**IS LAB**

**Assignment 2**

**By:**

**SAARAM HUSSNAIN**

**SP24-BSE-011**

**Submitted to:**

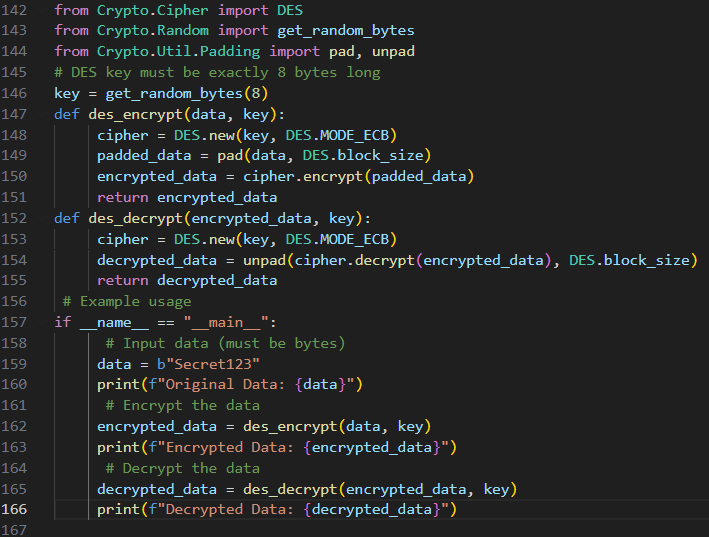
**MAM. Ambreen Gul**

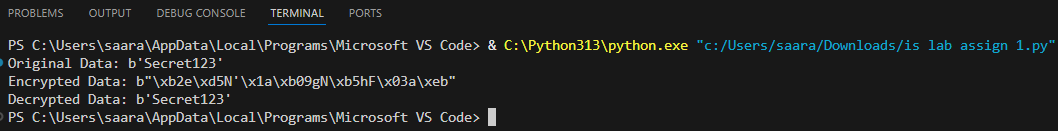
**Department of Computer Science**

COMSATS University Islamabad,

Attock Campus

**You have implemented DES there is built in implemented DES in python in crypto cipher module use it for encryption/decryption and provide output sample example**





**Visualization of MITM Attack Flow:**

Attacker intercepts plaintext (P) and ciphertext (C)

1. Guess K1

P --[Encrypt with K1]--> Intermediate Value 1 (I1)

2. Guess K2

C --[Decrypt with K2]--> Intermediate Value 2 (I2)

3. If I1 == I2, then K1 and K2 are likely correct.

Found the DES key: K = K1 + K2

**Assumptions:**

* The attacker knows or can guess some **plaintext-ciphertext pairs** (this is called a **known-plaintext attack**).
* The DES encryption and decryption processes can be divided into independent stages, allowing the attacker to perform partial encryption and decryption.

**Steps in Meet-in-the-Middle Attack:**

1. **Intercept the Ciphertext**: The attacker intercepts a **known plaintext** (i.e., a piece of the original message that is known or can be guessed) and the corresponding **ciphertext** (i.e., the encrypted version of that message).

2. **Divide the DES Algorithm into Two Stages**:

* DES operates in multiple rounds of encryption, but the MITM attack divides this into two stages:

1. **First encryption stage** (Encrypt a known plaintext).

2. **Second decryption stage** (Decrypt a known ciphertext).

The attack leverages the fact that the encryption can be split into these stages, and the intermediate value after one encryption round should match with the decrypted intermediate value after one decryption round.

3. **Guess the First Half of the Key**: The attacker guesses the first half of the key (let’s call it K1). The attacker encrypts the known plaintext using K1 and stores the result (intermediate encryption value).

4. **Guess the Second Half of the Key**: The attacker guesses the second half of the key (let’s call it K2). The attacker decrypts the intercepted ciphertext using K2 and stores the result (intermediate decryption value).

5. **Matching Intermediate Values**:

* The attacker compares the intermediate values from the first stage (encrypting with K1) and the second stage (decrypting with K2).
* If the intermediate values match, the attacker has likely found the correct combination of the two keys (K1 and K2), which together form the full DES key.
* Since DES uses a single 56-bit key, this is broken down into halves for this type of attack.