**CRYPTOGRAPHY CODING ASSIGNMENT**

**SANSKRATI JAIN**

**CSB20047**

**Assignment 3:**

Implement DES and AES.

**Solution**

Code Explanation for Encryption and Decryption in DES:

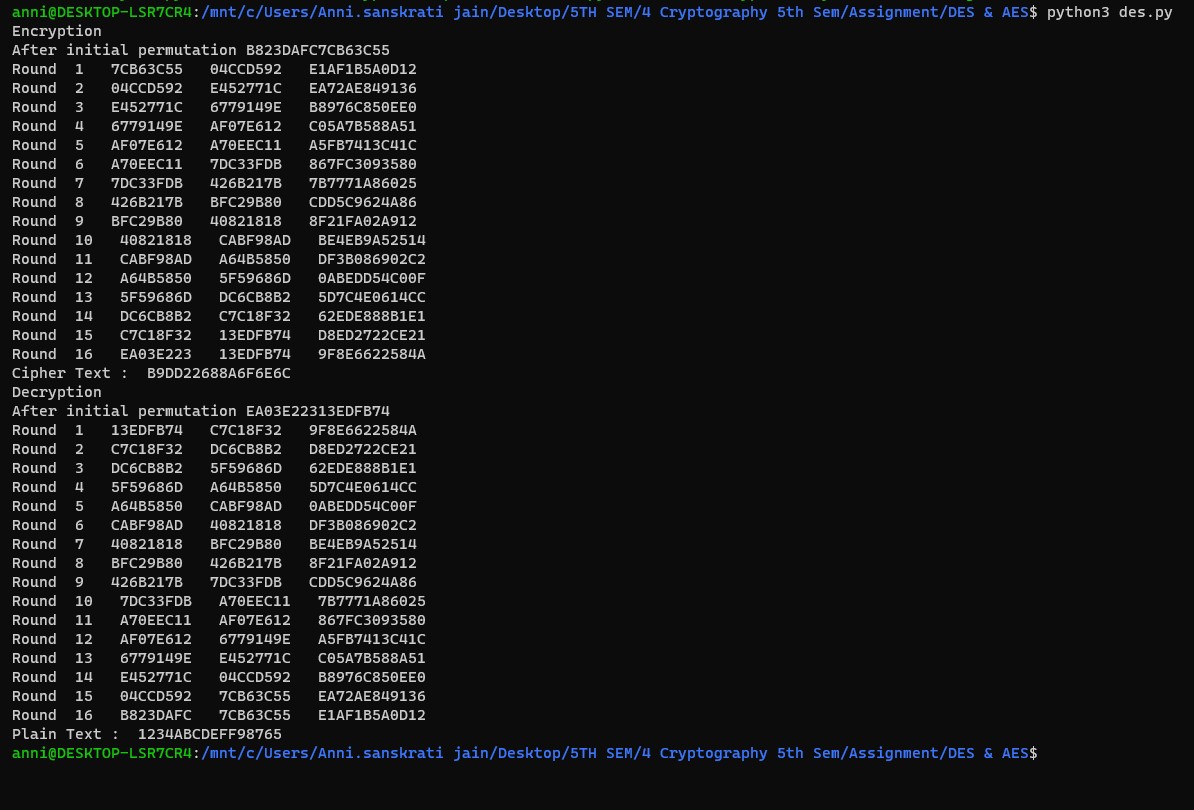
For encryption, the function takes a message and round keys as input. The message is then converted into binary. The converted binary form is passed through the permute function for initial permutation. After this, the message is split into left and right. Then, for the right part, expansion is done from 32 bits data into 48 bits using D-Box. Followed by an XOR operation and substitution using the S-box. Then rearranging of bits is done by Straight D-box. Then XOR between left and the output of substitution is done. This whole process is done 16 times as this is a 16 Fesitel network. After 16 rounds, left and right parts are combined, and the final permutation is done. The result is the cypher text.

For decryption, in the encryption function, instead of message cypher text is used, and reverse round keys are used in place of round keys.

**Code for DES:**

Attached file: des.py

**Output:**



**Code for AES:**

Attached file: aes.py

I have also attched cipher.txt that I have used for getting the following output.

**Output:**

