**Network Security**

Assignment 2: Project **0**

**Herschelle Gupta 2019045 | Ritik Vatsal 2019321**

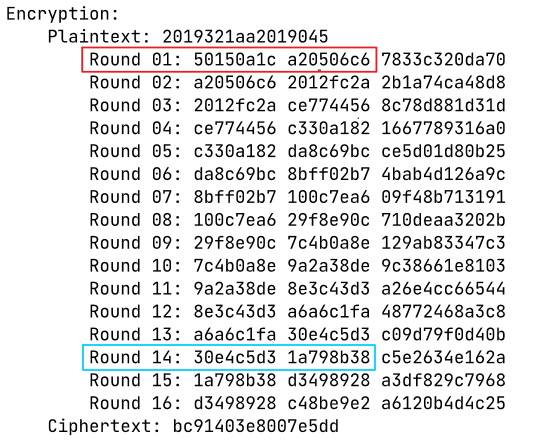
**Input**:

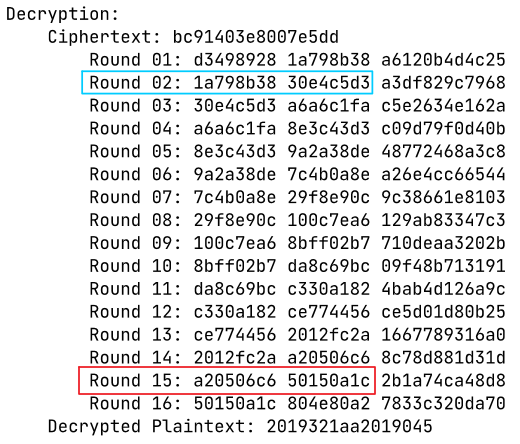
Inputs to the system are plaintext and key inside the ‘main’ function. They should be a 64-bit value in hexadecimal format.



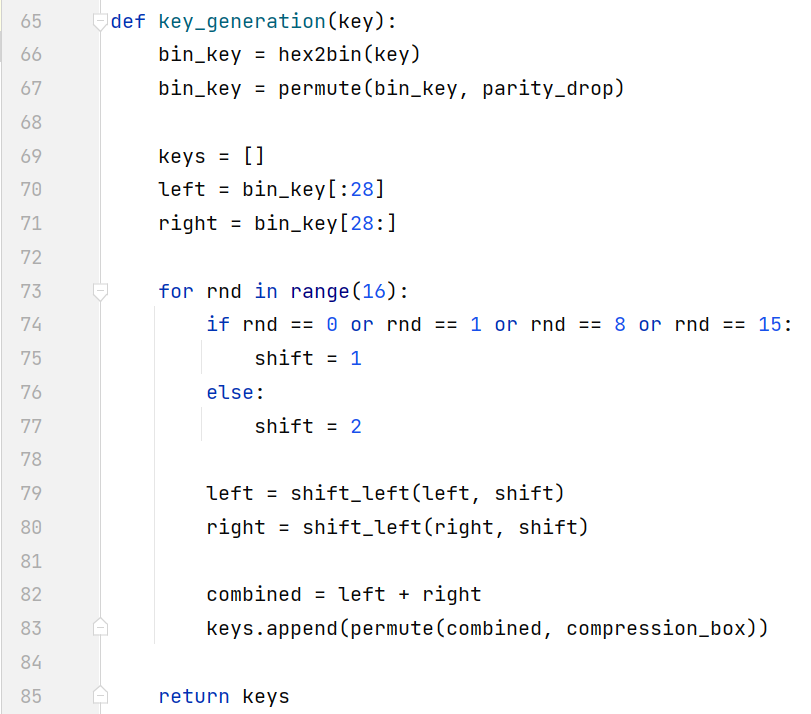
**Output:**

Upon running the code, it prints <Li, Ri, Ki> generated for all 16 rounds for both encryption and decryption in hexadecimal format.

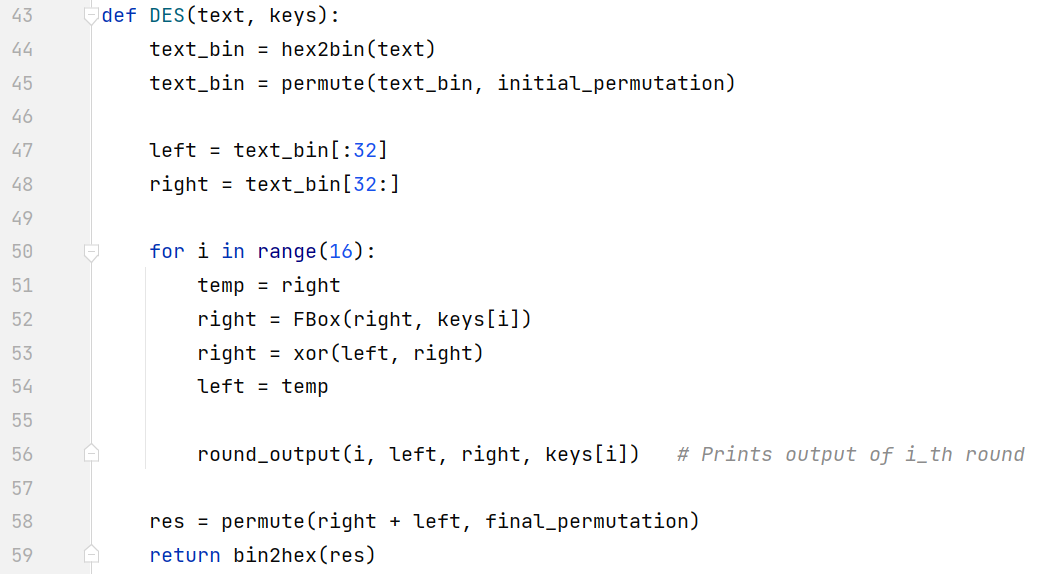




**Key Generation:**



**DES:**



**Encryption and Decryption:**

Let K = <K1, K2, … K16> and K**-1** = <K16, K15, … K1>

Encryption is the DES algorithm applied to plaintext using K, while decryption is the DES algorithm applied to ciphertext using K**-1.**