CMPS 485 - Computer Security - Fall 2018
Homework 2

You need to submit homework 2 Word document and your solution implementation to your GitHub repository.

1. [18 pts] The S-boxes are the most crucial elements of DES because they introduce a nonlinearity to the cipher, i.e., S(a)⊕S(b) ≠ S(a⊕b). Verify this property by computing the output of S_1 for the following pairs of inputs:
   - x_1 = 000000, x_2 = 000001
   - x_1 = 111111, x_2 = 100000
   - x_1 = 101010, x_2 = 010101

S-box S_1

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

2. [7 pts] Assume we perform a brute force attack against DES with one pair of plaintext and ciphertext. How many keys do we have to test in a worst-case scenario if we apply an exhaustive key search? How many on average?

3. [25 pts] Let **A** the state matrix of the input message to be encrypted using AES:

$$A = \begin{bmatrix} 01 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{bmatrix}$$

The first 2 subkeys are:

$$K_0 = \begin{bmatrix} 2B & 28 & AB & 09 \\ 7E & AE & F7 & CF \\ 15 & D2 & 15 & 4F \\ 16 & A6 & 88 & 3C \end{bmatrix} \qquad K_1 = \begin{bmatrix} A0 & 88 & 23 & 2A \\ FA & 54 & A3 & 6C \\ FE & 2C & 39 & 76 \\ 17 & B1 & 39 & 05 \end{bmatrix}$$

Write a Java or Python program to compute the output of the first round of AES using the input state matrix A and the subkeys K_0 and K_1. Output all intermediate steps for the computation including Initial Key Addition, SubBytes, ShiftRows, and MixColumns and Round Key Addition.