2. ЖАҢА ДӘУІРДЕГІ СИММЕТРИЯЛЫҚ КРИПТОЖҮЙЕЛЕР

Лекция мақсаты: Симметриялық криптожүйелердің негіздерімен таныстыру, DES және ГОСТ 28147-89 криптожүйелеріне ерекше назар аудару, олардың негізгі ерекшеліктері, шифрлау және декодтау алгоритмдері, сондай-ақ криптоанализ әдістері туралы түсінік беру.

Негізгі сұрақтар:

1. Симметриялық криптожүйелер дегеніміз не?
2. DES криптожүйесі қалай жұмыс істейді?
3. Фейстел құрылымы дегеніміз не және ол DES криптожүйесінде қалай қолданылады?
4. DES арқылы шифрлау және дешифрлау процесі қалай жүзеге асады?
5. ГОСТ 28147-89 алгоритмі DES-ке қарағанда қандай ерекшеліктерге ие?
6. Криптоанализ әдістері және олардың алгоритмдерге қауіпсіздік бағалаудағы рөлі қандай?

Қысқаша мазмұны: Лекцияда екі негізгі симметриялық криптожүйе — DES (Data Encryption Standard) және ГОСТ 28147-89 туралы баяндалады. Бұл алгоритмдердің жұмыс істеу принциптері, Фейстел құрылымының рөлі, шифрлау және дешифрлау процесі, сондай-ақ олардың қауіпсіздігіне қатысты мәселелер қарастырылады. Сонымен қатар, криптоанализ әдістері, оның ішінде дифференциалды және сызықтық криптоанализ сияқты әдістер талқыланады.

2.1. DES криптожүйесі

Блоктық шифрларда Фейстел желісі (Feistel Network) қолданылады. Фейстел желісі кез келген функцияны (F – функция) түрлендіру арқылы блоктарға алмастыру әдісі. Бұл Фейстел желісі (Хорст Фейстелдің атымен аталған) көптеген шифрларда қолданылады яғни DES, ГОСТ 28147-89 және т.б. криптожүйелерінде қолданыста болды. F – функциясы Фейстел желісінің негізгі блогын құрайды және ол әр уақытта сызықты емес сонымен қатар барлық жағдайларда кері қайтымды емес.

F функциясын бинелеу түрінде көрсетуге болады.

$$F: Z_{2,N/2} * Z_{2,k} \rightarrow Z_{2,N/2},$$

мұндағы N – мәтін блогының ұзындығы (жұп болу қажет), k – кілт блогының ұзындығы.

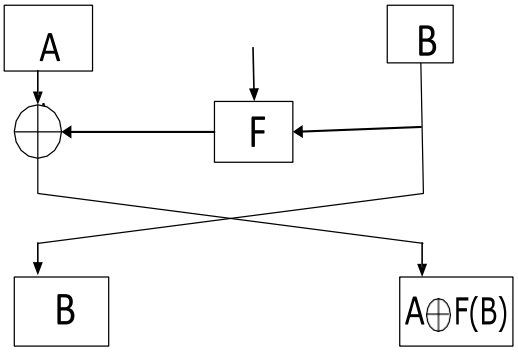
Егер X – мәтін блогы $X = \{A, B\}$ екі ішкі блогына бөлінсе, онда Фейстел желісінің қадамы келесідей болады:

$$X_{i+1} = B_i || (F(B_i, k) \oplus A_i),$$

мұндағы $X_i = \{A_i, B_i\}$, || - конкатенациялық амал. Фейстел желісінің қадамдары 1-суретте көрсетілген.

IBM фирмасы 30 жылдан астам бұрын DES шифрын ойлап тапты. 1977 жылы АҚШ-та федаралдық стандарт есебінде қабылданды [2, 12, 13, 16, 18, 21].

DES криптожүйесі 30 жылдай сенімді және жан-жақты қолданылып келді.

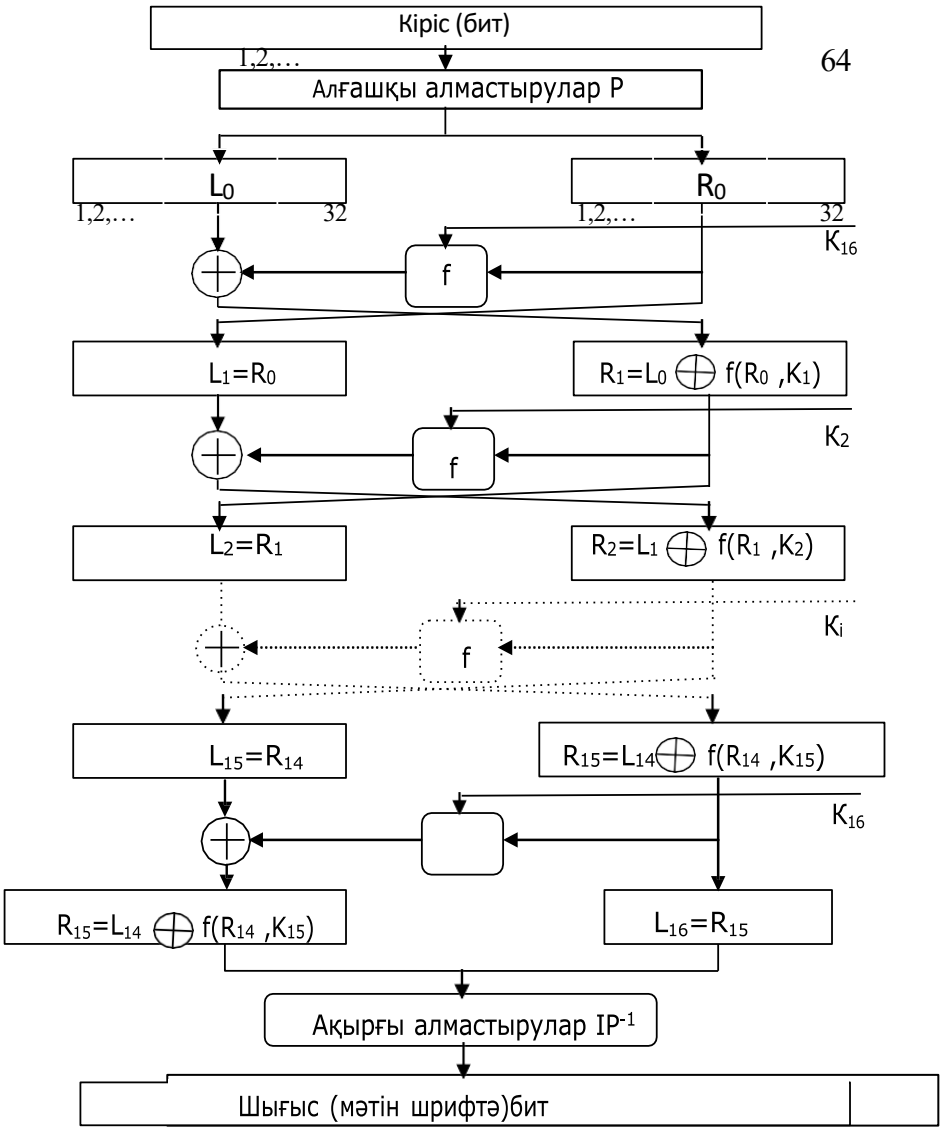


1-сурет. *Фейстел желісінің амалдары*

1997 жылы қаңтар айында RSA Data Security компаниясы DES шифрын қолданып шифрланған мәтінді жариялады және кімді-кім осы шифрланған мәтінді бұзып ашса, онда 10.000 АҚШ доллар сыйлық берілетіндігі айтылды. 1997 жылы 17 маусым айында Roske Verser шифрды ашып келесі сөзді Strong cryptography makes the world a safer place екенін анықтап және шифрлау кілтін тапты. Төрт айға созылған үлкен жұмысқа АҚШ және Канада сияқты елдердің кілтті толық анықтау үшін 78.000 компьютерлері қатысты.

Сонымен DES криптожүйесін толық сенімді шифр деп айтуға болмайды, бірақ DES құпиялы кілт криптожүйелерінің дамуына үлкен үлес қосты, сол себепті біз оқулықта DES криптожүйесінен бастағанды жөн көрдік. DES криптожүйесінің алгоритмі 2-суретте көрсетілген.

Алғашқы текст 64 биттік блоктың алмастыру битіне беріледі, одан соң 16 цикілдік шифрлау процесі басталады және одан кейін ақырғы алмастыру битіне беріліп шифр-мәтін алынады.



Шығыс (шифрланған мәтін) бит

1,2,… 64

2-сурет. *DES криптожүйесінің алгоритмі*

Кілтті таңдау алгоритмі

1-ші қадам. Әрқайсысы 28 биттен тұратын кілттің 56 биті C_0 және D_0 екі блокпен алмастырылады.

2-ші қадам. Келесі сәйкестіктерді және $C_{n-1}, D_{n-1}, n = 1,\ldots,16$ блоктарын қолдана отырып, $C_{n-1}, D_{n-1}, n = 1$ бір рет немесе екі рет жылжыту арқылы C_0 және D_0 блоктарын құраймыз.

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

3-ші қадам. 16 рет алмастыру жасау арқылы $K_n, 1 \le n \le 16$ кілт биттерін анықтаймыз. $C_{n-1}, D_{n-1}, n = 1$ биттерінен алынған $K_n, 1 \le n \le 16$ әрқайсысы 48 биттен тұратын келісі мәндер :

$$C_0 = \begin{matrix} 57 & 49 & 41 & 33 & 25 & 17 & 9 \\ 1 & 58 & 50 & 42 & 34 & 26 & 18 \\ 10 & 2 & 59 & 51 & 43 & 35 & 27 \\ 19 & 11 & 3 & 60 & 52 & 44 & 36 \end{matrix}$$

$$D_0 = \begin{matrix} 63 & 55 & 47 & 39 & 31 & 23 & 15 \\ 7 & 62 & 54 & 46 & 38 & 30 & 22 \\ 14 & 6 & 61 & 53 & 45 & 37 & 29 \\ 21 & 13 & 5 & 28 & 20 & 12 & 4 \end{matrix}$$

Бұл қадамнан кейін 64 биттен тұратын алғашқы хабар блогын қалай шифрланатынын көрсетеміз.

Шифрлау алгоритмі.

1-ші қадам. блогы алғашқы алмастыруға түседі.

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

2-ші қадам. Түрленген ω' блогын былай жазамыз.

$$\omega' = L_0 R_0,$$

мұндағы, L_0 және R_0 32 биттен тұрады.

3-ші қадам. L_{n-1} және L_{n-1} $(1 \le n \le 16)$ пайдаланып L_0 және R_0 келесі түрде анықтаймыз.

$$L_n = R_{n-1}$$
$$R_n = L_{n-1} \oplus f(R_{n-1}, K_n),$$

мұндағы, $\oplus$-модулі 2 бойынша қосу, ал f- шифрлау функциясы.

f функциясын есептеу алгоритмі.

1-ші қадам. Төмендегі таблица бойынша 32 биттік L_{n-1} 48 битке дейін кеңейтеміз:

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-ші қадам. 48 разрядтық кілт R_0 және 48 битке кеңейтілген L_{n-1} блогы биттері бойынша қосылады яғни

$$B = R_n'_{-1} \oplus K_n$$

3-ші қадам. B блогы 48 биттен тұратын сегіз 6 биттік блоктарға бөлінеді: $B = B_1 B_2 ... B_8$

B_i сегіз блоктың әрқайсысы s_i кестелерін қолдануарқылы 4 биттік B_i' блогына бөлінеді.

S_1

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

S_2

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

S_3

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

S_4

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

S_5

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

S_6

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

S_7

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

S_8

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

4-ші қадам. Келесі алмастырулар арқылы f -тің мәнін табамыз.

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

Шифрды ашу процесін келесі формула бойынша анықтауға болады:

$$R_{n-1} = L_n$$
$$L_{n-1} = R_n \oplus f(L_n, K_n).$$

DES криптожүйесінің ерекшіліктері олар:

- шифрлау уақыты жылдам;
- қорғаныс әдісі тек қана құпия кілтіне сүйенеді, оның алгоритмінің құпиялығына байланысты емес;
- әр блоктың берілгендері бір-біріне байланыссыз шифрланады. DES жүйесінің ең маңызды кемшілігі оның құпия кілтінің ұзындығының аз екендігі.

2.2. ГОСТ 28147-89 шифрлау алгоритмі

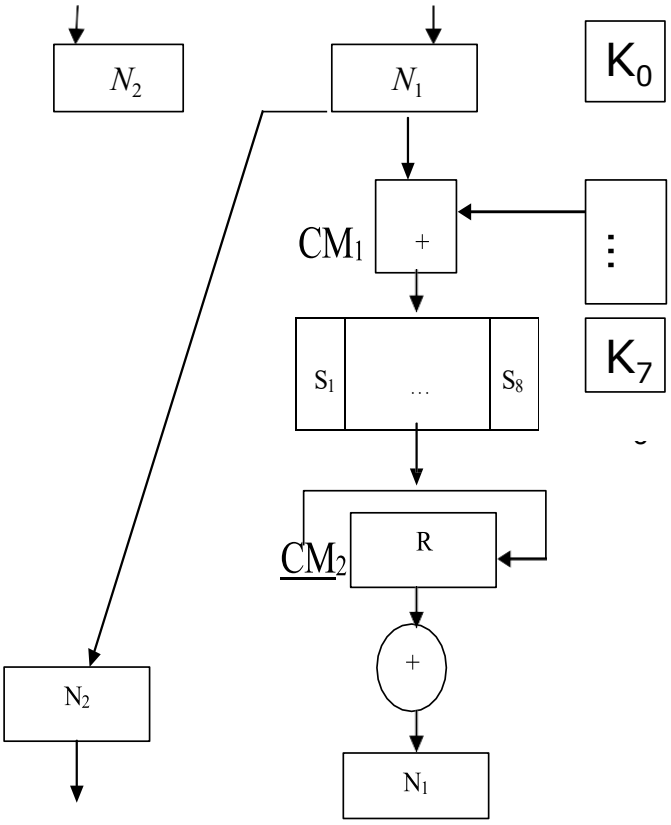
1. ГОСТ 28147-89-пен анықталатын [9], негізінен ТМД елдерінде қолданылатын шифрлау алгоритмі блокті DES класына жатады. Блок ұзындығы DES алгоритмі сияқты 64 битке тең.

Алгоритм төрт режимде қолданылады:

1. Жай алмастыру;
2. Гаммалау;
3. Кері байланысты гаммалау;
4. Шифрмәтін блоктарын тізбектеу.

Алгоритмде 32 цикл қолданылады. Циклдердің ішінде кілттермен басқарылатын біртипті түрлендірулер орындалады. Кілт ұзындығы 56

битке тең DES-тен айырмашылығы берілген алгоритмде ұзындығы 256 бит болатын кілт матрица түріндегі 32 биттік сегіз $K_0,...,K_7$ бульдік вектордан тұрады. Бұл цикілдік кілттерді шығару сызбасын біраз жеңілдетеді. Бір цикілде орындалатын түрлендірудің логикалық сызбасы келесі 3-суретте көрсетілген.



***3-сурет**. ГОСТ28147-89 алгоритмінің логикалық сызбасы*

N_1, N_2 -32 разрядты жинақтағыштар; КЗУ-кілттік сақтағыш құрылғысы

$K_i, 0 \le i \le 7$ - 32 биттік бульдік вектор;

$S_i, 1 \le i \le 8$ - 4x4 өлшемді S блок (қайтарымды түрлендіру $GF(2^4) \to GF(2^4)$);

R – жылжымалы регистр, ол үлкен разрядтар жағына 11 битті циклдік жылжытады;

$CM_1 - 2^{32}$ модулі бойынша қосындылаушы;

$CM_2 - 2$ модулі бойынша қосындылаушы;

Ашық мәтіннің 64 биттік блогы әрқайсысы 32 бит болатын 2 бөлікке бөлінеді. Оң жақ жартысы N_1 -жинақтағышына, сол жақ жартысы N_2 -жинақтағышына жүктеледі. Сақтағыш құрылғысының

кілт (КЗУ) векторларын: $K_0,...,K_7,K_0,...,K_7,K_0,...,K_7,K_7,...,K_0$ ретімен қолданатын, 3-суретте көрсетілген 32 цикл орындалады.

N_1,N_2 -жинақтағышындағылар мәтінді жай ауыстыру режимінде шифрланған мәтін болып табылады.

Берілген алгоритм американдық DES алгоритмдерінің принциптеріне негізделген, бірақ келесідей айырмашылықтары бар:

- цикілдер саны 16-дан 32-ге дейін өсірілді;
- кілттің ұзындығы 256 битке тең;
- әрбір цикілде қолданылатын кілттер жеңіл қалыптасады;
- 2^{32} модулі бойынша қосындылау қолданылады;
- DES-те қолданылатын ауыстыру орнына үлкен разрядтар жағына 11 битке цикілді жылжыту қолданылады;
- 2^{32} модулі бойынша қосындылау алгоритмге тиімді қасиетін береді. Бұл маңызды криптографиялық қасиетінің мәні ашық мәтіннің бір битінің немесе кілттің бір битінің өзгеруі шифрланған мәтіннің жарты биттерінің өзгеруіне алып келуінде.

S-блогына толығырақ тоқталайық. Әрбір S-блокты төрт бульдік айнымалыдан тәуелді төрт координаттық бульдік функция ретінде беруге болады, яғни

$$S = [f_1, f_2, f_3, f_4],$$

мұнда $f_i = f(x_1, x_2, x_3, x_4),\ 1 \le i \le 4$.

Егер барлық кіріс биттері шығыс биттеріне әсер етсе, яғни барлық шығыс биттері әрбір кіріс биттерінен тәуелді болса, сызба сегіз циклден кейін барлық аралық биттер әрбір кіріс биттеріне тәуелді болатындай етіп құрастырылған. Бұл барлық шифрланған мәтін биттеріне де қатысты.

DES-те қолданылатын S-блокты таңдау принциптері құпияланған. Бұл алгоритмді өңдеушілердің криптограмманы кілттсіз, яғни сәтті криптоталдау жүргізу көмегімен бұза алатындығы туралы пікірталас тудырды. ГОСТ 28147-89-да өзгертілетін s блоктар белгіленген тәртіп бойынша көрсетілген кездейсоқ жасалатын S- блокты қолдану туралы сұрақ туады. Қазіргі кезде бірнеше модификацияланған блоктық шифрларды талдау кезінде сәттілікке алып келетін криптоталдаудың екі әдісі (дифференциалдық және сызықтық) бар. Сондықтан S-блокты қорытып шығаратын процедура

Бақылау сұрақтары:

1. Симметриялық криптожүйелердің жұмыс принципі қандай?
2. DES алгоритмі қалай жұмыс істейді, Фейстел құрылымы қандай рөл атқарады?
3. ГОСТ 28147-89 DES-тен қандай ерекшеліктерге ие?
4. Криптоанализ дегеніміз не және оның симметриялық шифрларға әсері қандай?
5. DES жүйесін жақсарту үшін криптографиялық тұрғыда қандай ұсыныстар берер едіңіз?

Әдебиеттер тізімі:

1. Cortez R. M., Okoshi M. P., Okoshi K. (2022) "Cryptographic Algorithms and their Applications," Journal of Cryptographic Research.
2. Monte I. P., Faro D. C., Trimarchi G., et al. (2023) "A New Approach to Symmetric Cryptosystems," Cryptography and Security.
3. Martini L., Lisi M., Pastore M. C., et al. (2024) "Enhanced Security in Symmetric Cryptosystems," Journal of Computer Security.