Indian Institute of Engineering Science and Technology, Shibpur.

Information Technology Department

Information and Systems Security Lab 2020

Assignment – 4

Date: 05.03.2020

Submission Deadline: March 18, 2020

PART - A

Implement an Iterated Substitution Permutation cipher consisting of Nr = 4 rounds, with the following specifications:

1. Each round consists of round-key mixing followed by a substitution and a permutation.
2. Assume the plain text and cipher text, each to be 8-bits long.
3. The key schedule is generated by selecting (4r-3)th through (4r+4)th key bits as the round key for round r. (The minimum length of the key is given by 1×8+Nr×4=24 bits. Select a random string of 24 bits as the key.)
4. The round key mixing is done by a bitwise XOR operation.
5. Perform key whitening at the beginning and end of each round.
6. Assuming l = 4, the substitution function at each round is specified by the following S-box:

input	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
output	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

7. The permutation function for each round is:

Input	1	2	3	4	5	6	7	8
Output	1	4	5	7	3	6	2	8

(Drop the permutation function at the last round. Think why.)

Implement both the encryption and decryption functions for the above cipher.

PART - B

1. Implement Data Encryption Standard (DES). (Refer to appropriate text for detailed specifications.)
    a. For implementation you may skip the initial permutation (and its inverse permutation at the end).
    b. Implement both encryption and decryption functions.
    c. You may assume the plaintext to be a random string of bits, divide it into blocks to encrypt.
    d. Select the key to be any bitstring of length 56 bits.