**CSB: Cryptography and Network Security**

**ASSIGNMENT-4**

Date Assigned: **19/02/2024** Date Submitted:**25/02/2024**

***Submitted By:***

Name: Himanshu Verma (**201210023), CSE**

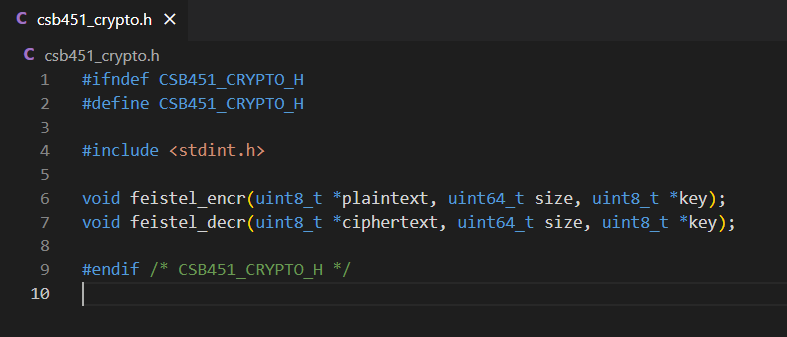
Semester: **8th Sem**

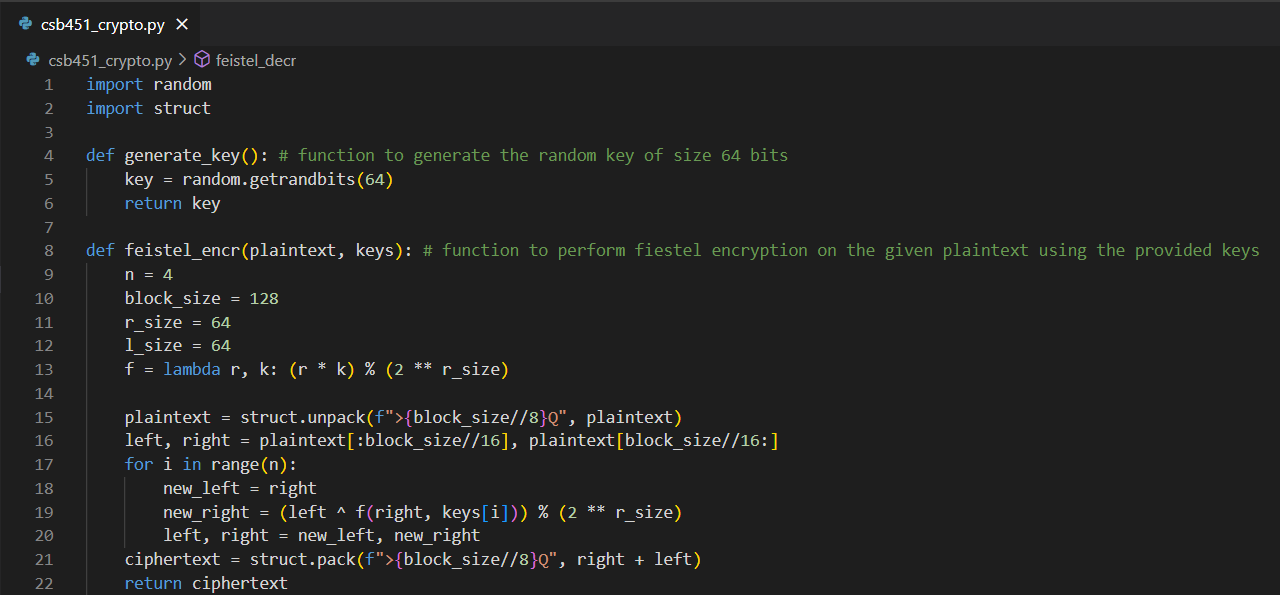
*Submitted To:* ***Dr. Karan Verma***

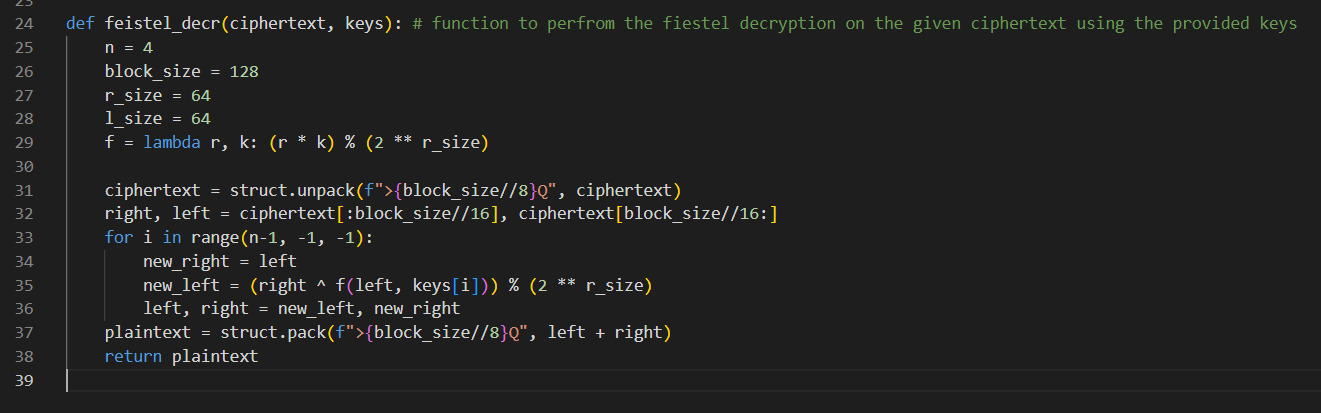
Question 1:

Code:

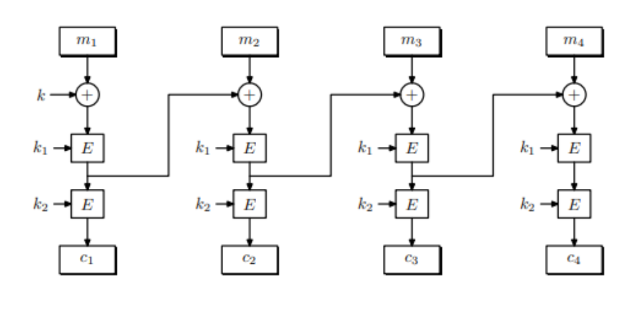
Header File:



Python Code:



Question 2:



**a.**

The decryption circuit for the system given can be defined as follows:

i. First of all take the cipher text (C1,C2)

ii.Use the key k2 to decrypt C2 to get D2

iii.Use the key k1 to decrypt D2 to get D1

iv.Use the key k to decrypt C1 to get the plaintext

**b.**

Let’s consider the two ciphertext decryption queries as mention in the hint.

•Query 1: h(C1, C2, C3, C4) with the known plaintext let’s say (P1,P2, P3, P4) where C1 = E(P1, k\_, C2 = E(P2, k), C3 = E(P3, k) and C4 = E(P4, k).

•Query 2: h(C01, C2, C03, C4) with the known plaintext let’s say (P1’, P2, P3’, P4) where C01 = C03 = E(0, k), C2 = E(P2, k) and C4 = E(P4, k) and P1’ and P3’ are random values. C01 and C03 are random ciphertext blocks.

The attacker’s goal is to recover the full key (k, k1, k2) from these queries.

Using the decryption circuit described in the first part of the question, it is seen that

i.For query 1, the attacker can obtain D2 = D(E(P4, k), k2) and D1 = D(D2, k1) and then recover the plaintext P1 = D(C1, k).

ii.For query 2, the attacker can obtain D2’ = D(C2, k2) and D1’ = D(D2’, k1) and then recover k = D(C0, P1’ XOR D1’). ( C0 is referred to both C01 and C03.)

The attacker can then combine these all results to obtain k1 and k2:

K1 = D2 XOR E(P4, k).

K1 = D(D2, D2’ XOR E(0, k)) XOR E(P2, k).

This attack takes approximately the rime it takes to run algorithm D 2^56 times, since then attacker needs to try all the possible values of k to recover it. Therefore, the attacker running time is O(2^56 time(D)), which is much faster then exhaustive search.