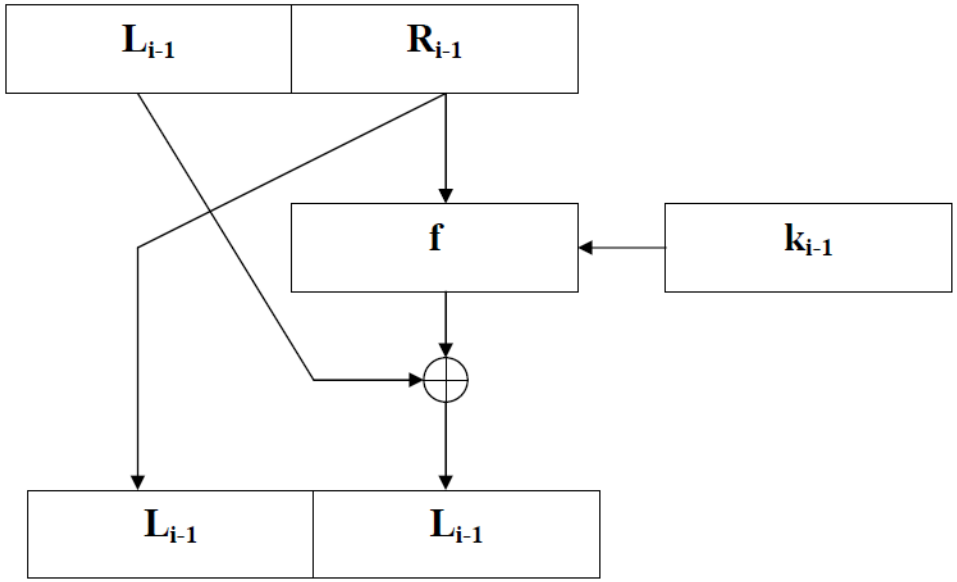
Дәріс 3. Блокты шифрларды құру принциптері

Дәріскер: PhD Темирбекова Ж.Е.

Дәріс жоспары:

- Блоктық шифрларды құрудың негізгі принциптері
- DES шифры
- DES алгоритмінің жұмыс режимдері

Блоктық шифрларды құрудың негізгі принциптері



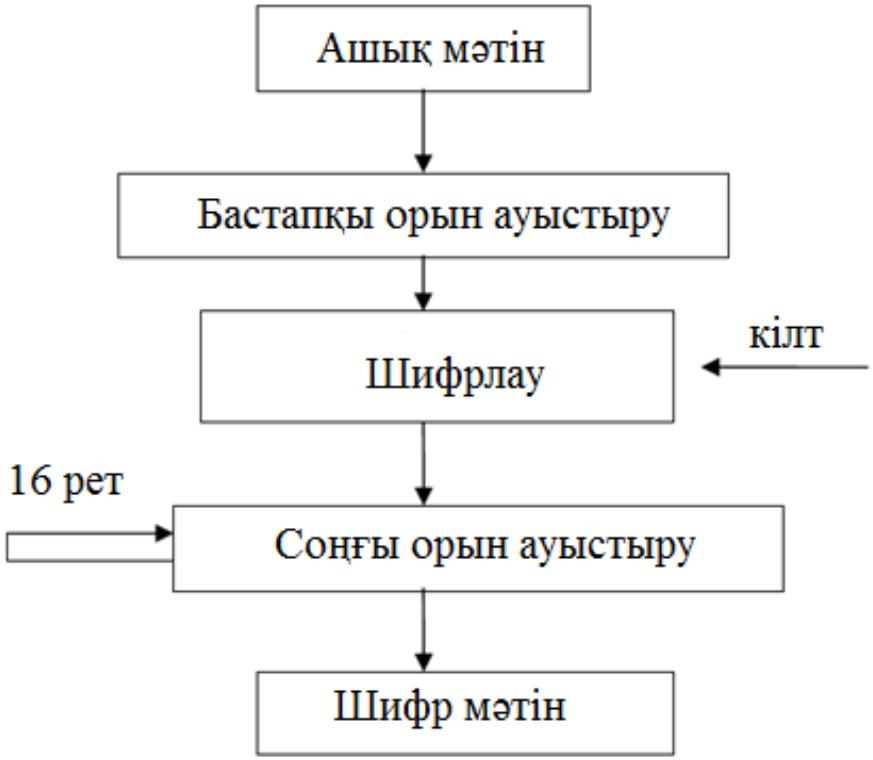
2.1 – сурет. Фейстель шифры (бір айналым)

DES шифры

- Ең алғашқы кеңінен қабылданған және қолданылатын деректерді шифрлау стандарттарының бірі DES (Data Encryption Standard) болды. Бұл стандарт Америкада 1977 жылы жарияланған. DES стандартының алдында IBM компаниясының Люцифер жүйесі болды. Оның үстіне DES шифрлау алгоритмі Люциферде қолданылатын алгоритмге өте ұқсас. Сондай-ақ, DES стандарты Фейстель шифрінің өкілі, дәлірек айтқанда, жалпылама болып табылатынын ескеру қажет.

DES шифры

- Циклдік алфавиттер, кілтпен шифрлау ережесі.

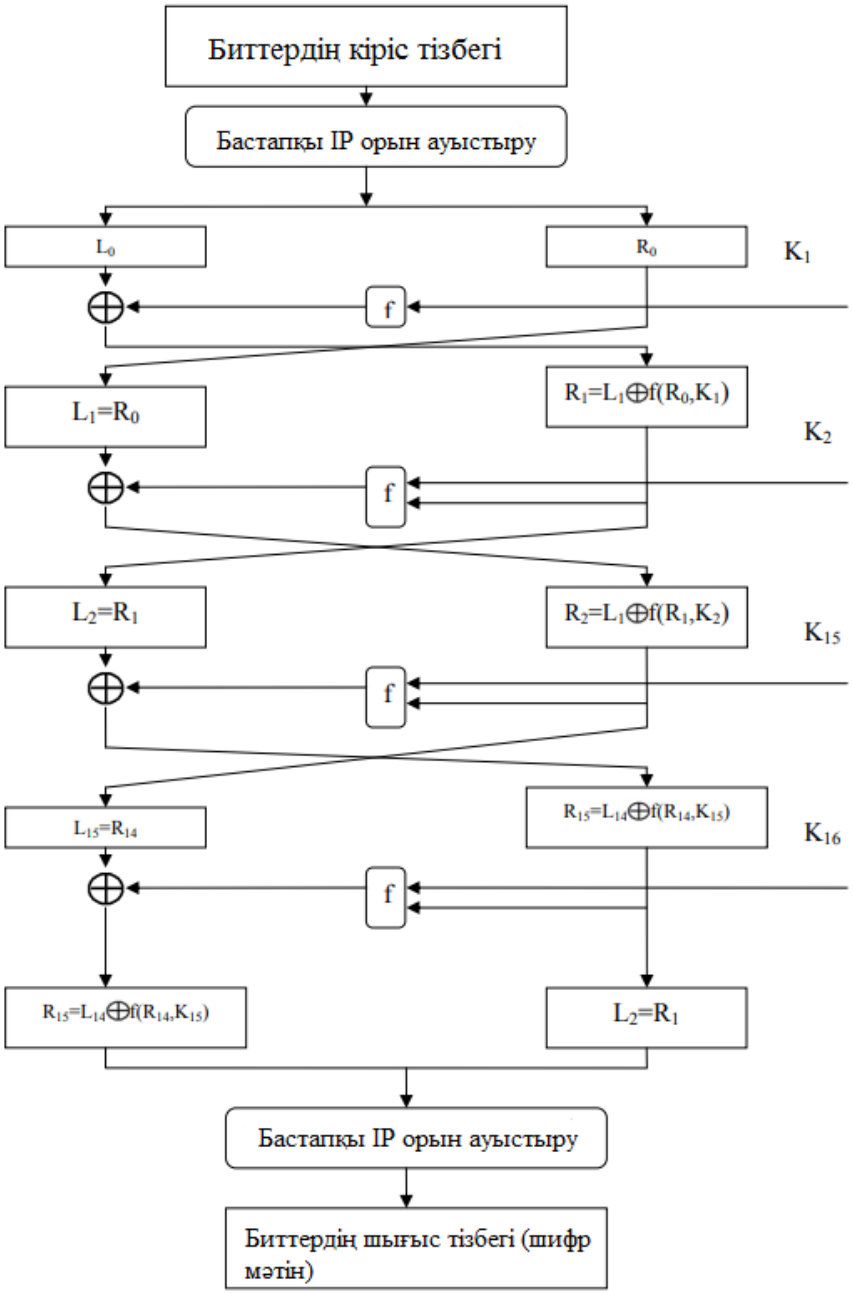


Бастапқы кілтті дайындаудың G функциясы

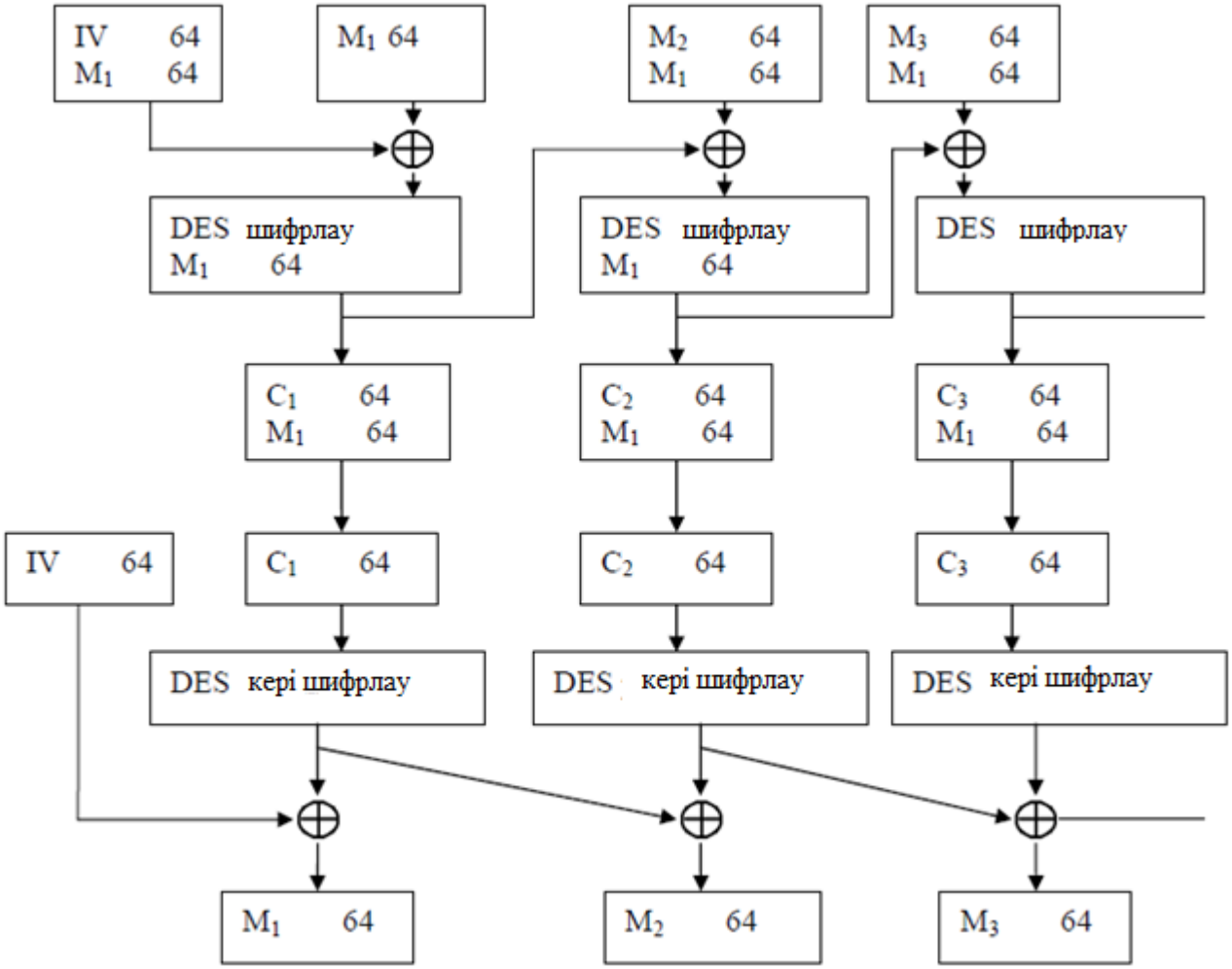
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

$S_1, S_2, \ldots, S_8$ түрлендіру функциялары

14	4	13	1	5	15	11	8	3	10	6	12	5	9	0	S_1
0	15	7	4	2	2	13	1	10	6	12	11	9	5	3	
4	1	4	8	14	6	2	11	15	12	9	4	3	10	5	
15	12	8	2	13	9	1	7	5	11	3	14	10	0	6	
15	1	8	14	4	11	3	4	9	7	2	13	12	0	5	S_2
3	13	4	7	6	2	8	14	12	0	1	10	6	9	11	
0	14	7	11	15	4	13	1	5	8	12	6	9	3	2	
13	8	10	1	10	15	4	2	11	6	7	12	0	5	14	
10	0	9	14	3	3	15	5	1	13	12	7	11	4	2	S_3
13	7	0	9	6	4	6	10	2	8	5	14	12	11	15	
13	6	4	9	3	15	3	0	11	1	2	12	5	10	14	
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	
7	13	14	3	3	6	9	10	1	2	8	5	11	12	4	S_4
13	8	11	5	8	15	0	3	4	7	2	12	1	10	14	
13	6	9	0	6	11	7	13	15	1	3	14	5	2	8	
3	15	0	6	0	1	13	8	9	4	5	11	12	7	2	
2	12	4	1	6	10	11	6	8	5	3	15	13	4	14	S_5
14	11	2	12	12	7	13	1	5	0	15	10	3	0	8	
4	2	1	11	10	13	7	8	15	9	12	5	6	9	0	
11	8	12	7	7	14	2	13	6	15	0	9	10	3	5	
12	1	10	15	4	2	6	8	0	13	3	4	14	4	5	S_6
10	15	4	2	10	12	9	5	6	1	13	14	0	7	3	
9	14	15	5	1	8	12	3	7	0	1	10	1	11	1	
4	3	2	12	9	5	15	10	11	14	0	7	6	13	8	
4	11	2	14	7	0	8	13	3	12	14	7	10	0	6	S_7
4	11	2	14	7	0	8	13	3	12	14	7	10	0	6	
13	0	11	7	2	9	1	10	14	3	12	12	14	10	8	
1	4	11	13	9	3	7	14	10	15	3	8	5	15	9	
6	11	13	8	15	4	10	7	9	5	15	15	0	5	3	S_8
13	2	8	4	4	15	11	1	10	9	5	14	15	2	12	
1	15	13	8	12	3	7	4	12	5	9	11	3	0	9	
7	11	4	1	1	12	14	2	0	6	5	13	2	14	5	


Биттердің кіріс тізбегі
Бастапқы IP орын ауыстыру
L0
R0
K1
f
L1=R0
R1=L1⊕f(R0,K1)
K2
L2=R1
R2=L1⊕f(R1,K2)
K15
L15=R14
R15=L14⊕f(R14,K15)
K16
R15=L14⊕f(R14,K15)
L2=R1
Бастапқы IP орын ауыстыру
Биттердің шығыс тізбегі (шифр мәтін)

DES алгоритмінің Шифр блоктарының ілінісу режиміндегі сұлбасы



Қолданылған әдебиеттер

- 1. Гольдвассер С., Беллар М. Достижения в криптологии / Гольдвассер С. – М.: Триумф, 2016. – 513 с.
- 2. Шнайер, Брюс. Криптографическая методы защиты информации, 26-я ежегодная международная конференция по криптологии, Санта-Барбара, Калифорния, США, 20–24 августа 2022 г.
- 3. Фергюсон Н., Шнайер Б., Коно Т. Криптографическая инженерия: принципы проектирования и практическое применение. / Фергюсон Н. – М.: Пресс, 2022. – 416 с.