngi, olingan qismkalitlar variantlarini taqqoslashdan iborat bo‘ladi. Ishimizning qulayroq bo‘lishi uchun 3-jadvalni tuzamiz.

Hosil bo‘lgan jadvalda mos K1, K2 va K3 kalit bitlarining kesishuviga 1 qo‘yamiz va eng ko‘p hosil bo‘lgan 1 lar katta ehtimol bilan qismkalit deb olishimiz mumkin bo‘ladi.

Aniqlangan qismkalitlar.

K1	K2								K3							
	000	***001***	***010***	***011***	***100***	***101***	***110***	***111***	***000***	***001***	***010***	***011***	***100***	***101***	***110***	***111***
0000	111 111 111	111 111							111 11	111 11	111 11	111 11	111 11	111 11	111 11	111 11
0001																
0010																
0011	111 111	111 111 111							111 11	111 11	111 11	111 11	111 11	111 11	111 11	111 11
0100	111 111	111 111 111							111 11	111 11	111 11	111 11	111 11	111 11	111 11	111 11
0101																
0110																
0111	111 111 111	111 111							111 11	111 11	111 11	111 11	111 11	111 11	111 11	111 11
1000																
1001	111	111							11	11	11	11	11	11	11	11
1010	111	111							11	11	11	11	11	11	11	11
1011																
1100																
1101	111	111							11	11	11	11	11	11	11	11
1110	111	111							11	11	11	11	11	11	11	11
1111																

3-jadval.

MUHOKAMA

Shunday qilib, tahlil natijadida hosil qilingan 3-jadvalda ko‘rish mumkinki, katta ehtimol bilan boshqalardan ko‘proq uchraydigan quyidagi qismkalitlarning dastlabki yettita bitlarni olishimiz mumkin: K1=0000, 0011, 0100, 0111, K2=000,

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00938

001. Lekin qismkalitning oxirgi uch bitini chiziqli holat bo‘lganligi uchun aniqlashning iloji bo‘lmadi.

XULOSA

Tahlil natijasida shuni xulosa va taklif sifatida aytish mumkinki, Blokli shifrlash algoritmining muhim o‘ng qismi f_K dagi: kengaytirish va o‘rin almashtirish, S almashtirish bloki va o‘rin almashtirish jadvallaridagi o‘zgarmas qiymatlar shunday optimal tanlanishi kerakki, kiruvchi farqga mos chiquvchi farqlar ichida soni yuqori bo‘lgan chiquvchi farq bo‘lmasin, ya’ni ehtimoli juda yuqori bo‘lgan juftlik uchramasin, shunda shifrlash algoritmi differentsial kriptotahlil hujumiga bardoshli bo‘ladi. $\Delta X=101111$ kirish va unga mos $\Delta Y=000100$ chiqish bo‘lgandagi matn juftliklari tanlanganda, dastlabki qismkalitning yettita bitni katta ehtimol bilan aniqlandi, lekin oxirgi uchta bitni aniqlash iloji bo‘lmadi, chunki chiziqli holatga duch kelindi. Shu sababli, qolgan uch bitini tanlash yo‘li bilan aniqlanadi. Ushbu algoritm ba’zi bir kamchiliklardan holi emasli, lekin o‘quv ahamiyati uchun qulayligini aytish mumkin.

REFERENCES

1. Л.К.Бабенко, Е.А.Мишустина «Криптографические методы и средства обеспечения». Таганрог: Изд-во ТРТУ, 2003. 66 с.
2. Sh.R.Bobobekov (2020). About teaching students an improved method of applying a block-based encryption algoritm based on the fiestel network. An international multidisplinary research journal. Academicia may 2020 full journal, 1398-1406. DOI 10.5958/2249-7137.2020.00392.4.