In this lab, I will use OpenSSL to encrypt files using the AES (Advanced Encryption Standard) symmetric encryption algorithm and decrypt them back to their original form.

Beginning with creating a basic test file for encryption using the echo command: echo "This is a sample file for AES encryption lab." > test_file.txt:

- Echo: outputs line of text
- '>' outputs that line of text into testfile.txt

I then use generate a random 256 bit (32 byte) key for AES encryption: openssl rand -base64 32 > aes_key.bin

- openssl rand: uses openssl random data generation
- base64: tag to generate random data into base 64 format
- 32: specifies 32 bytes

I then use the following command to encrypt the file using the created key: openssl enc -aes-256-cbc -salt -in test_file.txt -out encrypted_file.bin -pass file:aes_key.bin -iter 100000

- Openssl enc: uses openssl symmetric encryption capability
- aes-256-cbc: specifies the encryption algorithm AES with 256 bit key in Cipher Block Chaining mode.
- -salt: adds a random salt into the encryption to increase security
- -in test file.txt: the file being encrypted
- out encrypted_file.bin: where the output encrypted file is saved
- -pass file:aes_key.bin: the key being used
- -iter 100000: the amount of iterations for the key derivative function, increasing processing power to crack.

Using the cat command on the original and encrypted file shows a successful AES encryption.

Now I will decrypt the by using the following command:

openssl enc -d -aes-256-cbc -salt -in encrypted_file.bin -out decrypted_file.txt -pass file:aes_key.bin -iter 100000

Noticeable changes:

- -d: specifies decryption
- Swapped "-in test_file.txt" with "-in encrypted_file.bin" to specify file being decrypted
- Output changed to decrypted_file.txt

Now when I cat all the created files we can see the results :

```
theia@theia-bradleyrroff:/home/project$ openssl enc -d -aes-256-cbc -salt -in encrypted_file.bin -out decryp
ted_file.txt -pass file:aes_key.bin -iter 100000
theia@theia-bradleyrroff:/home/project$ ls
aes_key.bin decrypted_file.txt encrypted_file.bin test_file.txt
theia@theia-bradleyrroff:/home/project$ cat decrypted_file.txt
This is a sample file for AES encryption lab.
theia@theia-bradleyrroff:/home/project$ cat test_file.txt
This is a sample file for AES encryption lab.
theia@theia-bradleyrroff:/home/project$ cat encrypted_file.bin
Salted__f^@@@@@@@@@@@@@@@@@@@@.{\theia@theia-bradleyrroff:/home/project$}
@@ZZ<@@@@@@#G@n=@@@@@@@@@@.{\theia@theia-bradleyrroff:/home/project$}
```