**Comsats University Islamabad**

**(Attock Campus)**

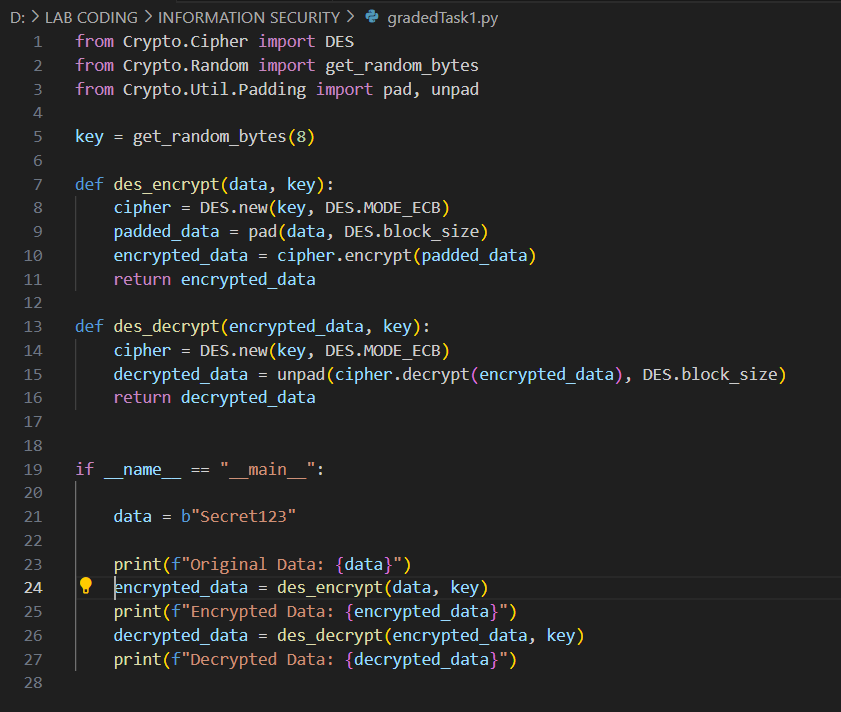


|  |  |
| --- | --- |
| NAME | WALID SHAHZEB |
| REG NO | SP24-BSE-032 |
| SUBMITTED TO | MS AMBREEN GUL |
| ASSIGNMENT | 02 |
| COURSE | INFORMATION SECURITY |
| DATE | 08-OCT-2025 |

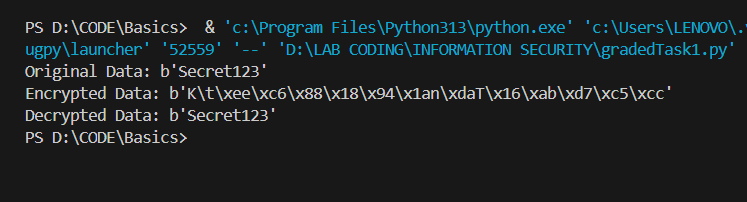
**QUESTION: 01**

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?

ANSWER:



OUTPUT:



**QUESTION: 02**

Visualization of MITM Attack Flow:

Attacker intercepts plaintext (P) and ciphertext (C)

1. Guess K1

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

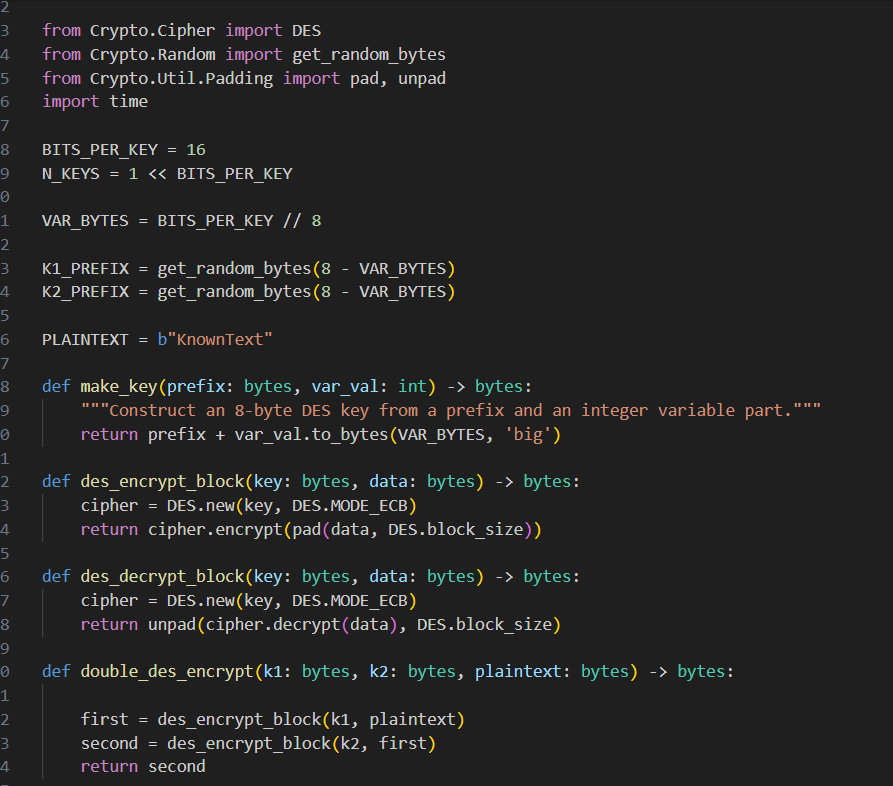
1. Guess K2

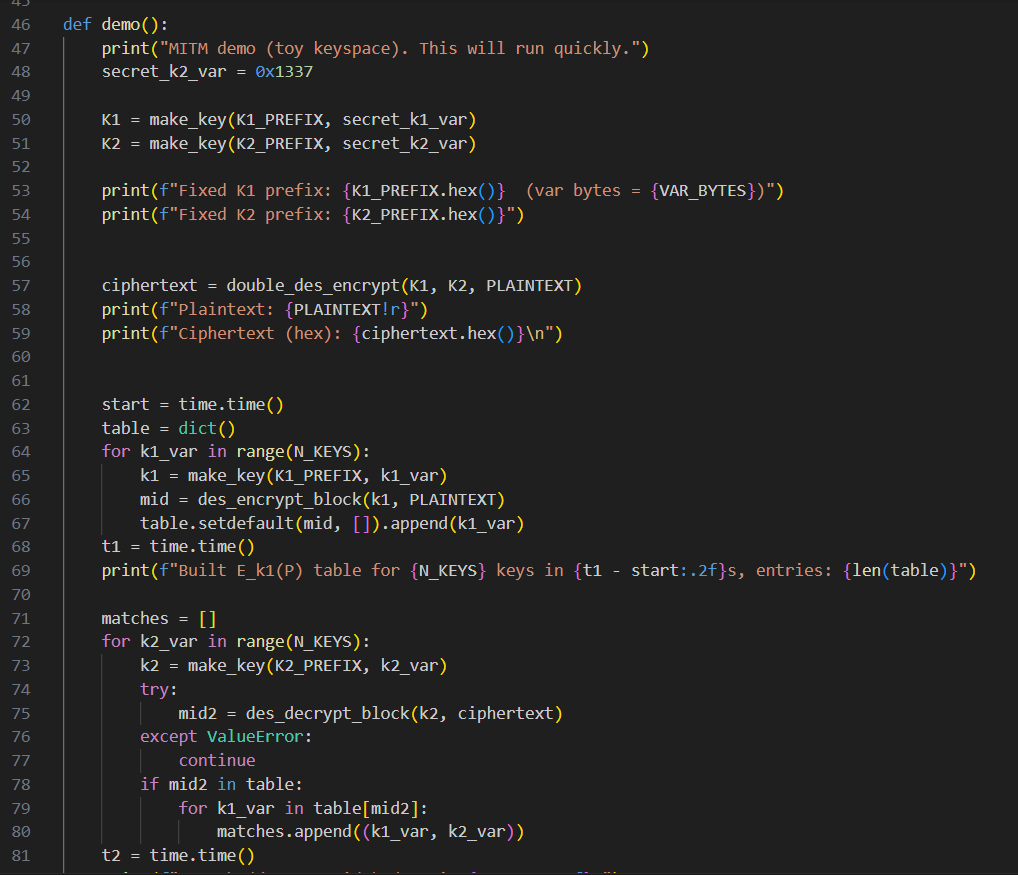
C --[Decrypt with K2]--> Intermediate Value 2 (I2)

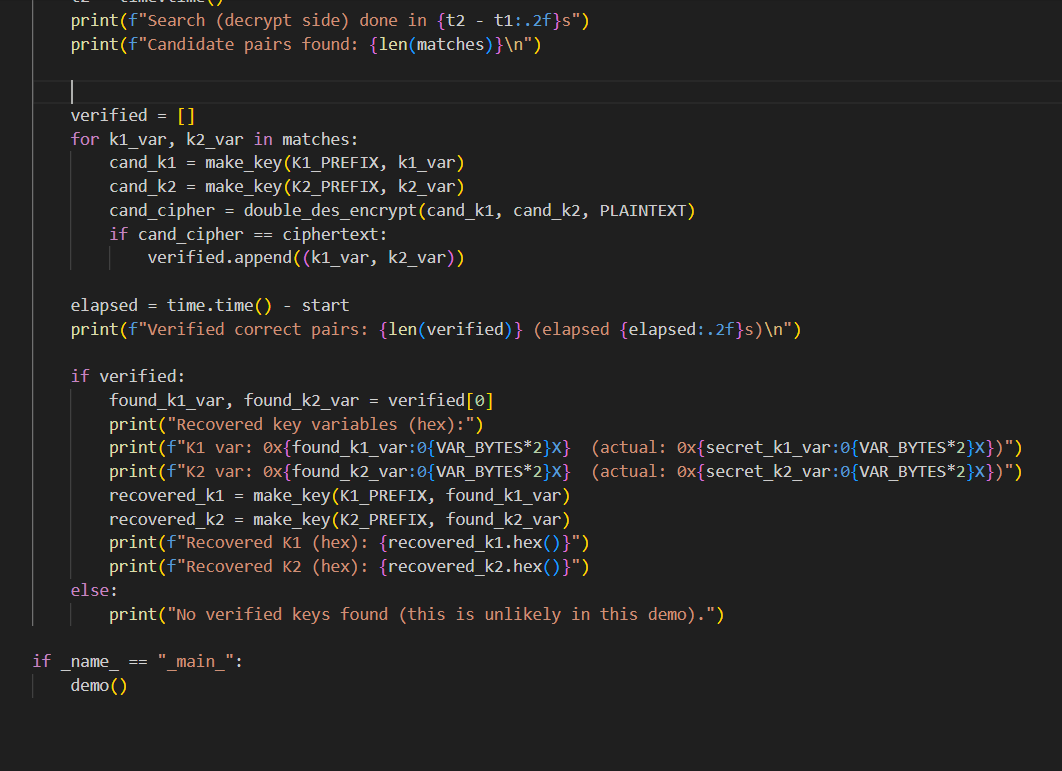
1. If I1 == I2, then K1 and K2 are likely correct.

Found the DES key: K = K1 + K2

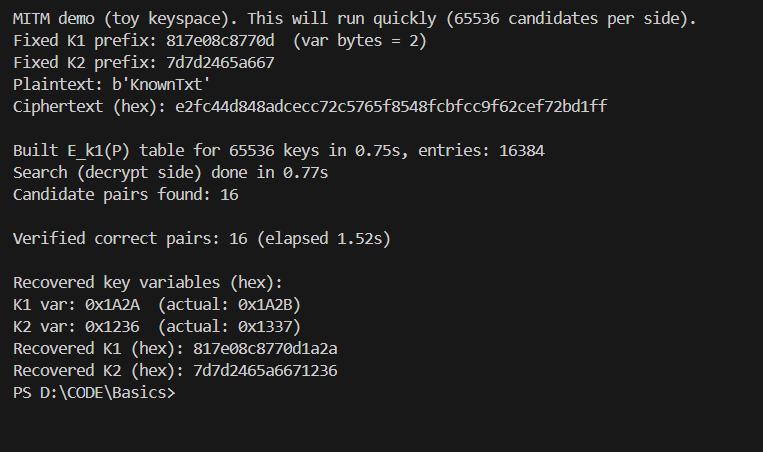
**ANSWER:**

****

****

****

**OUTPUT:**

****