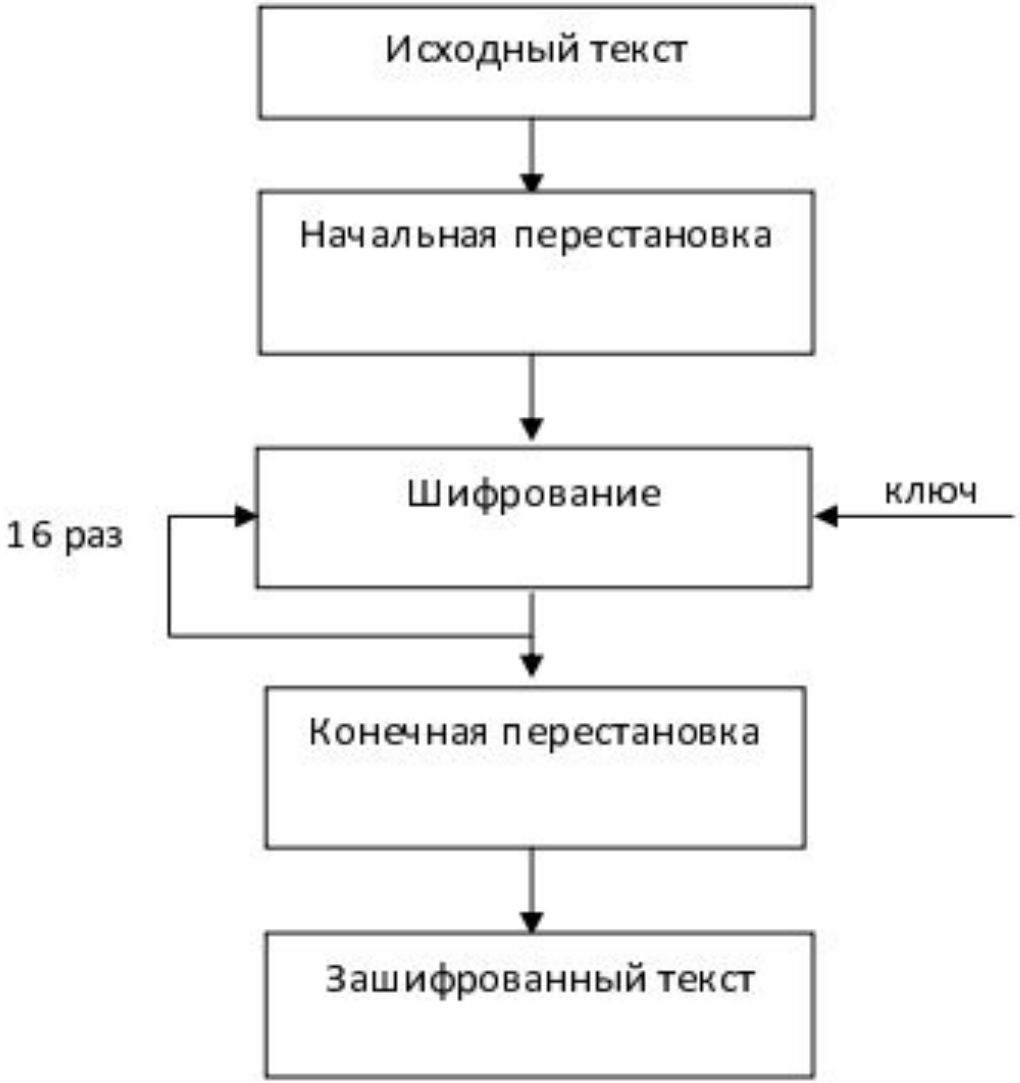
Дәріс 4

DES стандарты

DES (Data Encryption Standard) 1978 жылы қабылданған, деректерді криптографиялық жабудың американдық стандарты блоктық шифрлерді бірі болып табылады. Фейстель әдісіне негізделген DES 56-биттік кілт көмегімен деректердің 64-биттік блоктарын шифрлеуді жүзеге асырады. DES-те дешифрлеу шифрлеуге кері операция болып табылады және шифрлеу операциясын кері тізбекте қайталау жолымен орындалады. Шифрлеу процесі 64-биттік блок биттерін бастапқы орынға қою, шифрлеудің 16 циклін және биттерді кері орын ауыстырудан тұрады (1-сурет).



1-сурет. DES шифраторы

Бастапқы орын ауыстырудың P матрицасы мына түрге ие

58	50	42	34	26	18	10	02
60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06
64	56	48	40	32	24	16	08
57	49	41	33	25	17	09	01
59	51	43	35	27	19	11	03
61	53	45	37	29	21	13	05
63	55	47	39	31	23	15	07

Файлдан кезекті 8-байттық T блогы оқылады, ол бастапқы орын ауыстырудың P матрицасы көмегімен түрленеді, яғни T блогының 58 номері бар биті 1 номері бар бит, 50 номері бар бит – 2 номері бар бит және т.с.с. болады, нәтижесінде: T(0) = P(T). Бастапқы орын ауыстырудың криптотөзімділікке әсері туралы ештене белгісіз. Ол деректерді байт бойынша жүктеу үшін DES аппараттық қалыптасуында пайдаланылды деп есептеледі. Орын ауыстыру деректердің әрбір байтының алдымен оң биттерін (2,4,6,8), содан теріс биттерін таңдауға сәйкес келеді (1,3,5,7). Бірақ, бастапқы орын ауыстыруды орындау DES стандартымен сәйкестікті қамтамасыз ету үшін қажет.

Содан соң алынған T(0) биттер тізбегіекі тізбекке әрбіреуі 32 бит бойынша бөлінеді: L(0) – сол немесе үлкен биттер, R(0) – оң немесе кіші биттер. Содан 16 итерациясымен 2-суретте көрсетілгендей Фейстель әдісі бойынша шифрлеу орындалады, і –ші итерация келесі түрде сипатталады:

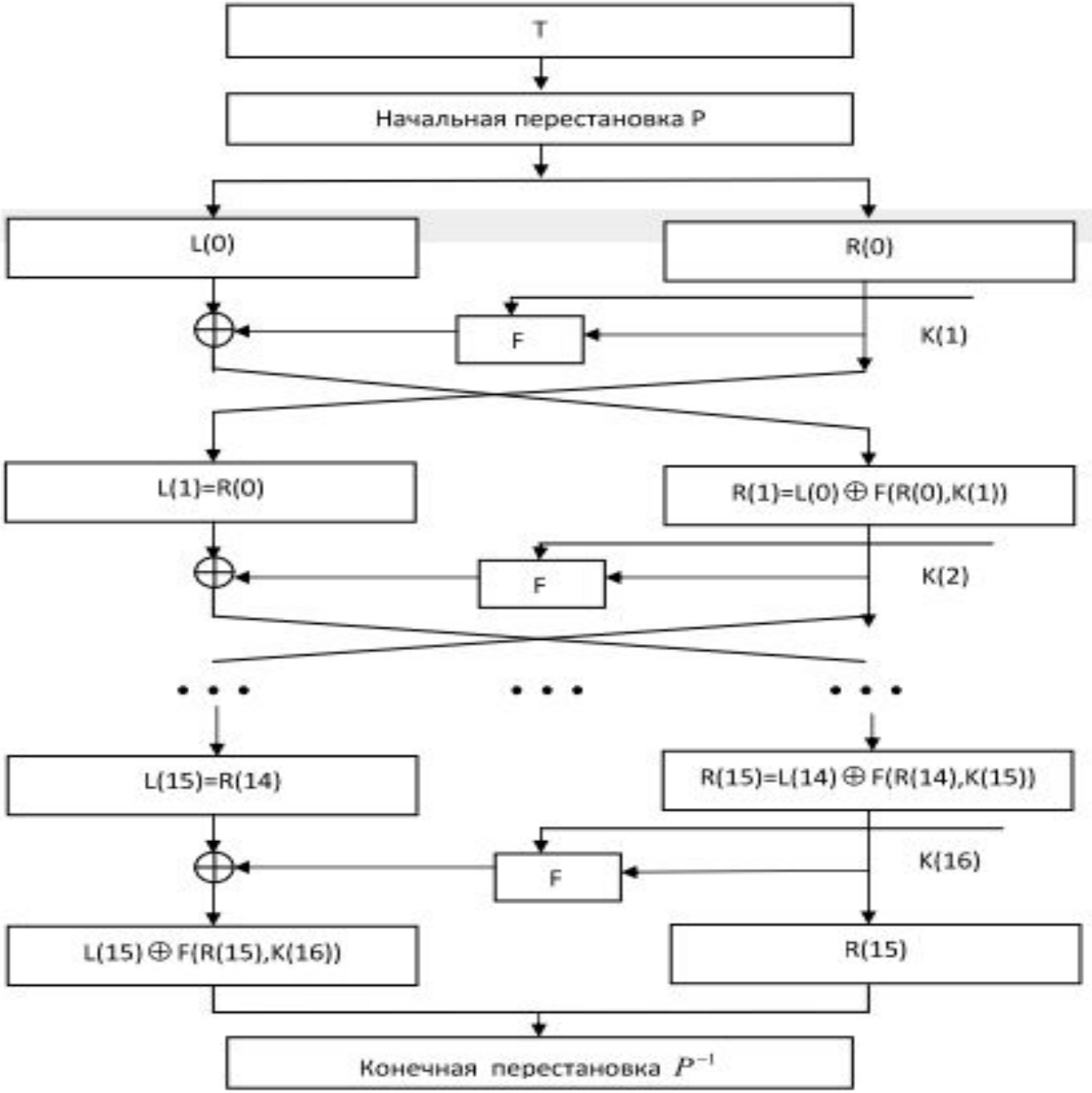
- $L(i)=R(i-1)$
- $R(i)=L(i-1)\oplus F(R(i-1),K(i))$,

Мұнда L(i)и R(i) – бұл і-ші тактте сол және оң ішкі тізбектер, K(i)- 64 биттік кілттен алынған 48 биттік кілт. 16-шы итерацияда R(16) мен L(16) (орын ауыстырусыз) тізбектерін алады, олар (R(16), L(16)) ні 64-биттік тізбекке біріктіреді. Содан осы тізбектің биттерін P^{-1} кері орын ауыстыру матрицасымен сәйкес орын ауыстырады.

40	08	48	16	56	24	64	32
39	07	47	15	55	23	63	31
38	06	46	14	54	22	62	30
37	05	45	13	53	21	61	29
36	04	44	12	52	20	60	28
35	03	43	11	51	19	59	27
34	02	42	10	50	18	58	26
33	01	41	09	49	17	57	25

- P^{-1} мен P матрицалары келесі түрде қатынасады: P^{-1} матрицасының 1-ші элементінің мәні 40 тең, ал P матрицасының 40-шы элементінің мәні 1 тең, P^{-1} матрицасының 2-ші элементінің мәні 8 тең, ал P матрицасының 8 элементінің мәні 2 тең және т.с.с.
- і-ші итерацияда K(i) – бұл 64 биттік алғашқы кілттен келесі түрде алынған 48 биттік кілт: итерацияның алдында 64 биттік кілттен 56 биттік кілтті әрбір сегізінші битті лақтыру жолымен алынады, яғни 8, 16, 24, 32, 40, 48, 56, 64 позицияларында тұрған биттер. Бұл биттер таңба ауысуын бақылау биттері ретінде қалыптастырылған және кілттің бүтіндігін бақылау үшін қолданылады. Содан G кестесімен сәйкес 56 биттік кілттің бастапқы орын ауысуы жүргізіледі.

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



2-сурет. DES шифраторының схемасы

Осылай алынған 56 биттік кілт екі 28 биттік блокқа бөлінеді: C(0) – сол және D(0) – оң. C(1) және D(1) блоктарында КР орын ауыстыру көмегімен 48 разряд таңдап алынады:

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

Бұл разрядтар бірінші итерацияда қолданылады. і-ші итерацияда C(i), D(i) блоктарын алу үшін C(i-1), D(i-1) блоктарын s(i) позицияға циклдік жылжыту жүргізіледі, мұнда s(i) кесте бойынша таңдалынады

1 кесте. 16 итерация үшін циклдік жылжыту

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

Ары қарай қайта КР орын ауыстыру көмегімен 48 разрядты кілтті таңдаймыз.

Кілтті есептеу алгоритмінің блок-схемасы 2-суретте келтірілген.

Енді DES стандартында F(R(i-l),K(i)) шифрлеу функциясын қарастырайық. Ол 3-суретте схема түрінде көрсетілген.

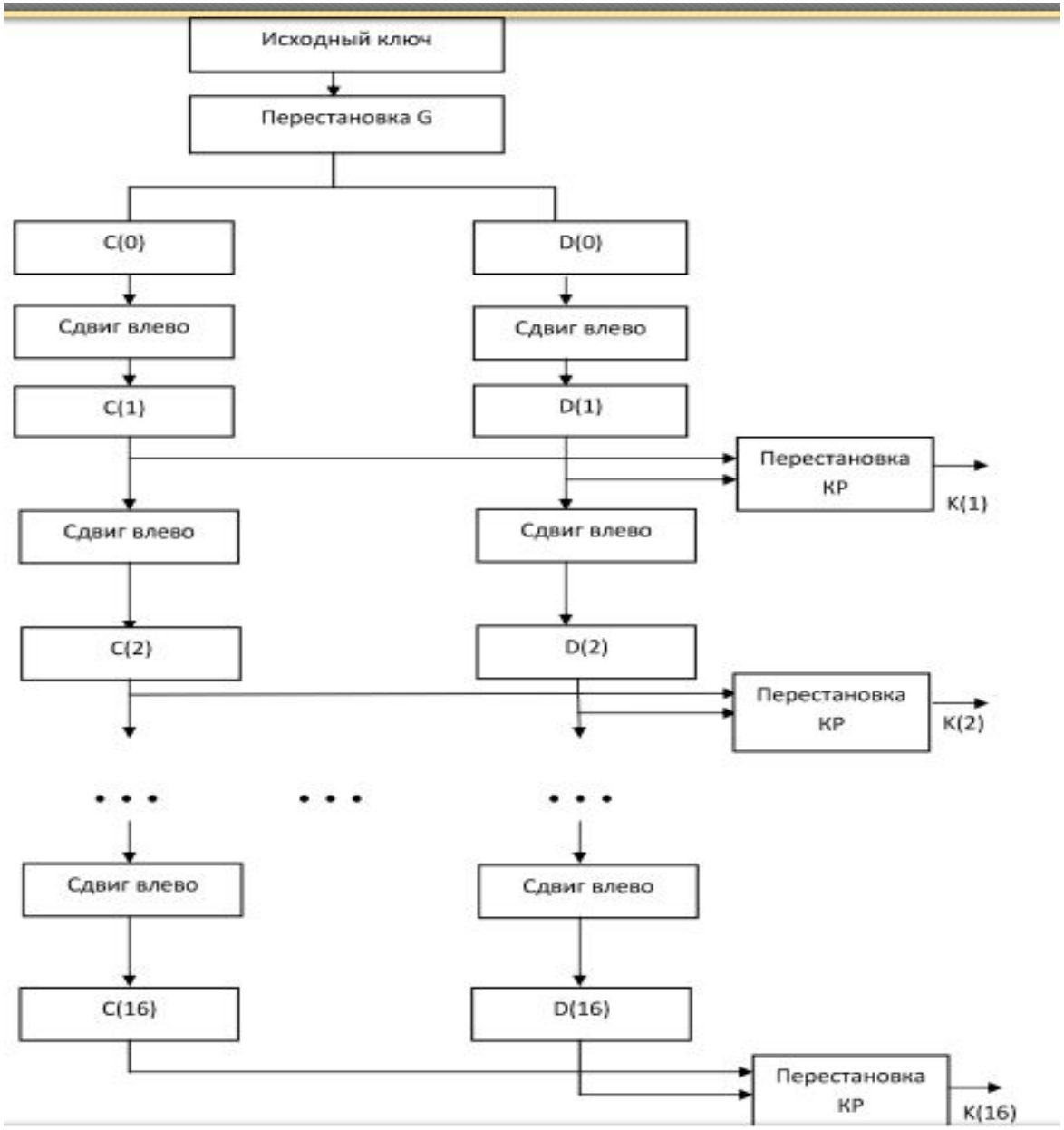
Ғ функциясын есептеу үшін келесі функция-матрица қолданылады:

- Е -32 битті тізбектің 48-биттікке кеңейтілімі,
- SI, S2, ..., S8- 6-биттік блоктың 4-биттікке сызықты емес түрленуі,
- Р2 – 32-биттік тізбекте биттің орын ауысуы.

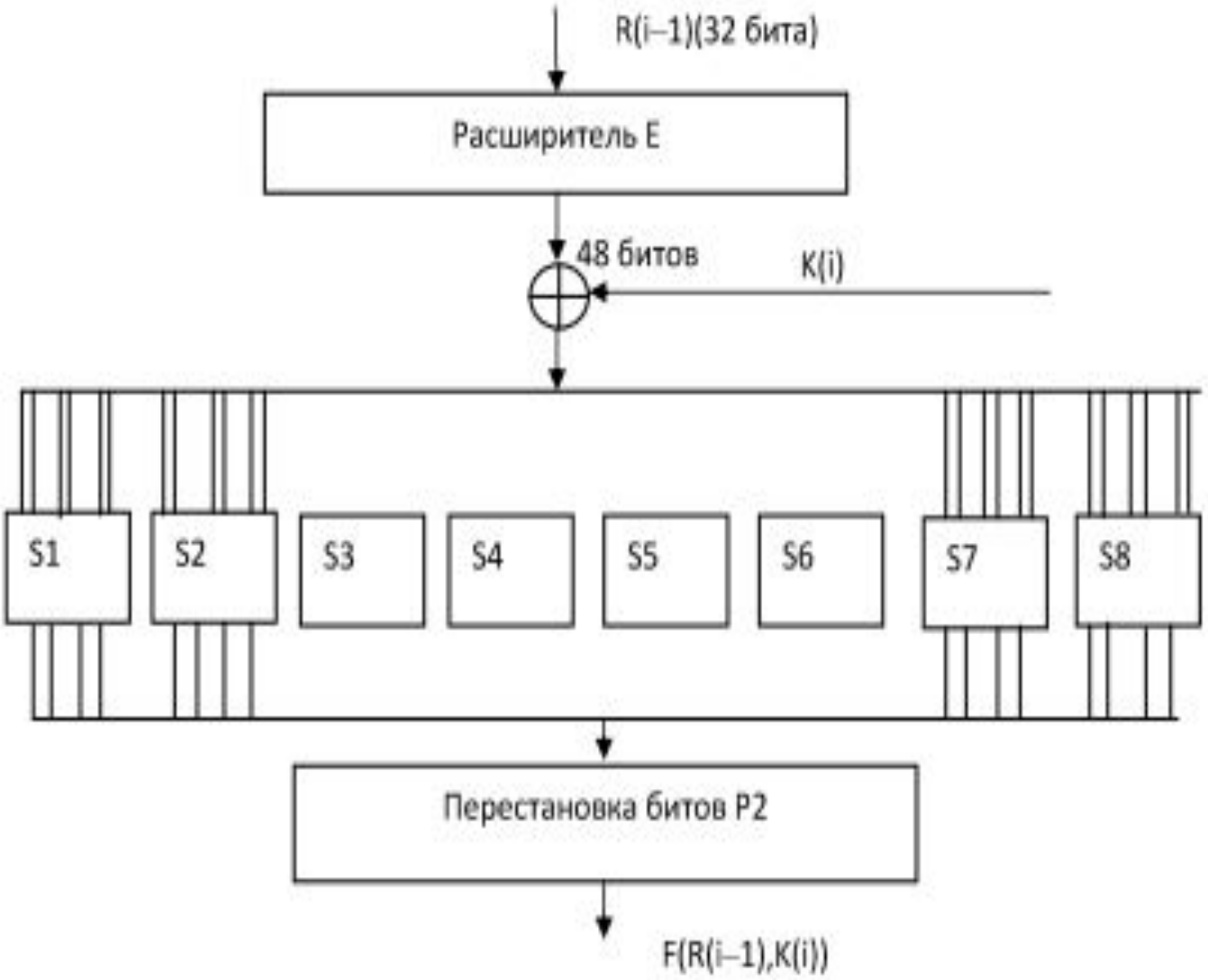
Е кеңейтілім функциясы келесі кестемен анықталады

32	**01**	**02**	**03**	**04**	**05**
04	**05**	**06**	**07**	**08**	**09**
08	**09**	**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**	**01**

E(R(i-l)) кеңейтілім нәтижесі 48-биттік тізбекті көрсетеді, ол 2 модулі бойынша K(i) 48-биттік кілттікпен қосындыланады. Нәтижелі 48-биттік тізбек 8 блокқа B(1) B(2) B(8) әрбіреуі 6 бит бойынша бөлінеді, яғни E(R(i-1)) xor K(i) = B(1)B(2)...B(8). S_j функция-матрица кірісіне 6-биттік блок $B(j) = (b_1,b_2,b_3,b_4,b_5,b_6)$ түседі делік. Сонда (b_1,b_6) биттер S_j сипаттайтын матрицадағы жол номерін анықтайды, ал (b_2, b_3, b_4, b_5) биттер осы матрицадағы баған номерін анықтайды. S_j блогының шығысы сәйкес жол мен баған қиылысында тұратын 4-биттік элемент болады.



3-сурет. Кілтті қалыптастыру схемасы



4-сурет. Шифрлеу функциясы

Мысалы, B(1)=(010111) болсын, онда жол номері 1 тең, ал баған номері 11, яғни S1 матрицасында 1-ші жол мен 11-ші баған қиылысында тұрған элементті табамыз. Бұл 11 блок шығысында 1011 түріне ие.
Әрбір 6 биттік блоктың сегізіне түрлендіруді қолдана отырып, 32-биттік шығыс тізбекті аламыз және оған P2 орын ауыстыруды қолданамыз.

16	07	20	21
29	12	28	17
01	15	23	26
05	18	31	10
02	08	24	14
32	27	03	09
19	13	30	06
22	11	04	25

Нәтижесінде F(R(i-l), K(i)) = P2(S1(B(1)),...S8(B(8))) аламыз.

Таблица 2. Функции преобразования S1, S2, ..., S8

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

DES стандартына шабуыл және DES күшейту нұсқалары

Кілт ұзындығы жеткілікті үлкен болып таңдалынғандықтан, кілт бойынша толық алмасу есептеулі орындалмайтын болатындай, онда криптошабуылдар толық алмасудан күшті әдістерге негізделген. Блоктық шифрлерді криптоталдау әдістерінің арасында мыналарды ерекшелейді:

- Сызықты талдау
- Дифференциалды талдау

Сызықты криптоталдау 1984 жылы ұсынылған. Негізгі идеясы кіру және шығудың қандайда бір биттерін байланыстыратын жасырын сызықты теңдеулерді пайдаланудан тұрады. Бұл шабуылды орындау кезінде көп ашық мәтіндерді және оған сәйкес шифрограммаларды қолдану ұсынылады.

Дифференциалды криптоталдау 2 модулі бойынша алғашқы мәтін қосындысы мен 2 модулі бойынша сәйкес шифрмәтіннің қосындысы арасында корреляцияны іздеуден тұрады. Дифференциалды талдау, мысалы, раундтың ішкі кілтін анықтау үшін Фейстель желісінің бір раундының нәтижесіне қолданылуы мүмкін. Дифференциалды криптоталдауға төзімді шифрлерді құру үшін 5-блокты қолдану керек, онда жоғары ықтималды айырмашылықтың туындауының минималды ықтималдығы бар. Ары қарай, дифференциалды және сызықты криптоталдауға дәлелденген төзімділігімен шифрлер құруға болатынын көреміз.

DES кілттің кіші ұзындығы үшін критикаға бірнеше рет ұшырады (2^{56}кілті бойынша алу қиындығы), ал 1998 жылы арнайы компьютерде “ашық мәтін-шифрмәтін” берілген жұбы бойынша шабуыл сәтті болды. Кілтті ашудың орташа уақыты 3 тәулікті құрады. DES дифференциалды және сызықты криптоталдауы 2^{47} мен 2^{48} ашық мәтіндерді сақтау үшін және 2^{47} мен 2^{48} қадам ашу үшін жадыны қажет етеді. Қазір DES төзімді алгоритм болып есептелмесе де, бұл қате тұжырым болады. Ол құпиялылықтың жоғары емес деңгейінде хабарламаны шифрлеу кезінде қолданылуы мүмкін, яғни дешифрлеуге үлкен қаржылық капиталы бар мемлекеттік құрылымдар немесе корпорациялардың қосылу мүмкіндігі жоқ болғанда. Кері жағдайда DES күшейтілген нұсқаларын пайдалану керек.

Осыған байланысты DES жүйесін жандандыру бойынша бірнеше ұсыныстар қабылданды.

Бірінші ұсыныс DES –ті әртүрлі кілтпен екі рет пайдаланудан тұрады, оның әрбіреуі 56 бит ұзындығына ие. Кілттің жалпы ұзындығы мұндай жүйеде 112 битке тең, бірақ, мұндай жүйеде кілтті ашу қиындығы DES-ке қарағанда 2 есе ғана өседі. Шынында да, K_x және K_y кілттерімен екі еселік шифрлеуді орындаймыз делік, сәйкесінше:

$Y = DES_{Ky}\,(DES_{Kx}\,(X))$.

Бұл жағдайда жүйе "meet-in- the-middle" (ортасында кездесу) шабуылына қатысты төзімді емес болып шығады. Бұл шабуылды сипаттайық. Бізде X_1 ашық мәтін және Y_1 шифрмәтін бар болсын, олар DES алгоритмі көмегімен екілік шифрлеу нәтижесінде алынған болсын. K_x мүмкін кілттер жиынына X_1 шифрлеп, нәтижесін кестеге жазайық. K_y мүмкін кілттер жиынына Y_1 шифрлеп, нәтижесін кестеге жазайық. Содан соң кестеде сәйкестікті іздейміз, бұл сәйкестік K_x және K_y ізделінді кілттер болу үшін мүмкін кандидаттар – кілттерге сәйкес келеді. Таңдауды қысқарту үшін тағы бір жұп – ашық мәтін – шифрмәтінді пайдалану керек және шабуылды қайталау керек. Бұл жағдайда шифрлеу және дешифрлеу кезінде біз кілттер-кандидаттарды ғана пайдаланамыз. Кестені сақтау үшін жады көлемі $2 \times 2^{56} = 2^{57}$ тең, сондықтан кілт бойынша таңдау қиындығы 2 есе ғана өседі.

DES күшейту бойынша ең белгілі ұсыныс мына формуламен анықталатын үштік DES деп аталады

$Y = DES_{Kz} (DES_{Ky}^{-1} (DES_{Kx} (X)))$.

Мұндай жүйеде кілт 56x3 = 168 бит ұзындыққа ие. 64 биттік блокта шифрлеу бір ішкі кілтпен шифрлеумен, дешифрлеу басқасымен және үшіншісімен шифрлеу жүзеге асырылады. Екінші қадам дешифрлеу болып табылудың мәні DES_{Ky}^{-1} дешифрлеуі- DES-пен сәйкестігінде болып табылады. Бірақ, үштік DES DES-ке қарағанда баяу.

Р. Ривестом ұсынылған тағы бір DES модификациясы “кеңейтілген DES” деген атау алды. Бұл жағдайда шифрмәтінді келесі түрде алады:

$Y = K_y DES_K (X K_x)$,

Яғни кілт үш ішкі кілттен және 54+64+64=184 биттен тұрады . K_x және K_y кілттерін алдын ала және аяқтайтын баспалы кілт деп атайды. DES пайдаланудың бұл нұсқасына қатысты, ол кілтті таңдауға негізделген шабуылға төзімділігін ұлғайтатыны дәлелденген. Сондай-ақ ол дифференциалды және сызықты криптоталдауға төзімділігін ұлғайтады.

1996 жылдың соңында жаңа стандарт құруға конкурс жарияланды, ол DES стандартының орнына келу керек болды. Кандидаттардың бірі SAFER+ алгоритмі болды. Оны Cylink компаниясы Армян ғылым академиясымен бірге ұсынды. Бұл алгоритм таңдаудың бірінші турынан өтті, бірақ жеңімпаз болмады. Қазіргі уақытта ол деректерді шифрлеу үшін емес, ал 10-нан 100 м арақашықтықта цифрлік электронды құрылғылар арасында сымсыз байланыстың Bluetooth хаттамасында хабарламалардың аутентификациясы үшін қолданылады. Бұл алгоритм Фейстель желісінің құрылымын пайдаланбайтындығымен қызықты. Шифр 128 бит ұзындықты блоктармен және 128,192 немесе 256 бит ұзындықты кілттермен жұмыс істейді. Шифрлеу және дешифрлеу процедуралары итерациялар тізбегін көрсетеді. Итерация саны (6-10) кілт ұзындығына байланысты. Әрбір итерация төрт сатыдан тұрады:

- Бірінші ішкі кілтті араластыру;
- Сызықты емес ауыстыру;
- Екінші ішкі кілтті араластыру;
- Сызықты араластыру.

Әрбір итерацияда128 бит(256 бит кілт кезінде) ұзындығымен екі ішкі кілт қолданылады. Бірінші ішкі кілт кіру блогының 1, 4, 5, 8, 9, 12, 13, 16 номерлерімен байттарымен екі модулі бойынша разрядты қосылады. 2, 3, 6, 7, 10, 11, 14, 15 номерімен байттар 256 модулі бойынша осы ішкі кілт байттармен қосылады. Екінші ішкі кілт итерация соңында қосылады, бірақ разряд бойынша қосылған байттар енді 256 модулі бойынша қосылады және керісінше.