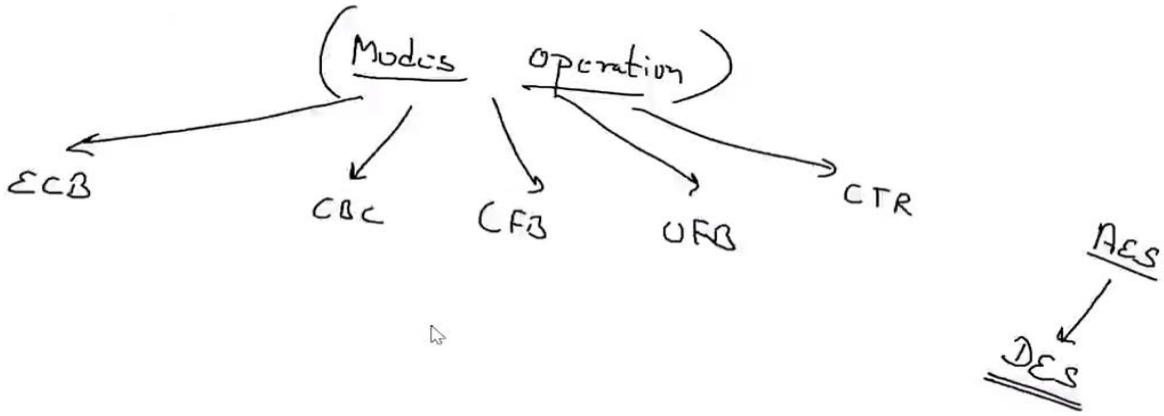
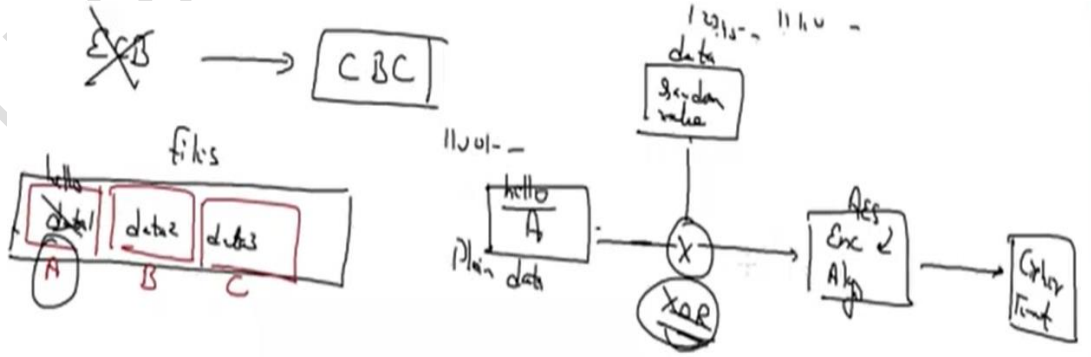
Cryptography Session No.4

Summary 21-07-2022

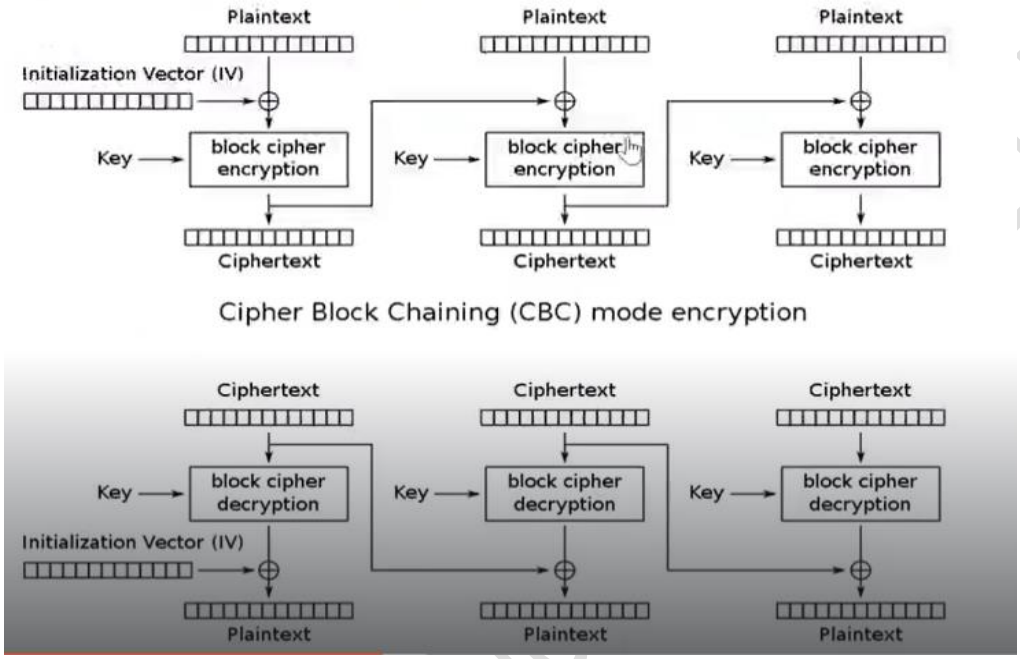
- In Symmetric Encryption, we have multiple block modes such that
  - ECB
  - CBC
  - CFB
  - OFB
  - CTR



- In CBC(Cipher Block Chaining) mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted this way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.



- CBC(Cipher Block Chaining)- It is the commonly used algorithm mode here we add some random Initialization vector(iv) with our plain data and then it will be encrypted, Hence Which makes this algorithm more secure, Now with this algorithm, we can encrypt our images/videos. And it would completely be changed after encryption, No one can guess the original image.



- **#openssl aes-256-cbc -p -** Her we can see, We have Key, Initialization vector and salt.

- You can get more details about Symmetric Encryption blocks here -

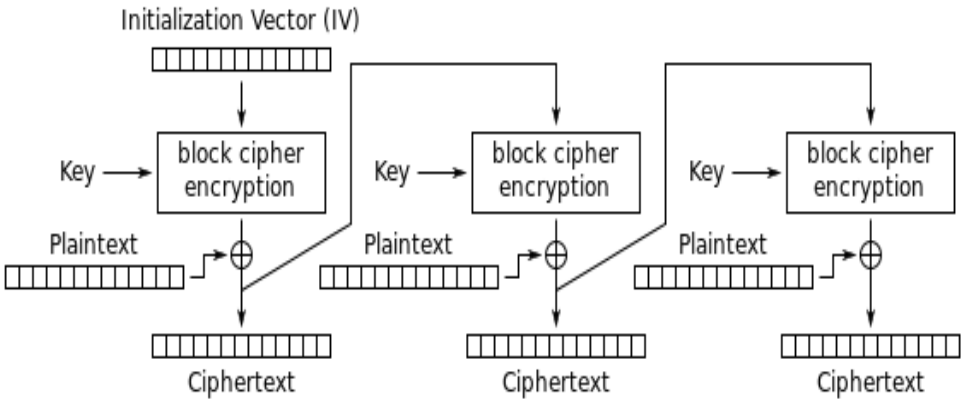
https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#:~:text=Electronic%20codebook%20(ECB),-ECB&text=The%20message%20is%20divided%20into,not%20hide%20data%20patterns%20well

- Check out the difference in image encryption of CBC and ECB – https://pthree.org/2012/02/17/ecb-vs-cbc-encryption/

- CFB mode performs cipher feedback encryption. CFB mode operates on segments instead of blocks. The segment length (called s) is between one bit and the block size (called b) for the underlying algorithm (DES or AES), inclusive. ICSF only allows segment sizes which are a multiple of eight bits (complete bytes).

- CFB is used in encryption algorithms such as Data Encryption Standard (DES), Triple DES and Advanced Encryption Standard (AES). If CFB mode is used within the encryption algorithm, it's often used to encrypt the following services: Wi-Fi communications. secure websites.

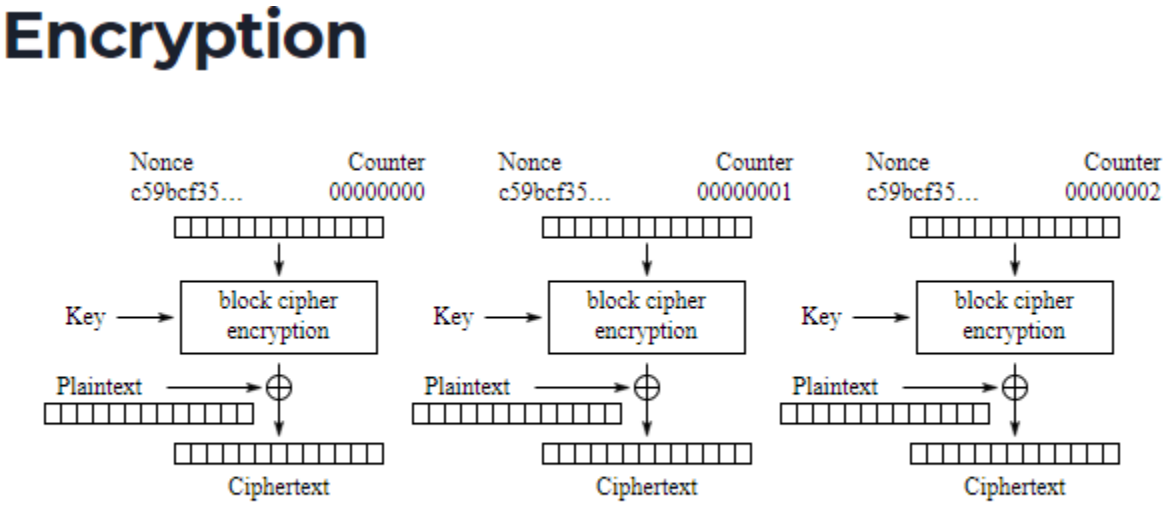
- difference between CBC and CFB mode?
  Cipher Feedback (CFB) mode is very similar to CBC; the primary difference is that CFB is a stream mode. It uses feedback (the name for chaining when used in stream modes) to destroy patterns. Like CBC, CFB uses an initialization vector that destroys patterns and errors propagate.



Cipher Feedback (CFB) mode encryption

- Hardware security modules (HSMs) are hardened, tamper-resistant hardware devices that secure cryptographic processes by generating, protecting, and managing keys used for encrypting and decrypting data and creating digital signatures and certificates.
- An HSM (Hardware Security Module) is a highly secure hardware-based solution for key management and cryptographic processing. Typical applications include PKI, digital signing, encryption key management, and securing of payment transactions.

- CTR (short for counter) is a popular AES block cipher mode in which every step can be done in parallel. CTR is similar to OFB as it also involves XOR-ing a sequence of pad vectors with the plaintext and ciphertext blocks. The main difference lies in how these pad vectors are generated.



Counter (CTR) mode encryption