**AMRUTHESH**

**241059041**

**CRYPTOLOGY**

**M.E – CYBER SECURITY**

**Introduction**

**openssl** is a powerful command-line tool used for various cryptographic operations, including key generation, encryption, and decryption. Below are examples of common **openssl** commands for generating keys and encrypting data.

**1. Generating RSA Keys**

**Generate a Private Key:** openssl genpkey -algorithm RSA -out private\_key.pem -aes256

* This command generates a private RSA key and saves it in private\_key.pem, using AES-256 encryption to secure the key.

**Generate a Public Key from the Private Key:**

openssl rsa -pubout -in private\_key.pem -out public\_key.pem

* This command extracts the public key from the private key and saves it in public\_key.pem.

**2. Encrypting Data with RSA**

**Encrypt a File:**

openssl rsautl -encrypt -inkey public\_key.pem -pubin -in plaintext.txt -out encrypted.dat

* This command encrypts the file plaintext.txt using the public key and saves the encrypted data in encrypted.dat.

**3. Decrypting Data with RSA**

**Decrypt the Encrypted File:**

openssl rsautl -decrypt -inkey private\_key.pem -in encrypted.dat -out decrypted.txt

* This command decrypts the file encrypted.dat using the private key and saves the decrypted data in decrypted.txt.

**4. Generating a Symmetric Key**

**Generate an AES-256 Key:** openssl rand -out aes\_key.bin 32

* This command generates a 256-bit AES key and saves it in aes\_key.bin.

**5. Encrypting Data with AES**

**Encrypt a File:**

openssl enc -aes-256-cbc -salt -in plaintext.txt -out encrypted\_aes.dat -pass file:aes\_key.bin

* This command encrypts the file plaintext.txt using AES-256 in CBC mode and the key from aes\_key.bin. The encrypted data is saved in encrypted\_aes.dat.

**6. Decrypting Data with AES**

**Decrypt the Encrypted File:**

openssl enc -aes-256-cbc -d -in encrypted\_aes.dat -out decrypted\_aes.txt -pass file:aes\_key.bin

* This command decrypts the file encrypted\_aes.dat using AES-256 and the key from aes\_key.bin, saving the decrypted data in decrypted\_aes.txt.

**Conclusion**

The openssl tool provides a wide range of functionalities for cryptographic operations. Mastering these commands is essential for managing keys and performing encryption and decryption tasks effectively.