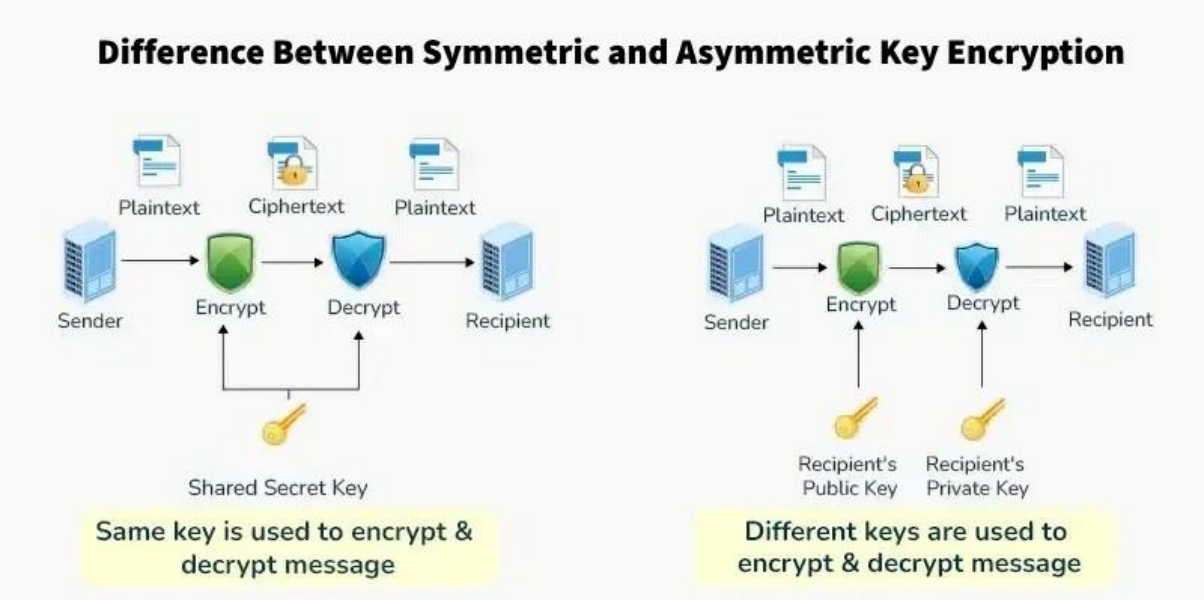
TASK 6

ENCRYPTION:

Encryption is the most common basic concept of cryptography, to protecting the integrity of the information from wrong hands. There are two types of techniques in encryption they are,

- ❖ Symmetric encryption
- ❖ Asymmetric encryption



SYMMETRIC ENCRYPTION:

In this type of encryption same key will be used for the both encryption and decryption the information. It also requires a secure method to transfer the key between them, it fast but less secure.

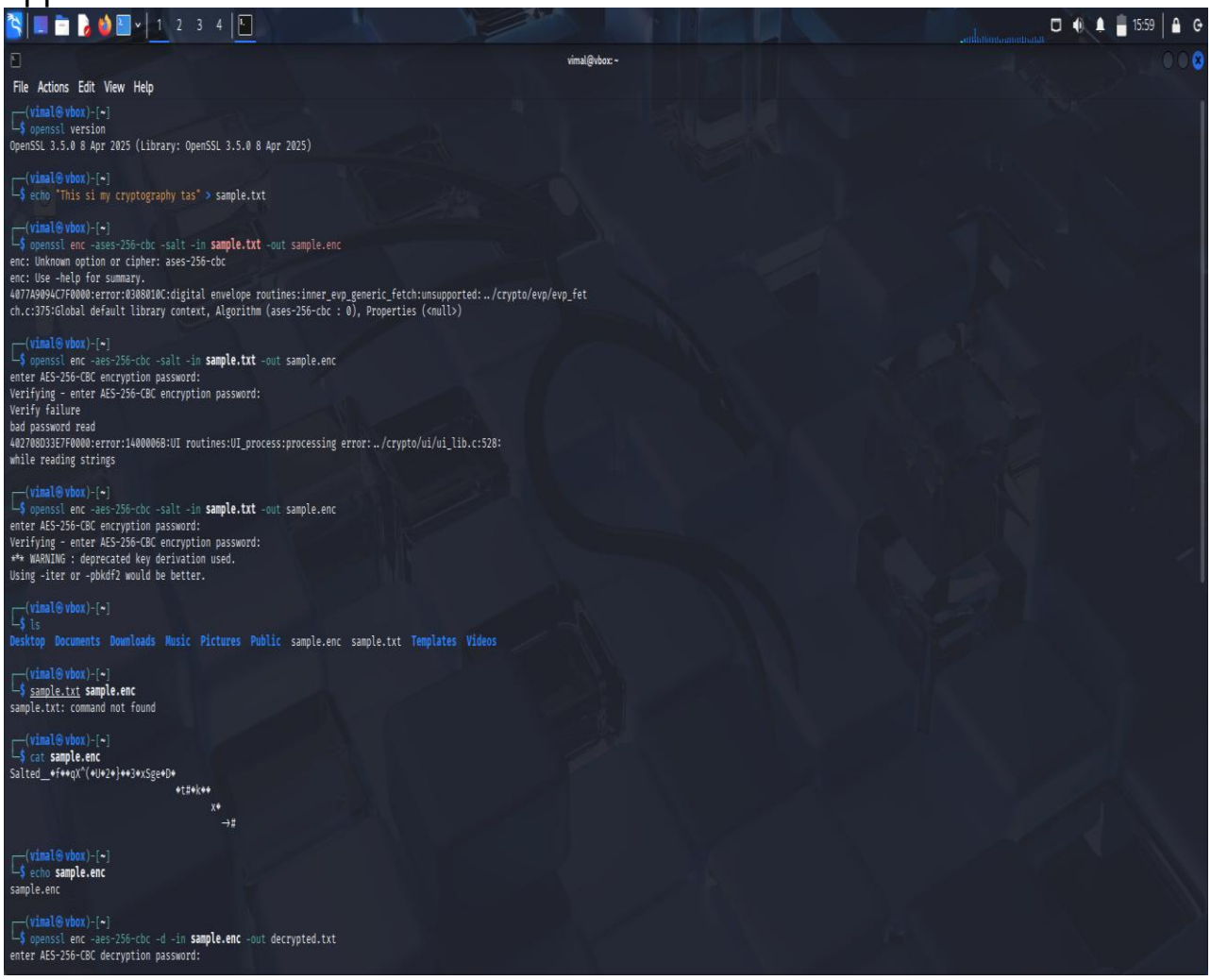
- It uses one key for both encryption and decryption.
- Faster and more efficient for large amounts of data.
- Requires a secure method to share the key between sender and receiver.
- Common algorithms include AES, DES, Blowfish.
- It is used in file encryption, VPNs, and secure data storage.

ASYMMETRIC ENCRYPTION:

Asymmetric encryption is the most common cryptographic encryption, here one key is used to encrypted the message and it is pendent and it will be share among the users called public key. Another key is used decrypt the message and it is called private key.

- It uses two keys a public key for encryption and a private key for decryption.
- More secure but slower than symmetric encryption.
- No need to share the private key, reducing the risk of exposure.
- Common algorithms include RSA, ECC, Diffie-Hellman.
- It is used in digital signatures, SSL/TLS, and secure email communication.

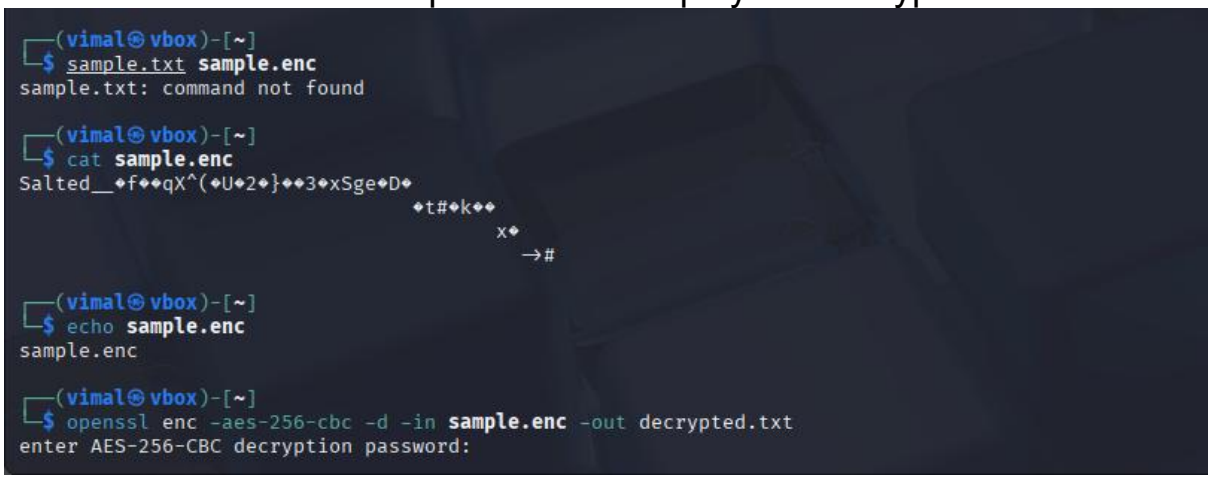
I have done this encryption and decryption process with openssl application:



I done the AES encryption decryption with the text "**this is cryptography text**" using the commands:
openssl enc -aes-256-cbc -salt -in sample.txt -out sample.enc

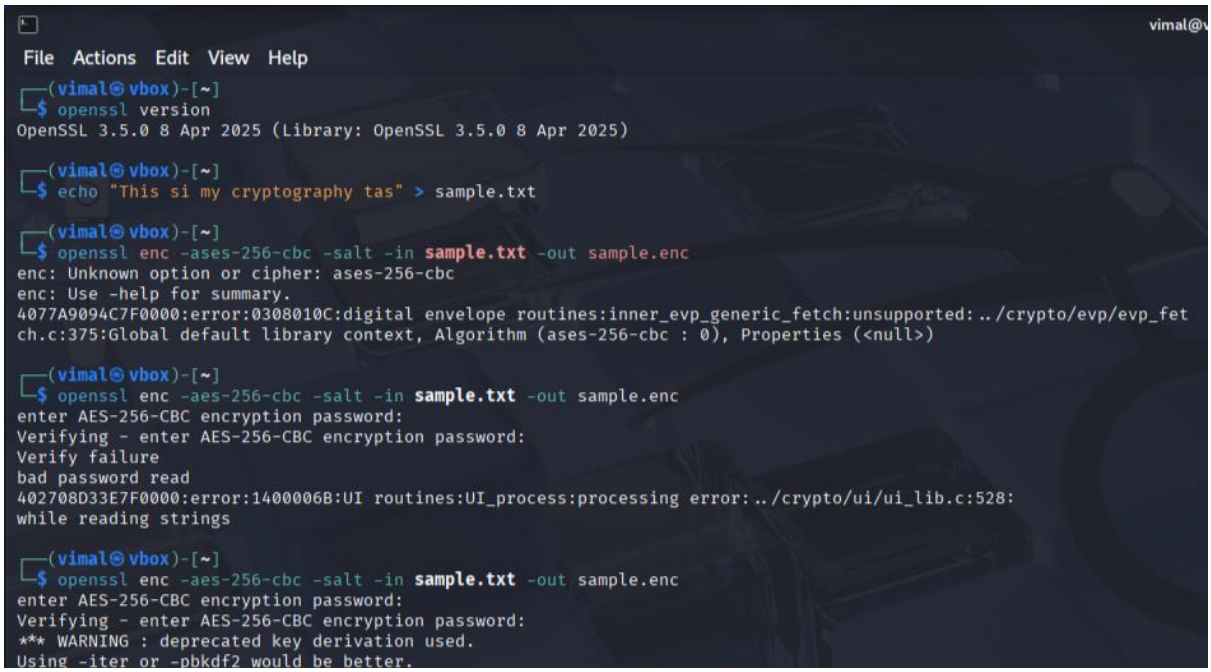
- openssl enc -It kick off the application
- aes-256 - Advance Encryption system 256 bits
- cbc -cipher block chain mode
- salt -random text to manipulate the cipher
- in sample.txt -file

CRYPER TEXT : cat sample.enc – to display the encrypted file



DECRYPTION THE TEXT - openssl enc -aes-256-cbc -d -in sample.enc -out decrypted.txt

- d -in :decrypt
- out decrypted.txt: output file



Final result after the decryption: