
CS369: INTRODUCTION TO CRYPTOGRAPHY AND NETWORK SECURITY LAB
LAB ASSIGNMENT II

Course Instructor: Dr. Dibyendu Roy

Due: Sep 29, 2024, 11:59 pm

Instructions: Clearly write your name and roll number on the top of your C code. Code must be well commented. Program file name should be YOUR ROLL NO.c

You need to implement a modified version of DES with 2 rounds. The description of the modified DES is as follows.

1. Your plaintext P will be 8 bit positive integer (input).
2. Your secret key K will be 10 bit positive integer (input).
3. Two round keys k_1 and k_2 are generated using the functions P_{10} , Shift, and P_8 .

P_{10}							
3	5	2	7	4	10	1	9

P_8							
6	3	7	4	8	5	10	9

$$\text{Shift}(x_1, x_2, x_3, \dots, x_{10}) = (x_2, x_3, x_4, x_5, x_1, x_7, x_8, x_9, x_{10}, x_6)$$

4. The first round key $k_1 = P_8(\text{Shift}(P_{10}(K)))$
5. The second round key $k_2 = P_8(\text{Shift}^2(P_{10}(K)))$
6. IP is applied on the plaintext and IP^{-1} is applied on the output after the second round. The description of IP and IP^{-1} are given below.

IP							
2	6	3	1	4	8	5	7

IP^{-1}							
4	1	3	5	7	2	8	6

7. The round function F works as follows.

- $F(R, K) = P_4(S(E(R) \oplus K))$

E							
4	1	2	3	2	3	4	1

P_4			
2	4	3	1

- $S(x) = S_1(x_1) \parallel S_2(x_2)$, where $x = x_1 \parallel x_2$ and $S_i : \{0,1\}^4 \rightarrow \{0,1\}^2$. For each x_i find r, c such that $x_i = r \parallel c$ and look into the row number r and column number c of table corresponding to the table of S_0, S_1 to compute the output.

$S_0 :$	01	00	11	10
	11	10	01	00
	00	10	01	11
	11	01	11	10
$S_1 :$	00	01	10	11
	10	00	01	11
	11	00	01	00
	10	01	00	11

Implement 2 rounds of encryption as well as decryption. If your code is correct then decryption of ciphertext generated from encryption function should match with plaintext for random input of plaintext and key. Your code will take plaintext and key as input (in decimal), print the ciphertext and decrypted text in decimal.