Sri Lanka Institute of Information Technology

Introduction to Cyber Security - IE2022

Lab Submission 07

IT22151056

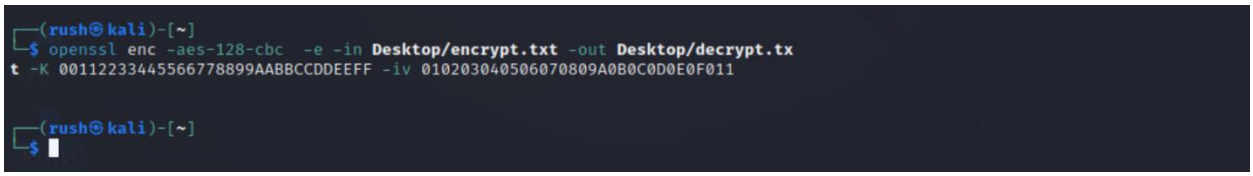
De Silva K.R.K.D

Group – WD.CS 01.02

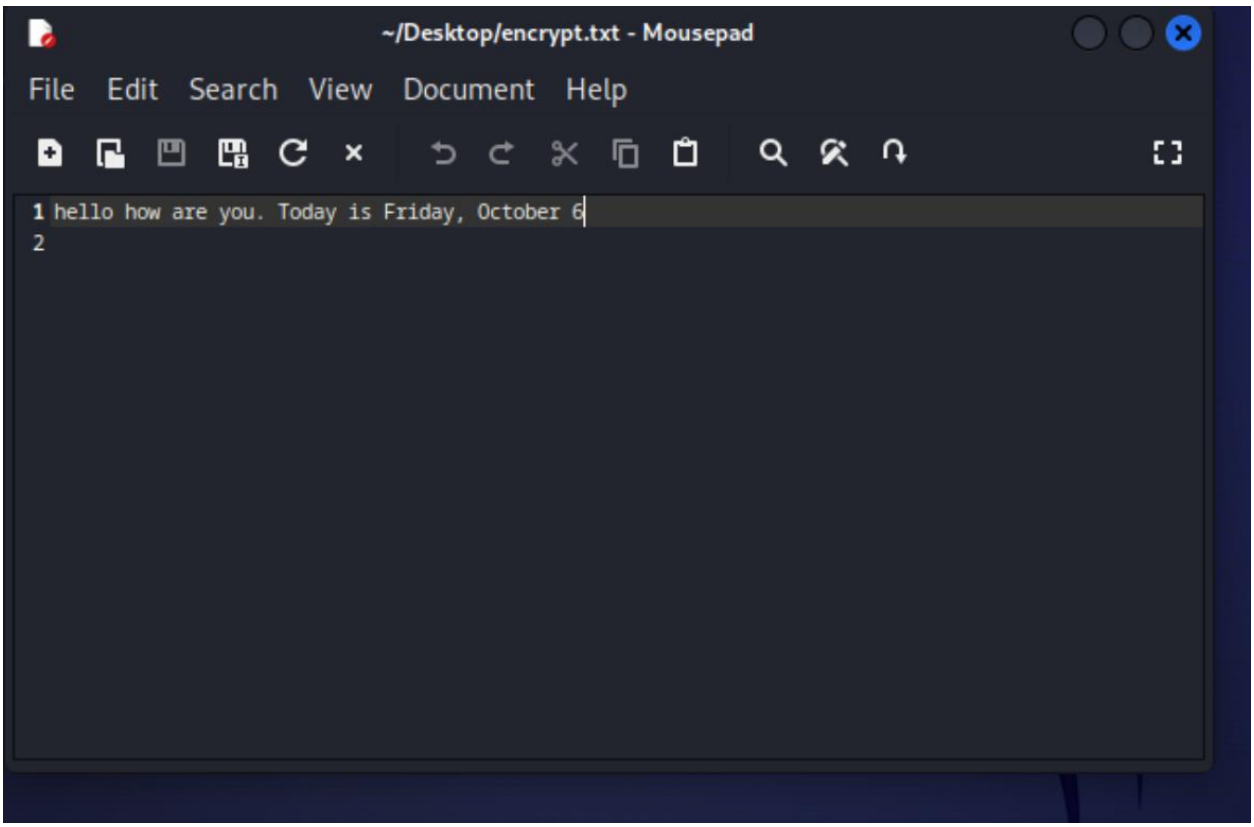
Task 01

encryption and Decryption using different ciphers and modes

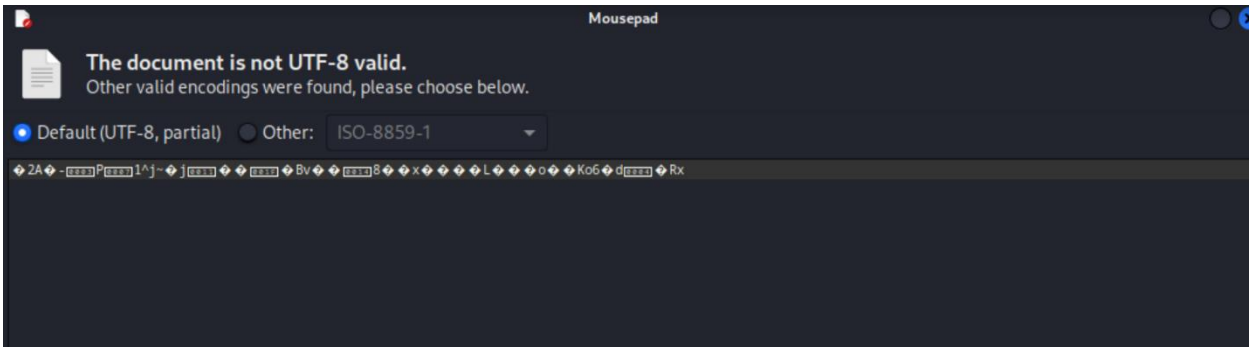
1.Encrypt using cbc mode.



Plaintext file



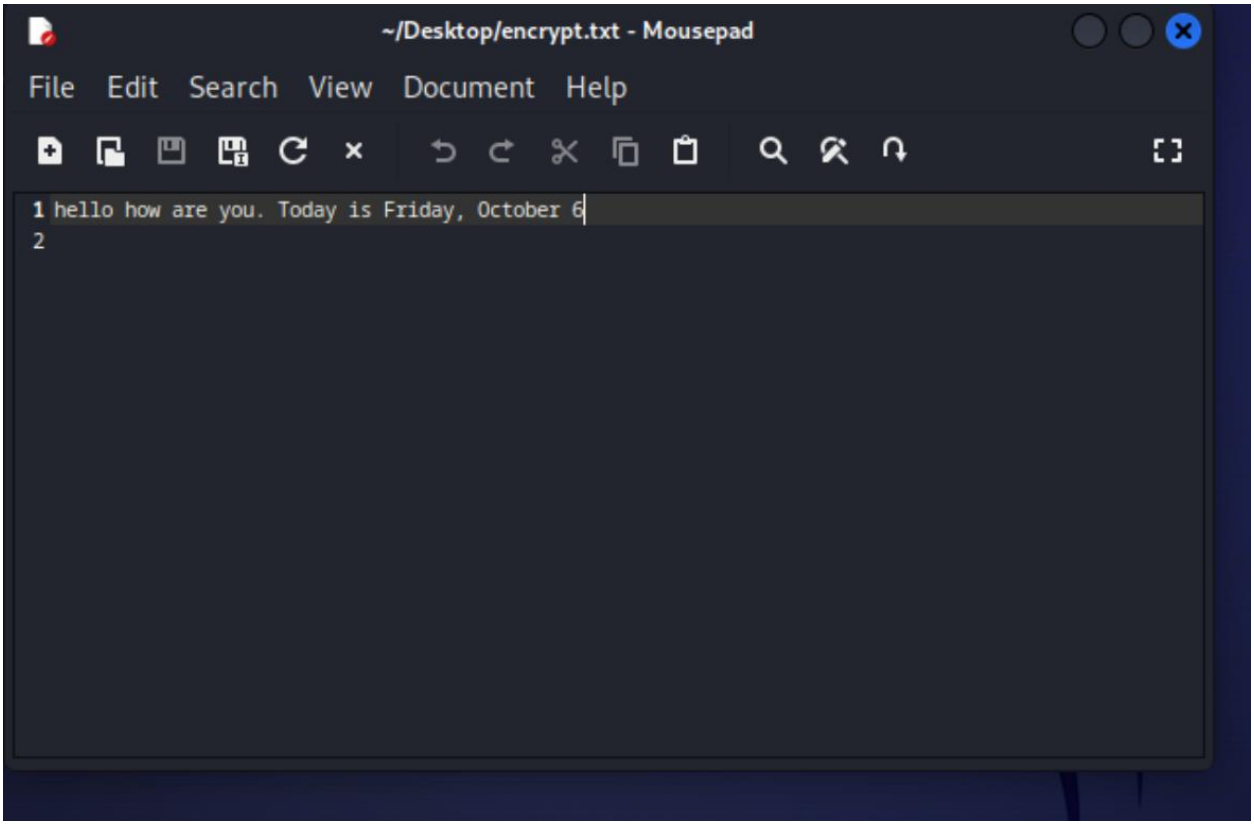
Decrypted file



2.Encrypt using CFB mode

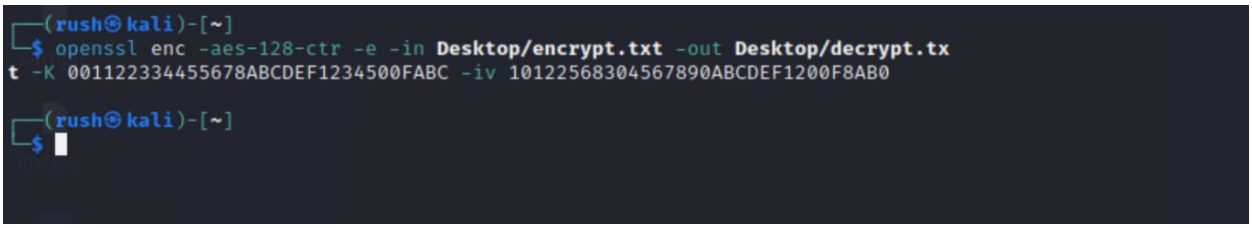
```
┌──(rush㉿kali)-[~]
└─$ openssl enc -aes-128-cfb -e -in Desktop/encrypt.txt -out Desktop/decrypt.txt -K 001122334455678ABCDEF1234500FABC -iv 10122
568304567890ABCDEF1200F8AB0
```

Plaintext file

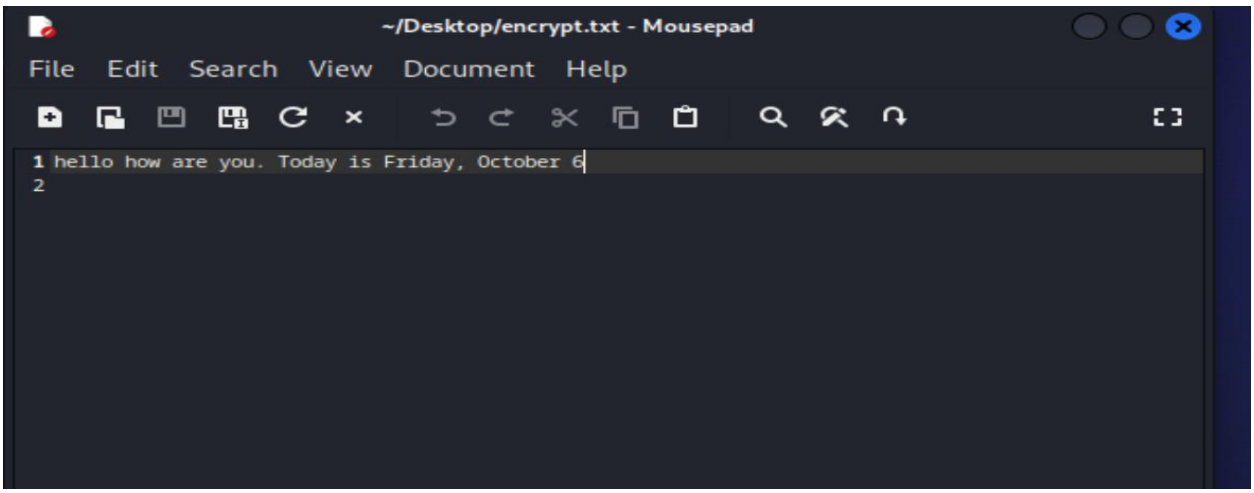


Encrypted File

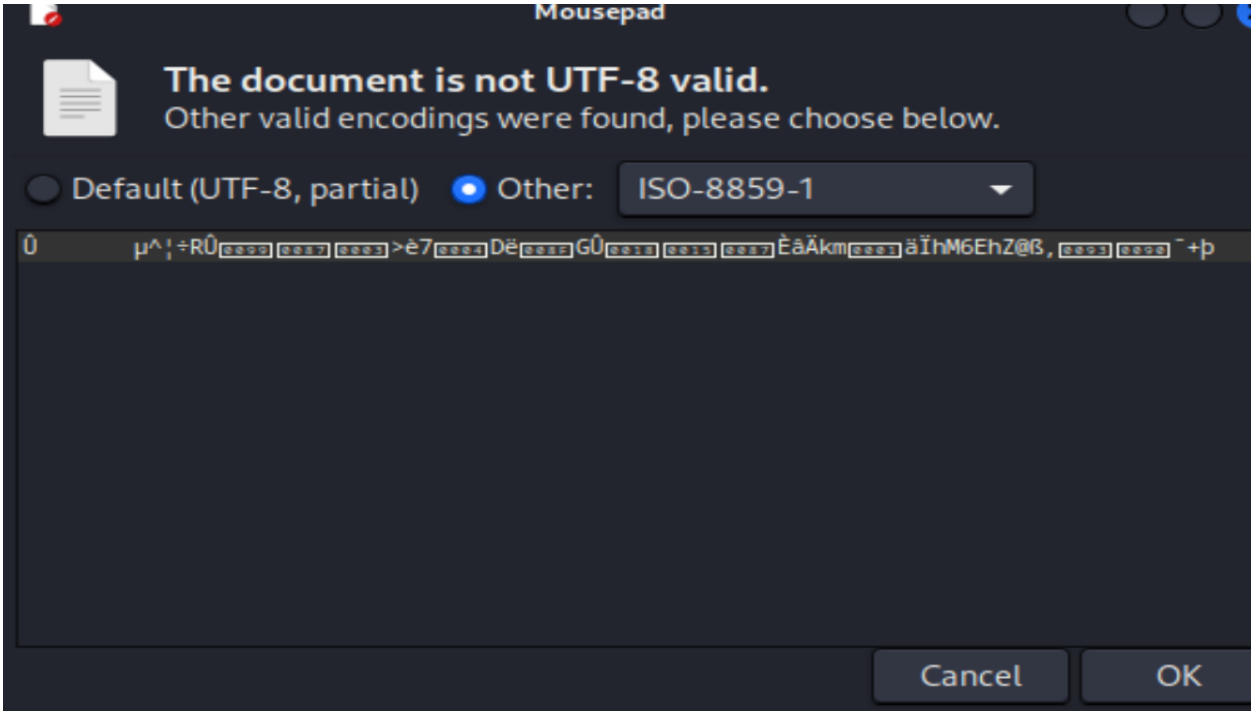
3.Encrypted Using CTR mode



Plaintext file



Encrypted File



Here, when different modes are used, even if the same key and iv value are used, different decryption values are obtained.