Date Day

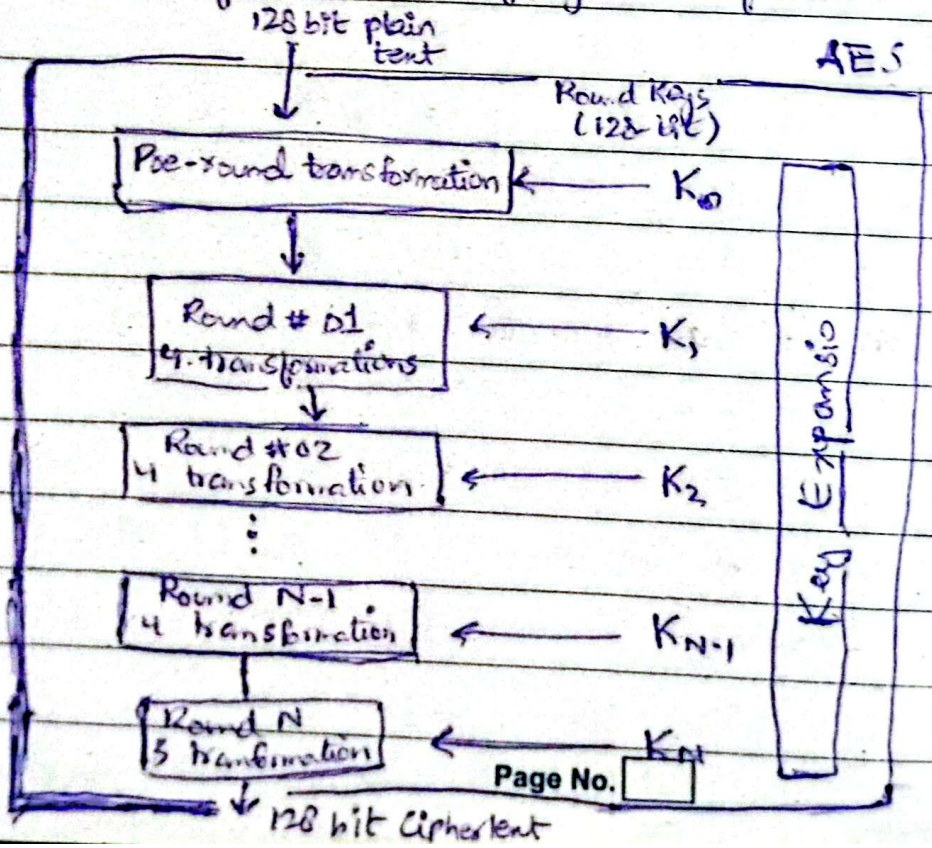
▷ Advance Encryption Standard (AES)

→ AES is a non-Feistel cipher that encrypts & decrypts a data block of 128 bits

→ AES Parameters

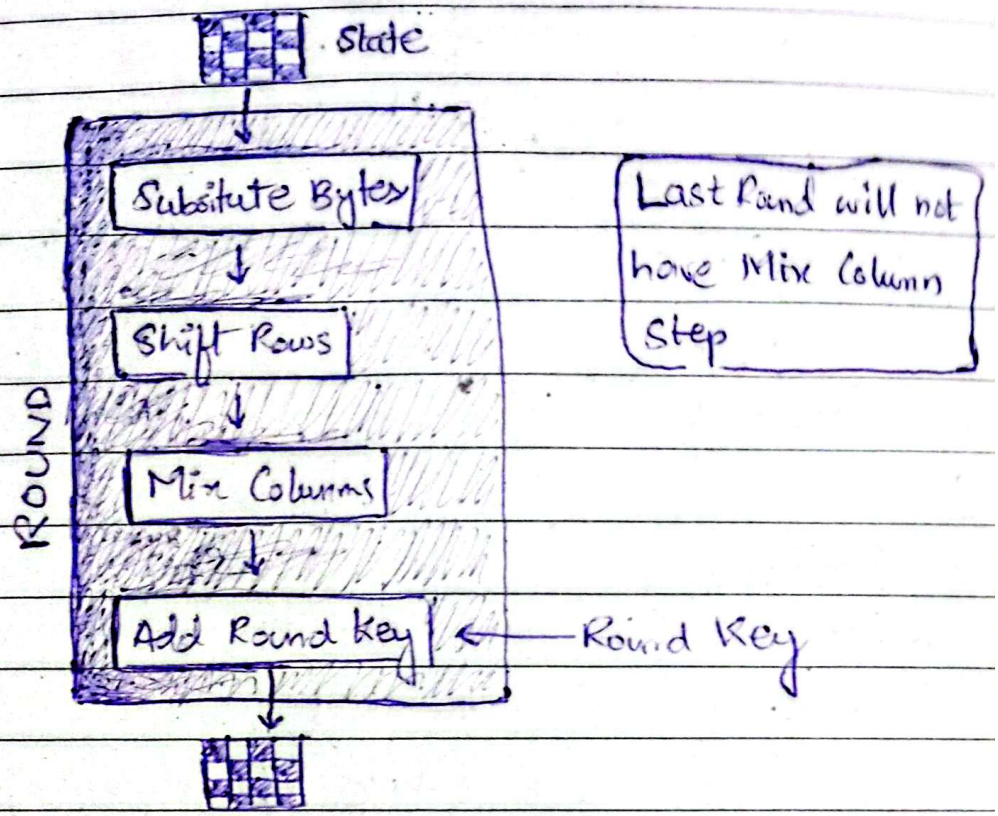
	AES-128	AES-192	AES-256
Key Size	128	192	256
Plaintext size	128	128	128
No. of rounds	10	12	14
Round Key Size	128	128	128

but the size of key in each round is 128-bits for every version of AES (No. of key = No. of rounds + 1)



Date _____ Day _____

▼ Structure of Each Round



AES Steps:

→ Four steps are used in each round (except last one which has 3), one of permutation & three of subsitution

(1) Subsitute Bytes

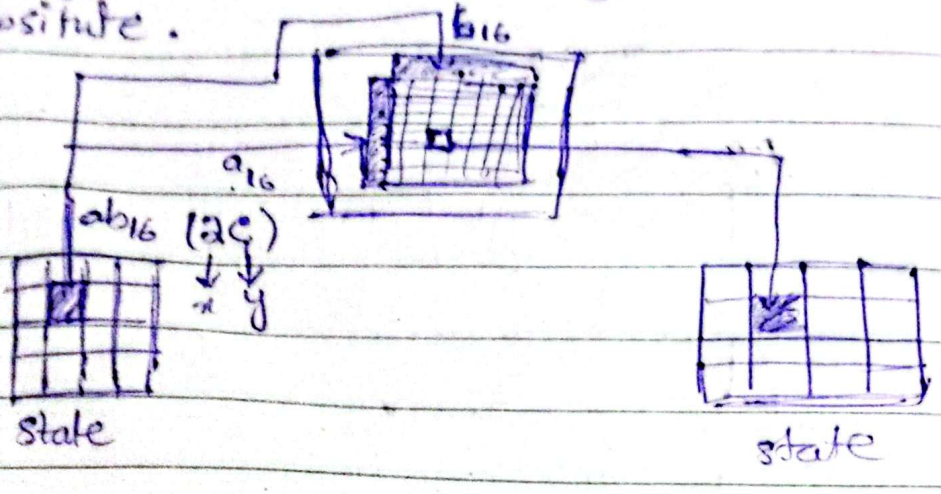
↳ It is simply a table lookup using a 16x16 matrix of byte values called an S-Box. This matrix consist of all the possible combinations of an 8-bit sequence

↳ A byte (8-bit) divided into two 4-bits, each giving a number btw (0-F).

1 word = 4 byte
1 byte = 8-bits

Date _____ Day _____

One of which is x & other is y we use them to substitute.



② Shift Rows

↳ Here we shift each row.

↳ Row #00 : No shift

Row # 01 : 1-byte left circular shift

Row # 02 : 2-byte left circular shift

Row # 03 : 1-byte right circular shift / 3-byte left "

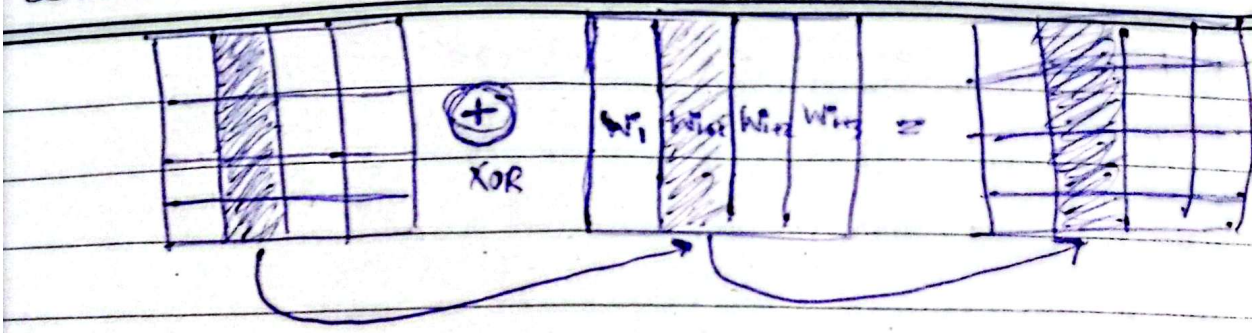
③ Mix Coloumn

↳ The state matrix is multiplied with another constant matrix to give a new state

④ Add Round Key

→ Each round key has 4 words in it so we add each word with state

Date _____ Day _____



- Confussion
  - ↳ Making the relationship b/w the key and cipher text as complex as possible
  - ↳ Achieved by Substitution
  - ↳ An AES - Sbox replaces each byte with another in a complex way

- Diffussion
  - ↳ Spreads the influence of one plain text symbol over many Ciphertext symbols
  - ↳ Achieved by permuting & mixing
  - ↳ In AES, Shift Rows + Mix Column does this.

Date _____ Day _____

▸ Block Cipher Modes of Operation

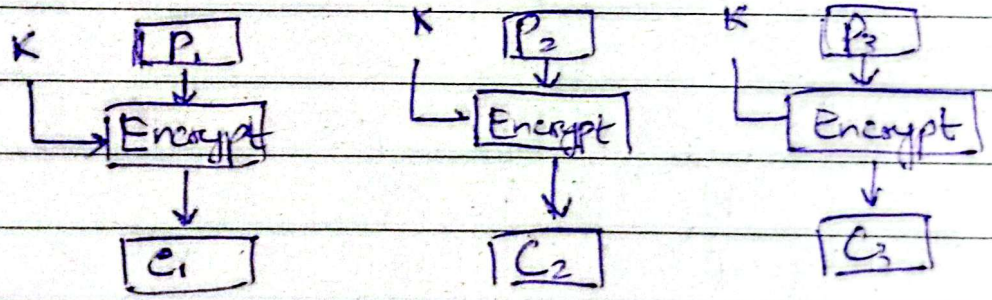
→ Each encryption algo has fixed input size. Like if an algo takes 'b' bits input but our data is greater than 'b' bits. Then we break it into blocks of 'b' bits.

→ There are 5 modes of operation

→ For different applications — different mode of operations are used.

• ECB (Electronic Code Book)

↳ Each block is encoded independently using the same key.



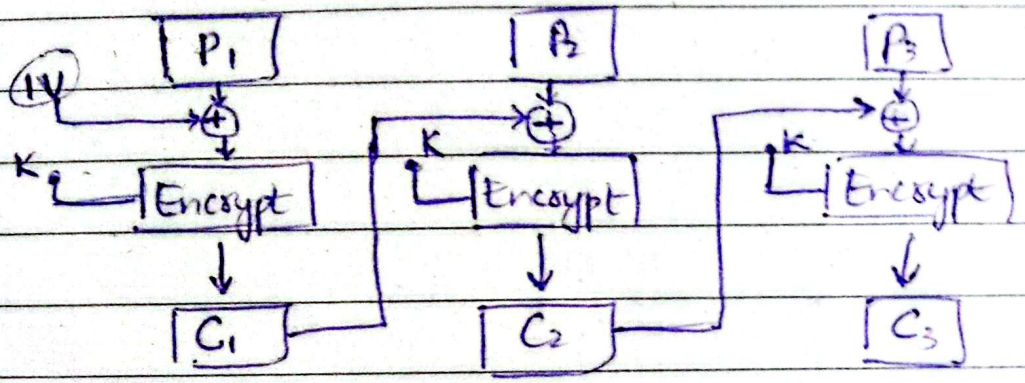
↳ Ideal for short amount of data.

↳ Since each one is independent so it can be fast if run ||y.

↳ If $P_1 = P_2$ then $C_1 = C_2$ (Less not good for long messages) Cryptanalysis is possible

Date _____ Day _____

- CBC (Cipher Block Chaining)
  - → Same PT block — Different CT block
  - → Same key will be used
  - → Chaining is used
  - → Each block encryption depends on previous one
  - → Therefore repeating patterns are not exposed



- Pros
  - ↳ Appropiate for larger messages
  - ↳ Confidentiality + Authentication → * both sender & recv have the initialization vector
- Cons
  - ↳ Slow — No //ism
  - ↳ Cannot encrypt any block since we need the cipher text of prev block
  - ↳ IV must be known to both sender & recv

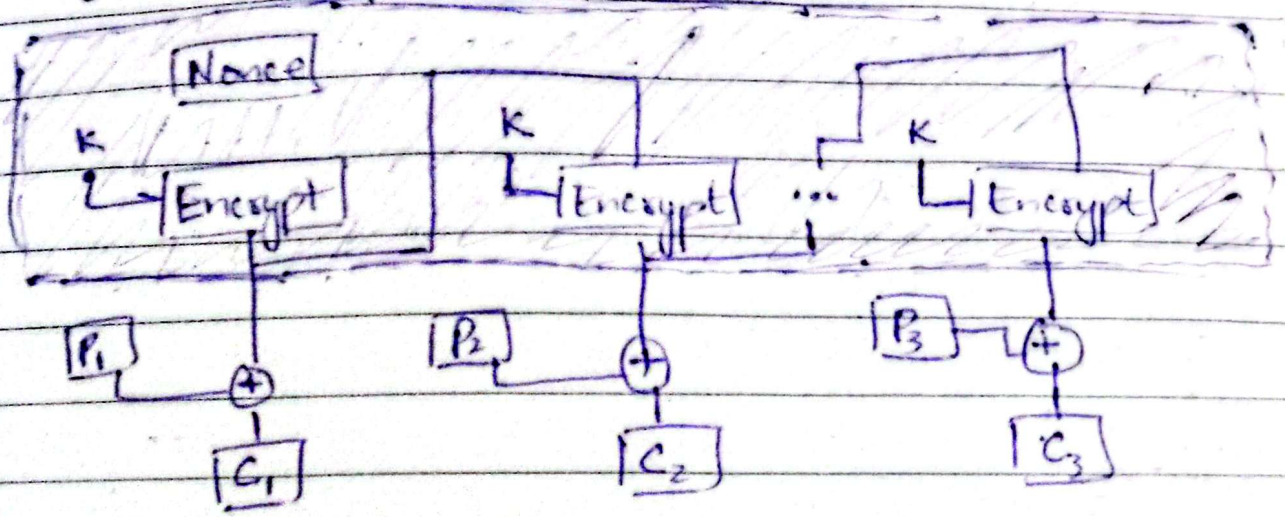
↳ General purpose block oriented transmission

Date _____ Day _____

- CFB (Cipher Feedback)
  - ↳ Convert a block cipher to stream cipher
  - ↳ Why stream cipher?
    - ↳ No need of padding (if length of block < b)
    - ↳ Real time applications
    - ↳ length of PT = len of CT
  - ↳ General purpose stream oriented transmission
  - ↳ Authentication
  - ↳ Preceding cipher text is used an input to the encryption algo to produce pseudorandom output which is XORED with PT to produce next unit of CT.
- Pros
  - ↳ Can operate in real time
  - ↳ Padding eliminated
  - ↳ Encryption func does decryption as well
  - ↳ len PT = len CT
- Cons
  - ↳ Chances of wastage of transmission

Date _____ Day _____

• OFB (Output Feedback)



↳ In CFB the ciphertext was feedback to next iteration but here the o/p of encryption function is used

↳ Stream oriented transmission over noisy channel (eg: Satellite Communication)

• Pros

↳ Same PT – Same Key – Different CT

↳ The PT len can be of random choice

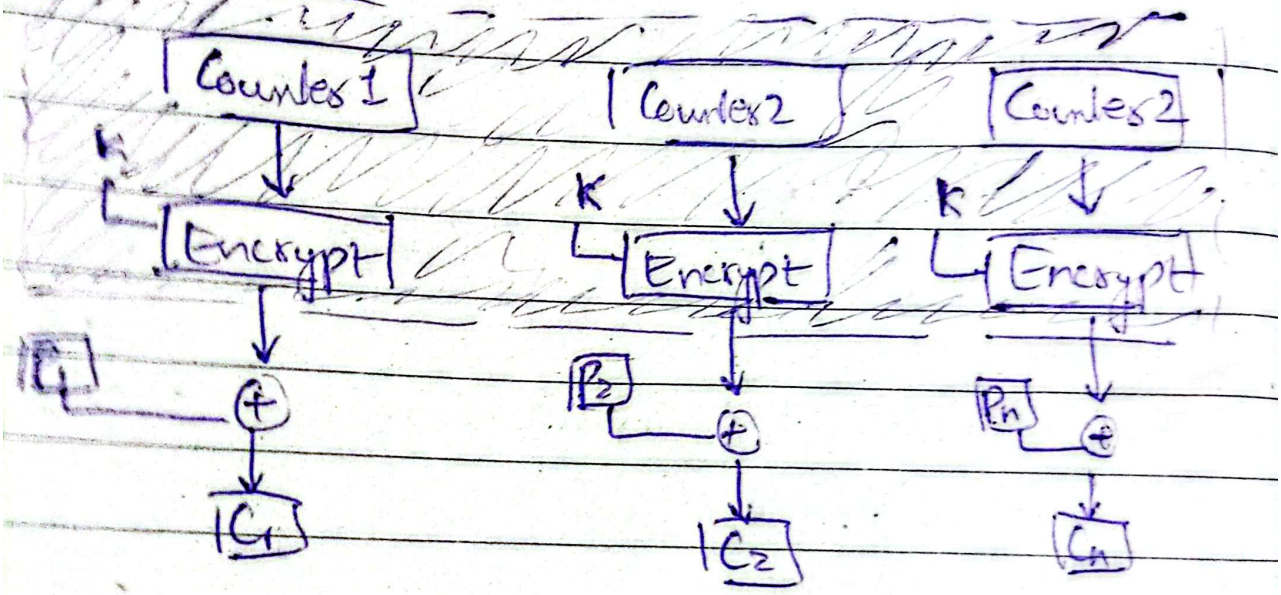
• Cons

↳ Sender & Recvr must by Synced

↳ No // ism

Date _____ Day _____

- CTR (Counter Mode)
  - ↳ Application to ATM, IP security etc.
  - ↳ Size of counter = plaintext block size
  - ↳ Different counter value for each plaintext
  - ↳ Counter value is initialized
  - ↳ Counter value will be incremented



- Pros
  - ↳ Can be implemented thru hardware / software
  - ↳ Fast ∵ ||ism can be done
  - ↳ Can be applied to real time data
  - ↳ Useful for high speed requirements.