Course: "Fundamentals of Cryptography" 23-11-2024

Laboratory work No. 6.

The purpose of the laboratory work: the formation of skills in working with encryption algorithms using the Feistel grid.

The objective of the laboratory work: modeling of coding algorithms using the main elements of the Feistel mesh transformation.

Exercise:

1. Write a program to implement a number of simplified DES operations. The information message is encoded in accordance with the general scheme of the DES algorithm.

The programs may be written in a high-level language and implement DES operations in a simplified form, but they are transferred: - the use of two rounds;

- no modification of keys in each round;
- the expansion operation is not converted.

Specification of the task:

1. As a test information notification, the vikorist notification is provided by USTASI. The English alphabet is used as part of the alphabet. I – student's official number.

Please note that the skin letter is one bit.

2. Parts L and R are designated as a subdivision of information communication throughout.
3. The mental table of the cob permutation of IP is shown below:

16	19	5	1	13
14	4	21	10	8
24	11	3	12	22
17	9	20	7	18
23	2	6	15	25

2. Using the Intel x86 IP initial and final permutation tables and the original DES IP initial and final permutation tables (shown below), fill in the correspondence table between the following elements of all tables:

Element value in initial permutation table in Intel x86	Element value in initial permutation table in original DES	Element value in final permutation table in original DES
14		
23		
61		
6		

Initial bit permutation (IP). Bit numbering in Intel x86.

6	14	22	30	38	46	54	62
4	12	20	28	36	44	52	60
2	10	18	26	34	42	50	58
0	8	16	24	32	40	48	56
7	15	23	31	39	47	55	63
5	13	21	29	37	45	53	61
3	11	19	27	35	43	51	59
1	9	17	25	33	41	49	57

Final bit permutation (IP $^{-1}$). Bit numbering in Intel x86.

24	56	16	48	8	40	0	32
25	57	17	49	9	41	1	33
26	58	18	50	10	42	2	34
27	59	19	51	11	43	3	35
28	60	20	52	12	44	4	36
29	61	21	53	13	45	5	37
30	62	22	54	14	46	6	38
31	63	23	55	15	47	7	39

Explanation: The first most significant bit in the numbering of bits in Intel x86 - and we see it is the number 6 - goes to the first place in the numbering of bits in the original DES - and this we see is the 58th place. That is, we hid it - this number somewhere (in this case, in place 58, but it could have been anywhere). But we remember that it is the senior bit that is the first - it is in the first place. In the final permutation table, we see that place 58 is in the second row from the bottom and the seventh column. That is, our number 6 should be placed in this cell. It is right there: you can see that the number 6 is right there. And it has to be the first one again so that we can decode the message correctly. Question: where should our number 6 go? We will find the answer in the table of the final permutation: this place is 40, because the number 40 itself is in the place of a_{11}.

3. Calculate the result of replacing the input 6-bit number using
- the first S-box (the table was given in the lecture);
- the second S-box (given below) if the first 6-bit part of the input block has the values:Calculate the result of using the first S-box (it was given in a lecture) if the first 6-bit part of the input block has the value:

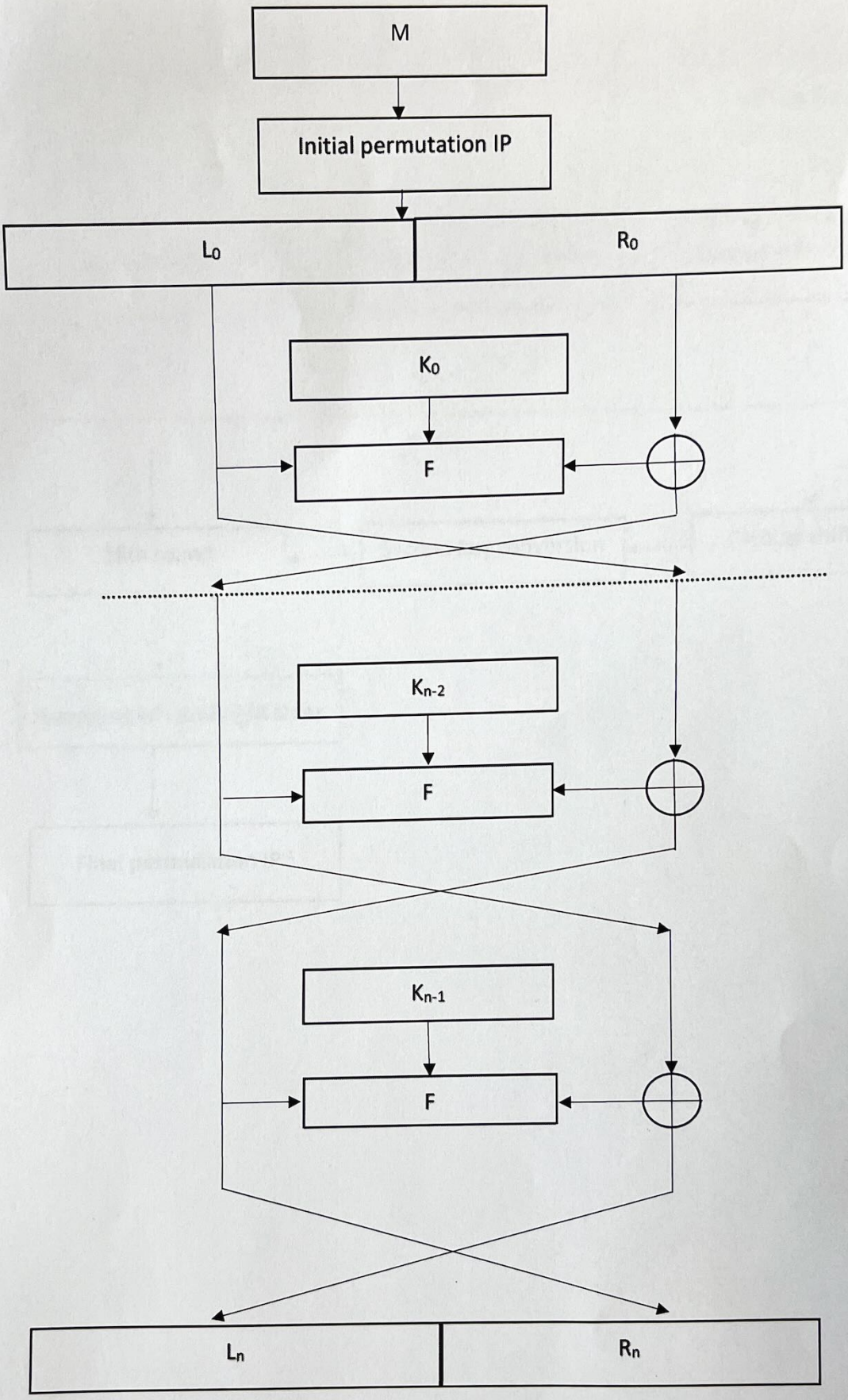
A. 011010 ;
B. 001111 ;
C. 110110 ;
D. 110011 .

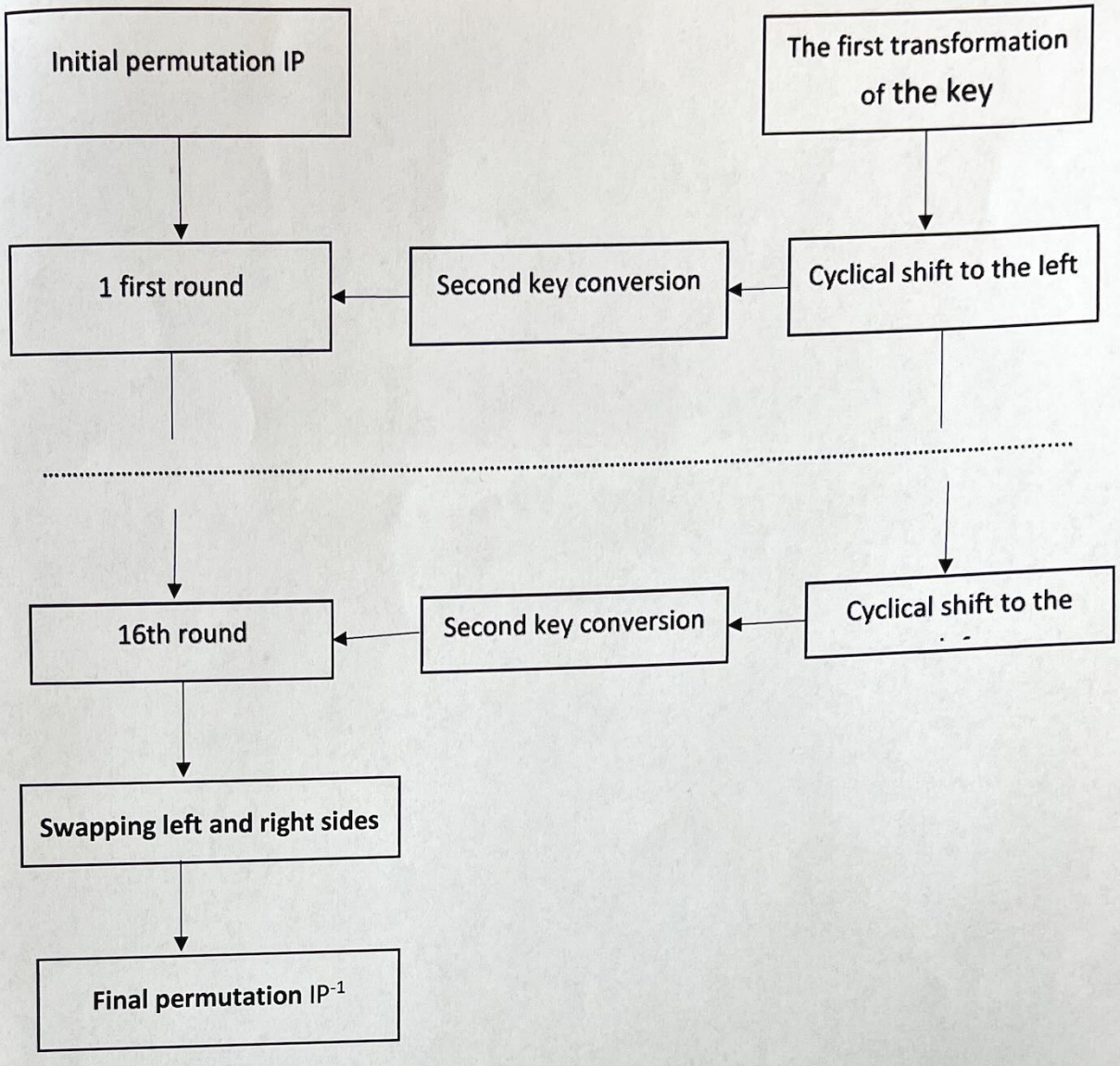
The second DES S-box

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

Application. Simple General Scheme of DES.

Simplified DES Scheme for Lab Assignment




Initial permutation IP
The first transformation of the key
1 first round
Second key conversion
Cyclical shift to the left
16th round
Second key conversion
Cyclical shift to the
Swapping left and right sides
Final permutation IP-1