Network Security
Assignment 2

Reshan Faraz (PhD19006)
Koustuv Kanungo (PhD18007)

Objective :

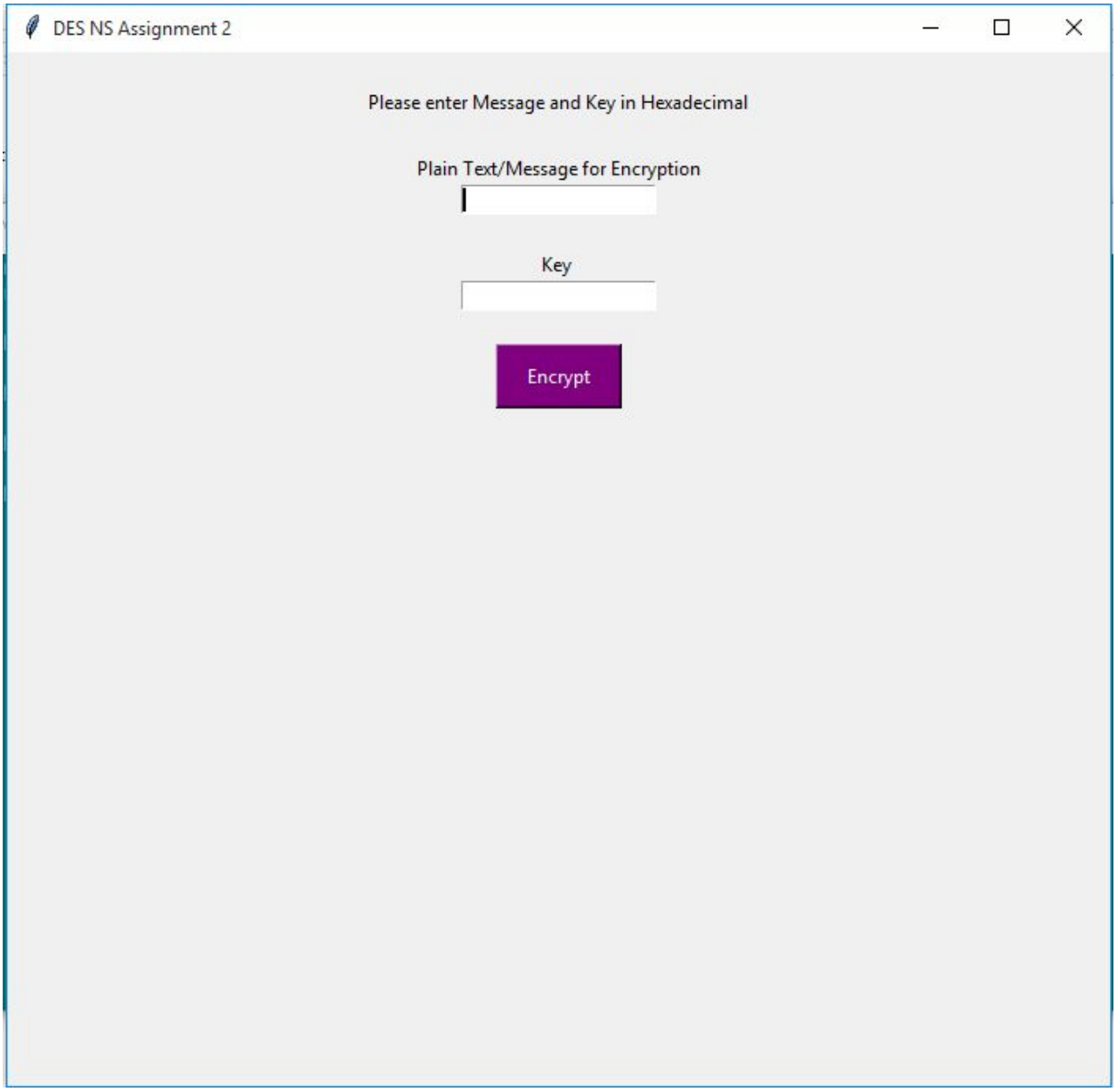
To develop and test a program to encrypt and decrypt a 64-bit plaintext using DES.
-- Verify the output of 1st encryption round to output of the 15th decryption round.
-- Verify the cipher text with the plain text.

Design of System :

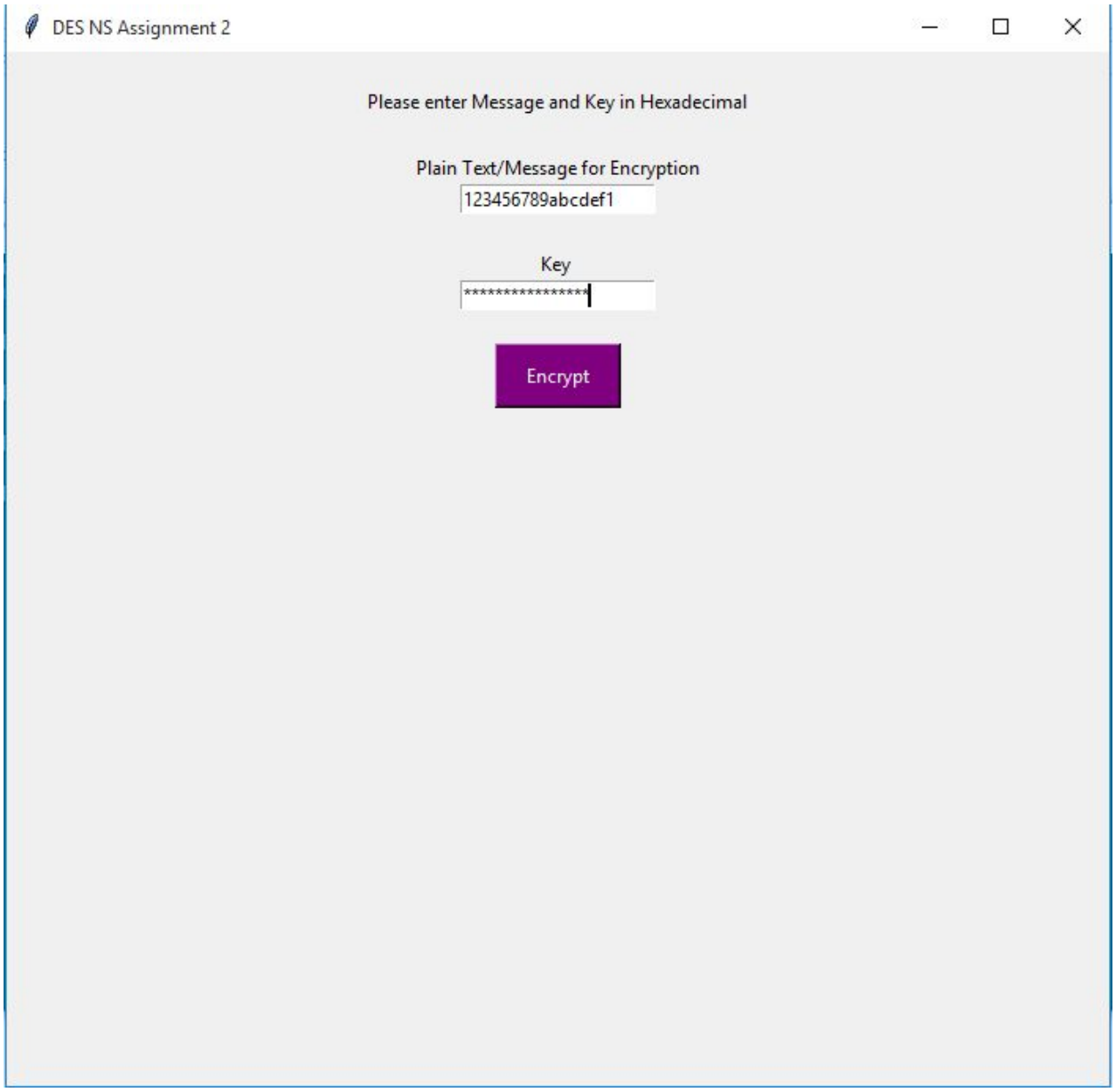
Application is Developed in python Basic UI is also provided for better visualization .
The user will input the Message/Plain Text and key in hexadecimal and then click on Encrypt button then on the next window the Cipher text will be seen along with Plain text which was obtained by decrypting the cipher text.
For the second part of the solution I also show the output of the 1st round of Encryption to the output of the 15th round of the Decryption, which is equal.

The Code will contain the encrypt,decrypt ,key generation function for the implementation of DES.
Library used :
Bitvector : converting hexadecimal to binary
Tkinter : For basic UI

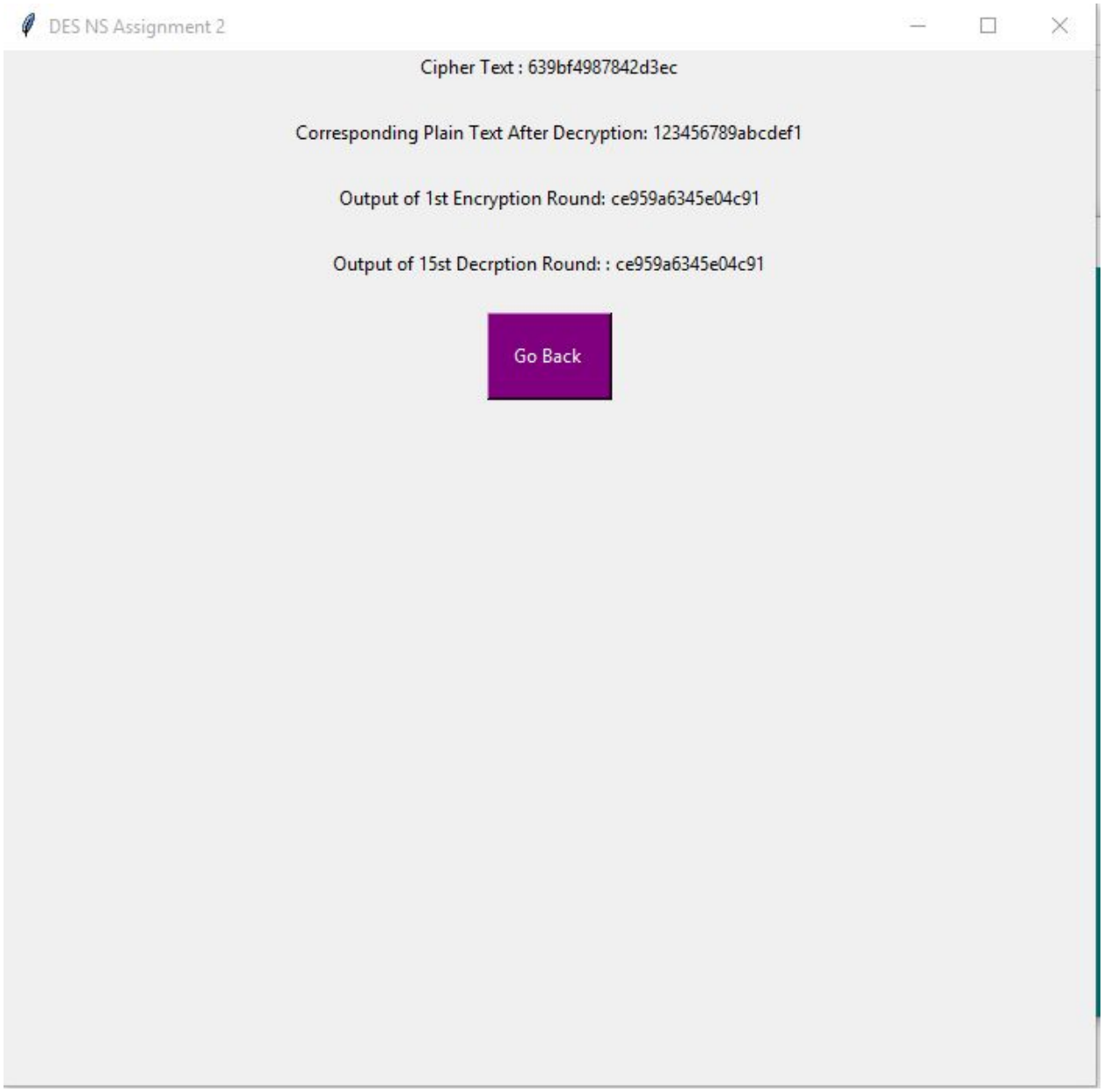
Following are the snapshot from the Application



Entering the Key and Plain Text:



Final Result :


DES NS Assignment 2
Cipher Text : 639bf4987842d3ec
Corresponding Plain Text After Decryption: 123456789abcdef1
Output of 1st Encryption Round: ce959a6345e04c91
Output of 15st Decrption Round: : ce959a6345e04c91
Go Back