МИРЗО УЛУҒБЕК НОМИДАГИ
ЎЗБЕКИСТОН МИЛЛИЙ УНИВЕРСИТЕТИ
МЕХАНИКА МАТЕМАТИКА
ФАКУЛЬТЕТИ

РЕФЕРАТ

Мавзу: **DES стандарт симметрик блокли шифрлаш алгоритми.**

Тайёрлади: Бозоров О.Н

Тошкент-2015

Режа:

1. DES стандарт симметрик блокли шифрлаш алгоритми
2. DES стандарт симметрик блокли шифрлаш алгоритмининг асосий акслантиришлари
3. DES шифрлаш алгоритмининг ишлаш режимлари
4. DES шифрлаш алгоритмларига ҳужум турлари

DES стандарт симметрик блокли шифрлаш алгоритми. DES стандарт шифрлаш алгоритми Америка Қўшма Штатлари (АҚШ) “Миллий Стандартлар Бюроси” томонидан 1977 йилда эълон қилинган. 1980 йилда АҚШнинг “Стандартлар ва Технологиялар Миллий Институти” бу алгоритмни давлат ва савдо-сотиқ молияси соҳасидаги махфий бўлмаган, аммо муҳим бўлган маълумотларни руҳсат этилмаган жисмоний ва юридик шаҳслардан муҳофаза қилинишида шифрлаш алгоритми сифатида қўллаш стандарти деб қабул қилди.

DES стандарт симметрик блокли шифрлаш алгоритмининг асосий акслантиришлари. DES алгоритмида: дастлабки 56 битли калитдан раунд калитларини ҳосил қилишнинг мураккаб эмаслиги, раунд асосий акслантиришларининг аппарат-техник ва дастурий таъминот кўринишларида қўлланилишини таъминлашнинг қулайлиги, ҳамда, улар криптографик ҳоссаларининг самарадорлиги – криптобардошлилигининг юқорилиги, бу алгоритмнинг асосий хусусиятларини белгилайди.

Шифрлаш жараёни 64 битли очиқ маълумот блокларини алгоритмда берилган *IP* –жадвал бўйича ўрин алмаштириш, унинг натижасини дастлабки 56 битли калитдан алгоритмда келтирилган жадваллар билан битларнинг ўринларини алмаштириш, циклик суриш ва баъзи битларни йўқотиш акслантиришларидан фойдаланиб ҳосил қилинадиган 48 битли раунд калитлари ҳамда асосий акслантиришлари билан 16 марта шифрлаш, шифрлаш натижаси блоки битларини берилган IP^{-1} –жадвал бўйича ўринларини алмаштиришдан иборат.

Алгоритм акслантиришларини ёритиш учун қуйидаги белгилашлар киритилади:

L_i ва R_i –ҳар бири 32 битли блоклар бўлиб, Фейстел тармоғини чап ва ўнг қисимларини ифодалайди, $i = 0,1,...,16$;

$\oplus$ – битлар блоклари векторлари кординаталарини $\bmod 2$ бўйича қўшиш;

K_i – 48 битли раунд калитлари;

F – Фейстел тармоғи асосий акслантиришлари функцияси;

IP – ўрин алмаштириш жадвали.

Навбатдаги Т –блокни шифрлаш жараёни бу блок битларини қуйидаги бошланғич *IP* – ўрин алмаштириш жадвали:

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

1-жадвал. *IP* – ўрин алмаштириш жадвали.

1-асосида акслантириш билан бошланади T –блокнинг 58-бити 1-бит ўрнига, 50-бити 2-бит ўрнига ва ҳоказо қолган битлар ҳам жадвалда кўрсатилган ўринларга ўтказилади. Сўнгра, олинган натижа иккита 32 битлик L_0 ва R_0 - қисмларга ажратилиб, 16 раундлик Фейстел тармоғи асосий акслантиришлари функцияси билан ҳар хил 48 битлик калитларда шифрланади. Яъни раунд натижаси, $T_{i-1} = L_{i-1}R_{i-1}$ $(i-1)$ деб белгиланса, у ҳолда, юқорида таъкидланганидек, i-раунд натижаси қуйидаги тенгликлар:

$$\begin{cases} L_i = R_{i-1}, \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i), \quad i = 1,2,\ldots,16; \end{cases}$$

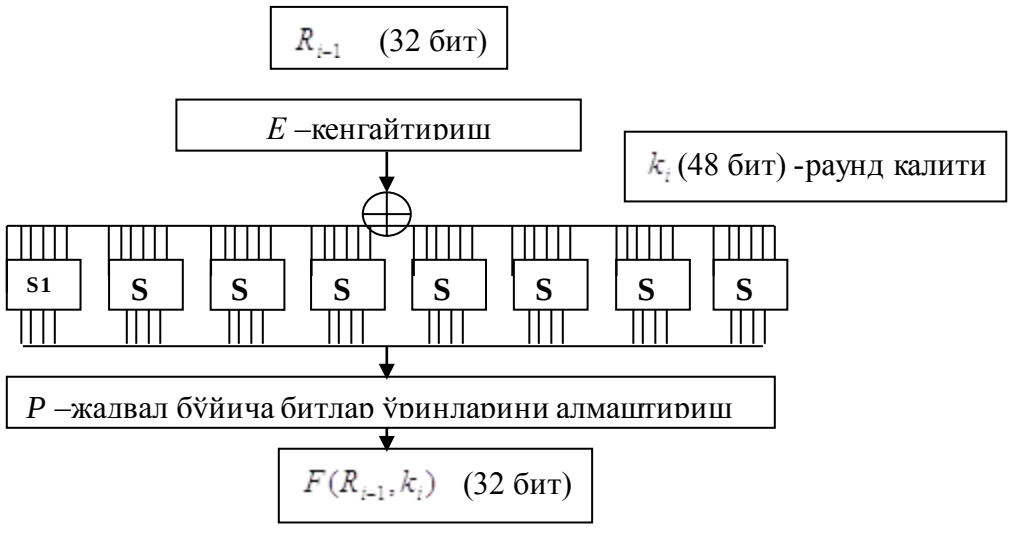
билан топилади. Бу ерда, $F(R_{i-1}, K_i)$ - 32 битли R_{i-1} ва 56 битли дастлабки калитни акслантириш натижасида олинган 48 битли K_i векторларнинг Фейтель тармоғи асосий акслантиришларининг функциясини ифодалайди. Охирги итерация-раунд натижаси $T_{16} = R_{16}L_{16}$ - блок бўлиб, бу блок битлари устида IP –жадвал бўйича IP^{-1} –тескари ўрин алмаштириш акслантириши бажарилади: T_{16}-блокнинг 1-бити 58-бит ўрнига, 2-бити 50-бит ўрнига ва хоказо қолган битлар ҳам жадвалда кўрсатилган ўринларга ўтказилади.

Дешифрлашда шифрлаш жараёнида бажарилган акслантиришлар тескари тартибда бажарилади, бунда ушбу:

$$\begin{cases} R_{i-1} = L_i, \\ L_{i-1} = R_i \oplus F(L_i, K_i), \quad i = 16,15,\ldots,1; \end{cases}$$

муносабатлардан фойдаланилиб, ҳар бири 32 битли бўлган L_{16} ва R_{16} шифрмаълумот блокларини кетма-кет акслантириш, L_0 ва R_0 блоклар олиш, 64 битли $L_0 R_0$ блок устида IP^{-1} - акслантиришни бажариш орқали, T -очиқ маълумот блоки олинади.

DES алгоритми Фейстел тармоғи асосий акслантиришларининг $F(R_{i-1}, K_i)$-функциясини ҳисоблаш схемаси қўйидагича:



1-схема. DES алгоритми $F(R_{i-1}, K_i)$-функциясини ҳисоблаш схемаси.

$E(R_{i-1})$-кенгайтириш функцияси R_{i-1}- 32 битли блокнинг 1, 4, 5, 8, 9, 12, 13, 16, 17, 20, 21, 24, 25, 28, 29 ва 32 –битларини икки мартадан такрорлаш, ҳамда, қуйидаги жадвал:

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-жадвал. $E(R_{i-1})$-кенгайтириш жадвали.

бўйича жойлаштириш натижасида ҳосил бўлган 48 битли $E(R_{i-1})$-блокнинг ҳар бир битини K_i - 48 битли раунд калитининг мос битларига $\oplus$ -XOR (mod2 бўйича) амали билан қўшилиб, натижа саккизта олти битлик $B_1,\ldots, B_8$, блоклар кўринишида ифодаланади: $E(R_{i-1}) \oplus k_i = B_1 B_2 \ldots B_8$.

Сўнгра ҳар бир B_j -олти битлик блок S – блокнинг мос жадвалли S_j – блоки орқали акслантирилиб, тўрт битли блок билан алмаштирилади. S_j – блоклар ўлчами 4×16 бўлган саккизта ўзгармас жадвалдан иборат:

	0	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***	***13***	***14***	***15***	
0	**14**	**4**	**13**	**1**	**2**	**15**	**11**	**8**	**3**	**10**	**6**	**12**	**5**	**9**	**0**	**7**	
1	**0**	**15**	**7**	**4**	**14**	**2**	**13**	**1**	**10**	**6**	**12**	**11**	**9**	**5**	**3**	**8**	S_1
2	**4**	**1**	**14**	**8**	**13**	**6**	**2**	**11**	**15**	**12**	**9**	**7**	**3**	**10**	**5**	**0**	
3	**15**	**12**	**8**	**2**	**4**	**9**	**1**	**7**	**5**	**11**	**3**	**14**	**10**	**0**	**6**	**13**	
0	**15**	**1**	**8**	**14**	**6**	**11**	**3**	**4**	**9**	**7**	**2**	**13**	**12**	**0**	**5**	**10**	
1	**3**	**13**	**4**	**7**	**15**	**2**	**8**	**14**	**12**	**0**	**1**	**10**	**6**	**9**	**11**	**5**	S_2
2	**0**	**14**	**7**	**11**	**10**	**4**	**13**	**1**	**5**	**8**	**12**	**6**	**9**	**3**	**2**	**15**	
3	**13**	**8**	**10**	**1**	**3**	**15**	**4**	**2**	**11**	**6**	**7**	**12**	**0**	**5**	**14**	**9**	
0	**10**	**0**	**9**	**14**	**6**	**3**	**15**	**5**	**1**	**13**	**12**	**7**	**11**	**4**	**2**	**8**	
1	**13**	**7**	**0**	**9**	**3**	**4**	**6**	**10**	**2**	**8**	**5**	**14**	**12**	**11**	**15**	**1**	S_3
2	**13**	**6**	**4**	**9**	**8**	**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**	**0**	**6**	**9**	**10**	**1**	**2**	**8**	**5**	**11**	**12**	**4**	**15**	
1	**13**	**8**	**11**	**5**	**6**	**15**	**0**	**3**	**4**	**7**	**2**	**12**	**1**	**10**	**14**	**9**	S_4
2	**10**	**6**	**9**	**0**	**12**	**11**	**7**	**13**	**15**	**1**	**3**	**14**	**5**	**2**	**8**	**4**	
3	**3**	**15**	**0**	**6**	**10**	**1**	**13**	**8**	**9**	**4**	**5**	**11**	**12**	**7**	**2**	**14**	
0	**2**	**12**	**4**	**1**	**7**	**10**	**11**	**6**	**8**	**5**	**3**	**15**	**13**	**0**	**14**	**9**	
1	**14**	**11**	**2**	**12**	**4**	**7**	**13**	**1**	**5**	**0**	**15**	**10**	**3**	**9**	**8**	**6**	

2	**4**	**2**	**1**	**11**	**10**	**13**	**7**	**8**	**15**	**9**	**12**	**5**	**6**	**3**	**0**	**14**	S_5
3	**11**	**8**	**12**	**7**	**1**	**14**	**2**	**13**	**6**	**15**	**0**	**9**	**10**	**4**	**5**	**3**	
0	**12**	**1**	**10**	**15**	**9**	**2**	**6**	**8**	**0**	**13**	**3**	**4**	**14**	**7**	**5**	**11**	
1	**10**	**15**	**4**	**2**	**7**	**12**	**9**	**5**	**6**	**1**	**13**	**14**	**0**	**11**	**3**	**8**	S_6
2	**9**	**14**	**15**	**5**	**2**	**8**	**12**	**3**	**7**	**0**	**4**	**10**	**1**	**13**	**11**	**6**	
3	**4**	**3**	**2**	**12**	**9**	**5**	**15**	**10**	**11**	**14**	**1**	**7**	**6**	**0**	**8**	**13**	
0	**4**	**11**	**2**	**14**	**15**	**0**	**8**	**13**	**3**	**12**	**9**	**7**	**5**	**10**	**6**	**1**	
1	**13**	**0**	**11**	**7**	**4**	**9**	**1**	**10**	**14**	**3**	**5**	**12**	**2**	**15**	**8**	**6**	S_7
2	**1**	**4**	**11**	**13**	**12**	**3**	**7**	**14**	**10**	**15**	**6**	**8**	**0**	**5**	**9**	**2**	
3	**6**	**11**	**13**	**8**	**1**	**4**	**10**	**7**	**9**	**5**	**0**	**15**	**14**	**2**	**3**	**12**	
0	**13**	**2**	**8**	**4**	**6**	**15**	**11**	**1**	**10**	**9**	**3**	**14**	**5**	**0**	**12**	**7**	
1	**1**	**15**	**13**	**8**	**10**	**3**	**7**	**4**	**12**	**5**	**6**	**11**	**0**	**14**	**9**	**2**	S_8
2	**7**	**11**	**4**	**1**	**9**	**12**	**14**	**2**	**0**	**6**	**10**	**13**	**15**	**3**	**5**	**8**	
3	**2**	**1**	**14**	**7**	**4**	**10**	**8**	**13**	**15**	**12**	**9**	**0**	**3**	**5**	**6**	**11**	

3-жадвал. S **– блокнинг мос жадвали**

Ҳар бир $B_j = b_1(j)b_2(j)..b_7(j)b_8(j)$, j=1,…,8; блоклар мос S_j -блокнинг $b_1(j)b_8(j)$-битлар билан аниқланувчи сатри ва $b_2(j)..b_7(j)$-битлар билан аниқланувчи устунларининг кесишувида жойлашган соннинг иккилик саноқ тизимида ифодаланувчи $z_1(j)z_2(j)z_3(j)z_4(j)$ -тўрт битлик ифодаси билан алмаштирилади. Ҳосил бўлган 32 –битлик $z_1(1)z_2(1)z_3(1)z_4(1)\ldots z_1(8)z_2(8)z_3(8)z_4(8)$ -блок битлари ўринлари алгоритмда берилган *P*–жадвал асосида алмаштирилади, унинг кўриниши қуйидагича:

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

4-жадвал. ***P*–алмаштири жадвали.**

Дастлабки 56 битли блок 7 битли қисмблокларга ажратилиб, 8, 16, …, 64 позицияларга, ҳар бир байтдаги бирлар сони тоқ бўладиган қилиб битлар қўшилади. Бу битлар шифрлаш жараёнида ишлатилмайди, улар калитларни узатиш ва сақлашда хатоликларга йўл қўймасликни назорат қилиш учун ишлатилади. Шундай қилиб ҳосил қилинган 64 –битли калит блокининг 56 та битлари ўринлари алгоритмда кўрсатилган жадвал бўйича алмаштирилади. Бундай алмаштириш ифодаси қуйидаги жадвалда келтирилган.

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
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

5-жадвал. *P*–алмаштири жадвали.

Бу жадвалнинг юқоридаги тўртта сатри $С_0$ ва кейинги тўртта сатри $Д_0$, деб белгиланади. Сўнгра, 56 битли $С_0$ $Д_0$ -блокдан ушбу: 9, 18, 22, 25, 35, 38, 43, 54 ўринларда турган битлар ўчирилиб, 48 битли блок ҳосил қилиниб, шу блок битлари ўринларини яна алгоритмда берилган қуйидаги:

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

6-жадвал. Раунд калитларини шакллантириш жадвали.

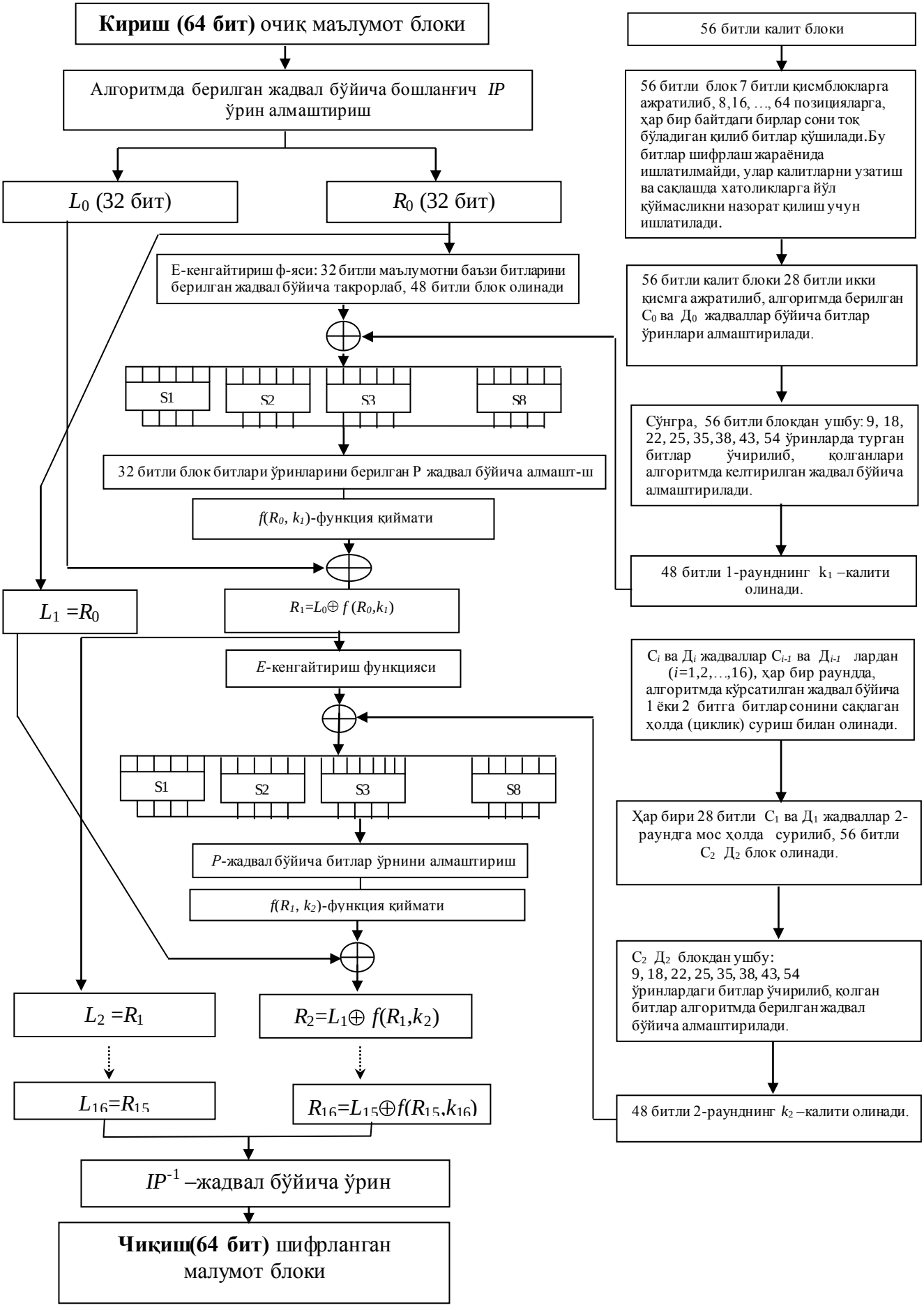
6-жадвал асосида алмаштирилиб 1-раунднинг k_1 –калити олинади.

$С_i$ ва $Д_i$ жадваллар улардан олдинги $С_{i-1}$ ва D_{i-1} (i=1,2,…,16), жадваллардан алгоритмда кўрсатилган:

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

жадвал бўйича 1 ёки 2 битга циклик суриш, ҳамда, ҳосил бўлган 56 битли блокдан ушбу: 9, 18, 22, 25, 35, 38, 43, 54 ўринларда турган битлар ўчирилиб, 48 битли блок ҳосил қилиниб, шу блок битлари ўринлари яна алгоритмда берилган 6-жадвал асосида алмаштирилиб i -раунднинг k_i –калити ҳосил қилинади.

DES шифрлаш алгоритми АҚШда 1998 йилнинг 31 декабргача стандарт шифрлаш алгоритми деб ҳисобланган. Бу алгоритмда қўлланилган акслантиришлар криптографик нуқтаи назардан бардошли, аммо дастлабки 56 - битли калитнинг узунлиги, бугунги кун ҳисоблаш техника ва технологияларининг ютуқларидан фойдаланилганда, мумкин бўлган барча 2^{56} та калитларни тўла танлаб чиқиш имкониятини сезиларли қисқартиради. Қуйида DES шифрлаш алгоритмининг блок схемаси келтирилган.



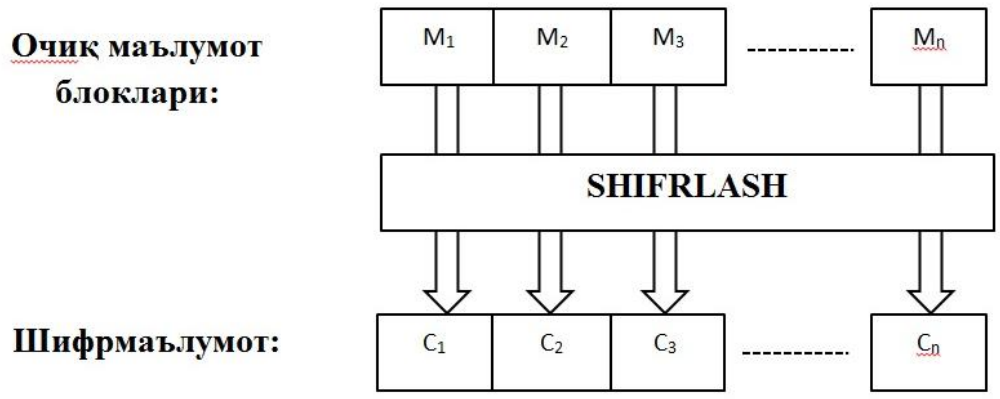
2-схема. DES шифрлаш алгоритмининг блок схемаси.

DES шифрлаш алгоритмининг криптобардошлилиги. DESнинг криптобардошлилиги S блокларнинг чизиқсизлик даражасига боғлиқ. Кучсиз S блоклар шифрмаълумотларни таҳлил қилишни осонлаштирилади. S блокларни танлаш қуйидаги талаблар асосида шакллантирилади:

- S блокнинг ҳар бир сатри $\{0,1,...,15\}$ ларнинг ёйилмасидан иборат бўлиши керак ;
- S блокар акслантиришлашла чизиқсиз ёки аффин функция бўлиши керак;
- Киришнинг бир битини ўзгариши S блокдан чиқишнинг камида икки битини ўзгариши керак;
- Иҳтиёрий x киришга мос чиқиш $S(x)$ ва $S(001100_2)$ қийматлар камида икки битга фарқ қилиши талаб қилинади.

DES шифрлаш алгоритмининг ишлаш режимлари. DES шифрлаш алгоритмидан тўртта режимда фойдаланиш мумкин.

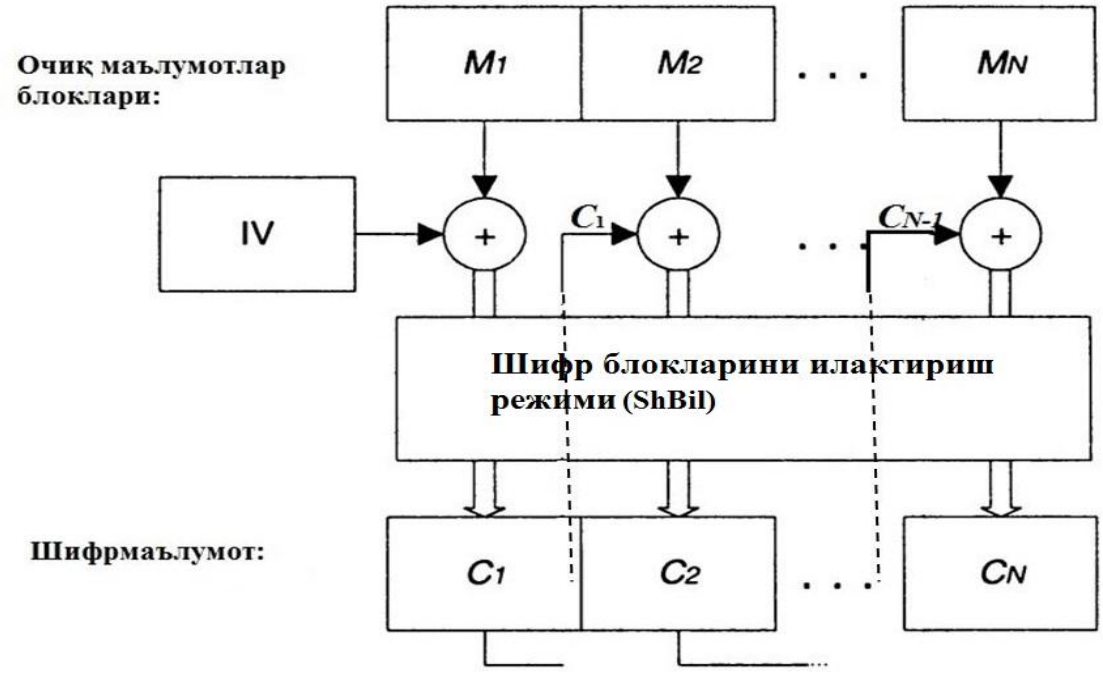
1. Электрон код китоби режими. Электрон код китоби (1-расм) режимида дастлабки матннинг барча блоклари бир-бирига боғлиқ бўлмаган ҳолда, дастлабки матннинг ҳар бир блокини шифрматн блоки билан (шифрматн блокини дастлабки матн блоки билан) алмаштириб, шифрланади. Яъни, $C_i = Des(M_i)$



1-расм электрон код китоби режими

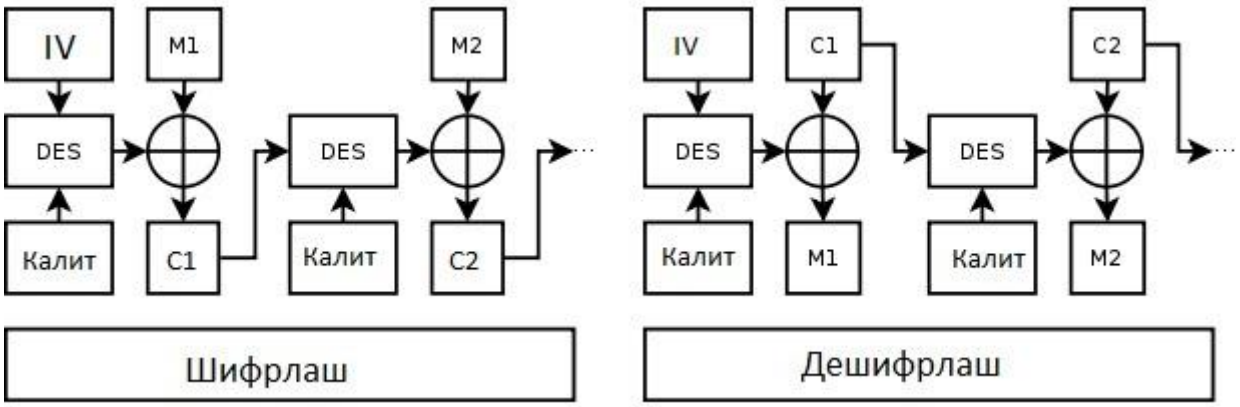
2. Шифр блокларини илактириш режими (2-расм) **тескари алоқа** механизмидан ва махсус кириш блоки бўлган ҳар бир сеансда янгиланадиган тасодифий инициализациялаш вектори IV дан фойдаланади. Яъни,

$(M_i^* = M_i \oplus C_{i-1},\ C_0 = IV,\ C_i = Des(M_i^*))$.



2-расм. Шифр блокларини илактириш режими

3. Шифрматнга тескари алоқа режими (3-расм) **тескари алоқа** механизмидан ва махсус кириш блоки бўлган ҳар бир сеансда янгиланадиган тасодифий инициализациялаш вектори IV дан фойдаланади. Яъни, $(C_i = Des(C_{i-1}) \oplus M_i,\quad C_0 = IV)$.



3-расм. Шифрматнга тескари алоқа режими

4. Шифрматнга тескари алоқа режими (3-расм) **тескари алоқа** механизмидан ва махсус кириш блоки бўлган ҳар бир сеансда янгиланадиган тасодифий инициализациялаш вектори IV дан фойдаланади. Яъни, $(C_i = Des(C_{i-1}) \oplus M_i, \quad C_0 = IV)$.

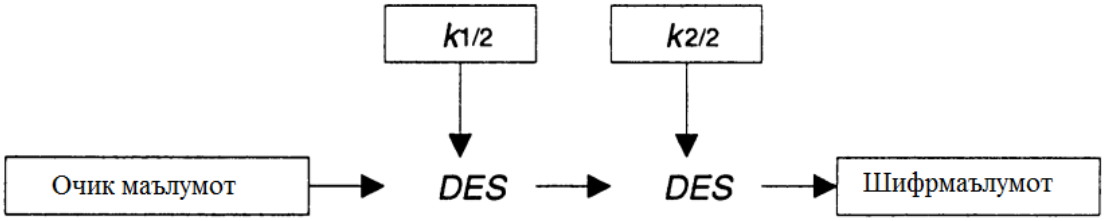
DES шифрлаш алгоритмларига ҳужум турлари:

Қўпол куч" (brute-force attack) методи. "Қўпол куч" (brute-force attack) методи мумкин бўлган барча шифрлаш калитларини текшириб чиқишга асосланади.

Шифрлаш калитининг узунлиги $K_i = 0,1,2,...,b-1$ бит бўлса. Мумкин бўлган барча шифрлаш калитлар $i = 2^b$ тани ташкил қилади. "Қўпол куч" криптоаналитик аниқ натижага эришиш 2^b маротаба, ўртача эса криптоаналитик шифртексти очиш учун $\frac{2^b}{2} = 2^{b-1}$ марта шифрлаш тестини амалга ошириши талаб қилинади.

"Ўртадаги учрашув" (meet-in-the-middle) синф ҳужуми. Ушбу методга содда мисол сифатида-шифрлаш алгоритмида икки алоҳида калит ёрдамида шифрланадиган Double DES (4-расм) алгоритмининг кўриниши одий DES алгоритми ёрдамида икки марта қайта шифрлаш

$$C = DES_{k_2/2} \; DES_{k_1/2} \; M \quad ,$$

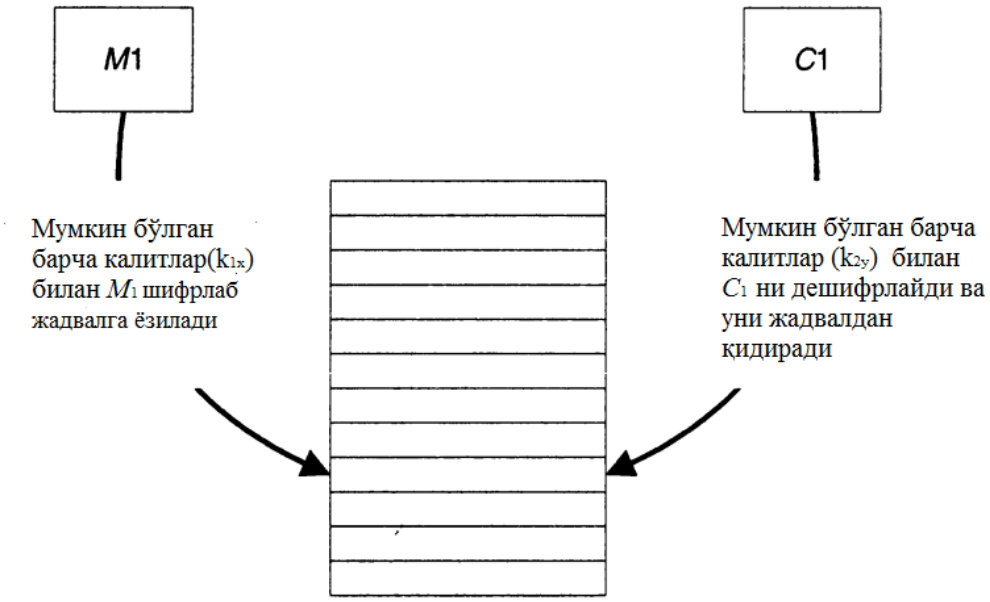


4-расм

бу ерда $k_1 / 2$ ва $k_2 / 2-$ қисм калитлари оддий ***DES*** алгоритминики каби 56 битли ***Double DES*** алгоритмининг қисм калитларидир.

Double DES алгоритмига криптоҳужум очиқ матн асосида ташкил қилинади. Криптотаҳлилиличи ўзига маълум M_1 очиқ матн ва унга мос C_1 шифртекстни билган ҳолда қуйидаги амалларни бажаради.

1) Мумкин бўлган барча калитлар $k_{1x} = 0...2^{56} - 1$ билан M_1 – шифрлайди $C^* = DES_{k_1 x}\ M_1$ ва барча C^* – ларни жадвалда сақлайди.
2) Мумкин бўлган барча калитлар $k_{2y} = 0...2^{56} - 1$ билан C_1 – дешифрлайди $M^* = DES^{-1}{}_{k_2 y}\ C_1$ ва барча C^{2*} – ларни жадвалда сақлайди.
3) Ҳосил қилинган жадвалдан $C^* = M^*$ тенгликни текшириб куради ва бирор бир ҳолатда тенглик ўринли бўлишидан $k_{1/2} = k_{1x}$, $k_{2/2} = k_{2x}$ калитлар топилади.



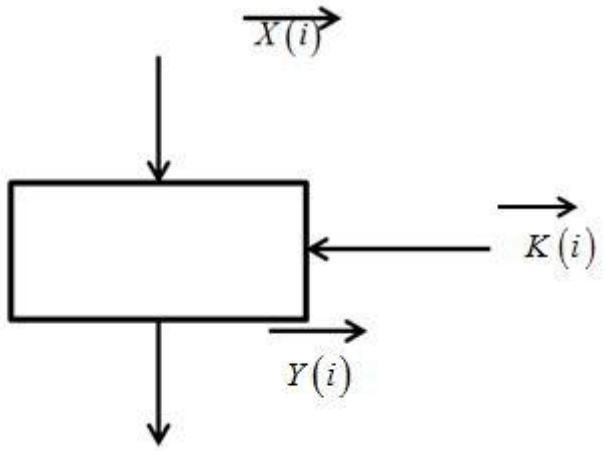
5-расм “Ўртадаги учрашув” синф ҳужуми.

1981-йилда германиялик криптотаҳлилчи Стефан Лакс “Ўртадаги учрашув” криптоҳужум орқали калит узунлиги 198-битли DEAL алгоритмини 148-битли алмаштиришлар орқали очишга муваффақ бўлган.

Чизиқли криптотаҳлил. Чизиқли таҳлил блокли шифрлаш схемаларидан фойдаланишда криптотаҳлилчининг очиқ ва шифрланган матнни билишига асосланади.

Чизиқли криптотаҳлил чизиқсиз функцияни унинг чизиқли аналоги билан алмаштириш имконияти мавжудлигига асосланади. Барча шифрланадиган матнлар иккилик кўринишда берилиши туфайли $Q-$ 0,1 тасодифий миқдорни кўриб чиқамиз, унинг учун $P\ Q=1\ =\ p$, мос равишда

$$P\ Q=0\ =\ 1-p,\ \ \Delta(Q)=\ |1-2p|.$$



$i-$ циклда ихтиёрий блокли шифр схемасини кўриб чиқамиз: бу ерда $E-$ шифрлаш функцияси, $X\ i\ -i-$ циклдаги очиқ матн блоки, *Y(i)* – шифрматн блоки, $K\ i\ -i-$ чи циклда фойдаланиладиган қисмий калит. $Y\ i\ ,X\ i\ \in V_n,\ K\ i\ \in V_m,$ бу ерда n – блок ўлчови, m – қисмий калит ўлчови.

$$Y\ i\ \ =E\ X\ i\ ,K\ i\ \ .$$

$(X,a)=X_1a_1\oplus..\oplus X_na_n=\ X_{i1}\oplus...\oplus X_{ik}=X\left[i_1,...,i_k\right]$орқали иккита X ва α иккилик векторларнинг скаляр кўпайтмасини белгилаймиз, бу ерда $(a_{i1},...,a_{ik})\ -a$ векторнинг бирлик координаталари, моҳияти бўйича 2 модуль бўйича α векторнинг нолга тенг бўлмаган мос келувчи битларининг X вектор битларига қўшишдир.

Чизиқсиз функциянинг статистик аналоги топилади, яъни

$$Q\ i\ =\ Y\ i\ ,a\ i\ \ \oplus\ X\ i\ ,b\ i\ \ \oplus\ K\ i\ ,c\ i\ \ ,$$

тасодифий катталикни топамиз, агар тасодифий танланган очиқ матн $X\ i$ учун эҳтимоллик

$$P(Q\ i\ =1)\ =p\neq 1/2$$ бўлса.

$\Delta\ Q\ i\ =\left|1-2p\right|$ четлашиш (оғиш) (2) чизиқли статистик аналогнинг самарадорлигини аниқлаб беради.

Чизиқли криптотаҳлилни қўллаш учун қуйидаги масалаларни ҳал этиш зарур:

1) самарали статистик чизиқли аналогни топиш ва унинг эҳтимоллигини ҳисоблаб чиқиш;

самарали статистик чизиқли аналогдан фойдаланиб, калитни (ёки калитнинг айрим битларини) аниқлаш.

Ушбу усулни биринчи япониялик олим Matsui ишлаб чиққан бўлиб. Бу метотда ёпиқ калитни тиклаш учун у 2^{47} та очиқ калитларни танлаган. DES алгоритмига биринчи ҳужумда Matsui 12 HP 9735 номли автоматлаштирилган тизими орқали 50 кун ичида очишга муваффақ бўлган.

Дифференциал криптотаҳлил. Дифференциал криптотаҳлил тушунчаси илк бора 1990 йил Эли Бихам ва Ади Шамир томонидан киритилган[7]. Ушбу усулдан фойдаланиб, Бихам ва Шамир «тўғридан-тўғри» ҳужумдан кўра самаралироқ бўлиб чиққан, танланган очиқ матндан фойдаланиб, DES алгоритми ҳужум усулини топдилар.

Усулнинг асосини танланган очиқ матн асосидаги ҳужум ташкил қилади. Дифференциал криптотаҳлил ғояси дастлабки аниқ тафовутларга эга бўлган очиқ матнлар X_1, X_2 $\Delta = X_1 \oplus X_2$ иккита жўфтлигининг битта калит билан шифрлаш цикллари орқали ўтиш жараёнида ўзгаришларининг ўхшаш эмаслигини таҳлилидан иборат. Очиқ матнларни танлашга ҳеч қандай чеклов йўқ. Айрим позицияларда тафовут бўлиши кифоя. Ўхшаш эмаслик ўлчови сифатида, қоидага кўра, Хэмминг масофаси фойдаланилади.

Шифрматнлардан ҳосил бўлган тафовутлардан келиб чиқиб, калитларга турли эҳтимолликлар берилади. Ҳақиқий калит шифрматнлар жўфтликларини кейинчалик таҳлил қилиш жараёнида аниқланади – бу кўплаб даъвогар калитлар орасида эҳтимоли энг юқори бўлган калитдир.

DESга ушбу усулда биринчи бўлиб Бихам ва Шамир ҳужум уюштирган. Бунинг учун уларга 2^{47} та очиқ матнни танлаш кифоя қилган.

АҚШнинг “Стандартлар ва Технологиялар Миллий Институти” томонидан 1997 йилда янги стандарт учун конкурс эълон қилиниб, 2000 йилнинг 2 октябрида унинг ғолиби аниқланди. Бу стандарт шифрлаш алгоритми AES FIPS -197 деб номланиб, у Фейстел тармоғига асосланмаган.

Фойлаланилган адабиётлар рўйхати:

1. Акбаров Д.Е “Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши” Тошкент 2009.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. “Основы криптографии” Гелиос АРВ, 2005.
3. Панасенко С.П “Алгоритмы шифрования” Справочник.2009.
4. www.wikipedia.com