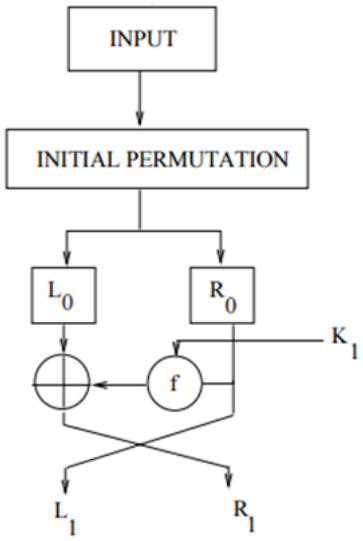
Introduction to Cryptography—Homework 3
Due: Sunday, February 28, 2021, 11:59pm

- You may work on and submit your homework in **groups of 2** or individual.
- Submit your solutions to the appropriate dropbox folder on myCourses as **single (readable) pdf**.
- The homework must be entirely your own work.
- Before you start on the homework, please read the rules on collaboration and submission in the syllabus.
- Keep in mind that, as stated in the syllabus, I will not answer questions the day the homework is due.
- Each homework problem indicates the number of points it is worth for grading purposes. While individual problems may be worth more or fewer points than others, each homework assignment carries weight as stated in the syllabus.

1. **(3 points)** We consider Feistel network, which operates on 16-bit blocks of plaintext. A sketch of the encryption with first round is given below:



Consider the following bit sequence as the input data:

1011000110101100

a) Describe L_1 and R_1 with respect to R_0 and L_0

b) The 16 bits of the input are first reorganized by the following initial permutation (IP):

$$\begin{array}{cccc} 8 & 13 & 4 & 9 \\ 16 & 5 & 12 & 1 \\ 7 & 14 & 3 & 10 \\ 15 & 6 & 11 & 2 \end{array}$$

- Write down the permuted input.
- Compute the inverse permutation namely IP^{-1}.

2. **(2 points)** What is the output of the DES S-box below for the following inputs:

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

a) 111100

b) 010101

c) 000111

d) 011101

3. **(3 points)** What is the output of the first round of the DES algorithm when the plaintext and the key are both all zeros? Write the output of each S-box (S-boxes)?

4. **(3 points)** This problem deals with the DES key schedule. Calculate the round key for the first round using the following table:

Key	BBBB 5555 1111 EEEE$_{Hex}$
Key state after $PC-1$	
Key state after rotation left	
Round key for Round 1 (after $PC-2$)	

5. (**4 points**) We analyze the security of DES double encryption ($2DES$) by doing a cost-estimate:

$$2DES(x) = DES_{K_2}(DES_{K_1}(x))$$

a) First, let us assume a pure key search without any memory usage. For this purpose, the whole key space spanned by K_1 and K_2 has to be searched. How much does a key-search machine for breaking $2DES$ (worst case) in 1 week cost? In this case, assume ASICs which can perform 10^7 keys per second at a cost of \$5 per IC. Furthermore, assume an overhead of 50% for building the key search machine.

b) Let us now consider the meet-in-the-middle (or time-memory tradeoff) attack, in which we can use memory. Answer the following questions:

- How many entries have to be stored?
- How many bytes (not bits!) have to be stored for each entry?
- How costly is a key search in one week? Please note that the key space has to be searched before filling up the memory completely. Then we can begin to search the key space of the second key. Assume the same hardware for both key spaces.

For a rough cost estimate, assume the following costs for hard disk space: \$8/10 GByte, where 1 GByte = 10^9 Byte.