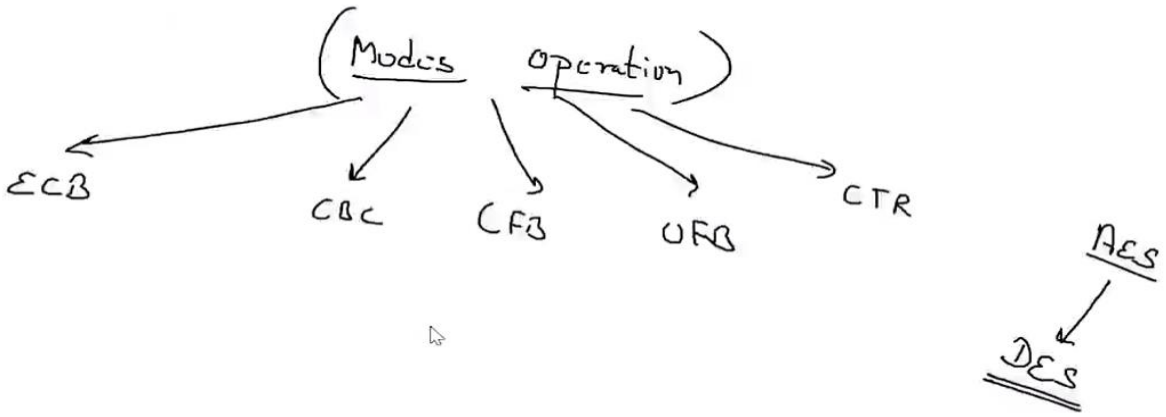
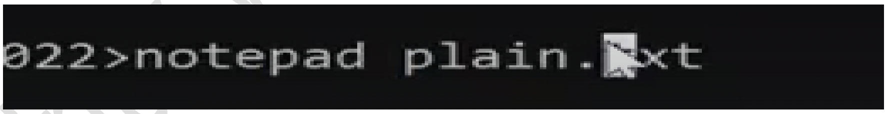
Cryptography Session No.3

Summary 21-07-2022

- In Symmetric Encryption, we have multiple block modes such that
  - ECB
  - CBC
  - CFB
  - OFB
  - CTR

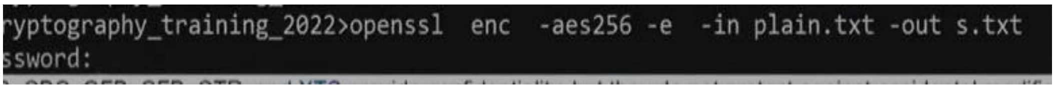


- **#openssl enc -ciphers** -> It will show all encryption ciphers available in your OpenSSL
- Create a **plain.txt** file and put some data here, Which we will try to encrypt with our further algorithms.



```
022>notepad plain.txt
```

- **#openssl enc -aes256 -e -in plain.txt -out secure.txt** -> Now when we run this command it will encrypt our plain.txt data with the help of the aes256 algorithm by generating a random Key, And before that, it will ask for a password.



```
ryptography_training_2022>openssl  enc  -aes256 -e  -in plain.txt -out s.txt
ssword:
```

NOTE- This password will not encrypt our data, This password is just to secure the random key(substitution table), with which our data is been secured.

- While running the above command each time a random key(key is like a table used for substitution) will be generated by the AES algorithm
- **#Openssl enc -aes256 -d -in secure.txt** -> Now before decrypting it will ask for a password, if the password matches the password you created at the time of encryption, Then only the key that was used at the time of encryption will be open, and with the use of that, data will be decrypted.
- **#Openssl aes-256-cbc -p** -> This command will show us here what random key, It has chosen, It has generated a 256-bit key
- We have one more algorithm for encryption like **DES**, This algorithm was broken in the past, So normally we don't use this algorithm for encryption,

  #openssl des -p -> Here we can see it has also generated a random key but its size is 56bits, So if anyone wants to do a brute-force attack to decrypt data that was encrypted by the DES algorithm, Then it can be decrypted after choosing 2^56 combinations in the worst case.
- As big as the key size is that much secure data is.
- To encrypt data with your own given key

  #openssl enc -aes128 -e -in plain.txt-out c.txt -K 123ABC -iv aaaaaa
- Now to decrypt the same data->**# openssl enc -aes128 -d -in c.txt -K 123ABC -iv aaaaaa** -> Now this will decrypt our data without asking for the password we have given at the time of encryption, It proves that the Password is just to secure the key, Here as we remember the key, so we don't need to provide any password
- The AES128 algorithm is used almost everywhere in the market even in banks, because it is secure, and to decrypt it, a 2^128 combinations hacker will have to check which is an impossible task as of now.
- AES is one of the top Symmetric encryption algorithms
- Transposition Cipher- A transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system so that the ciphertext constitutes a permutation of the plaintext.
- Shift Cipher - A shift cipher involves replacing each letter in the message with a letter that is some fixed number of positions further along in the alphabet. We'll call this number the encryption key. It

is just the length of the shift we are using.

- Now If we have a big file to encrypt then our algorithms will pick the data from the file in some blocks and in those small chunks it will encrypt the complete file, It saves the memory as well In this way we have the option to parallel computing
- DES algorithm uses the block size of 64 bits hence from the plain.txt file at one time it will pick the first 64-bit data
- AES algorithm block size is 128 bits
- The smaller the block size, more the time it will take to encrypt the complete data
- ECB mode(Electronic Codebook) - Here it will encrypt the same data with the same substitution value
  For eg. Data- “Hello How are you Hello WhatsUp! “
  Now to understand the concept imagine all the words in the above sentence are one block(have to say 64-bit size), Now as Hello is used two times in the sentence so to encrypt the complete sentence, With the same value, both Hello will be encrypted. Now this has a big problem If we have an image/video to encrypt then using ECB mode, it will just change the color of the image throughout, but still, anyone can easily guess the image, so it is not encrypting as such here
- One good thing in ECB, i.e. parallel computing, We can encrypt multiple blocks parallelly with this algorithm.
- **#openssl aes-256-ecb -p -** Here we can see we have the Key and salt, No initialization vector is there.