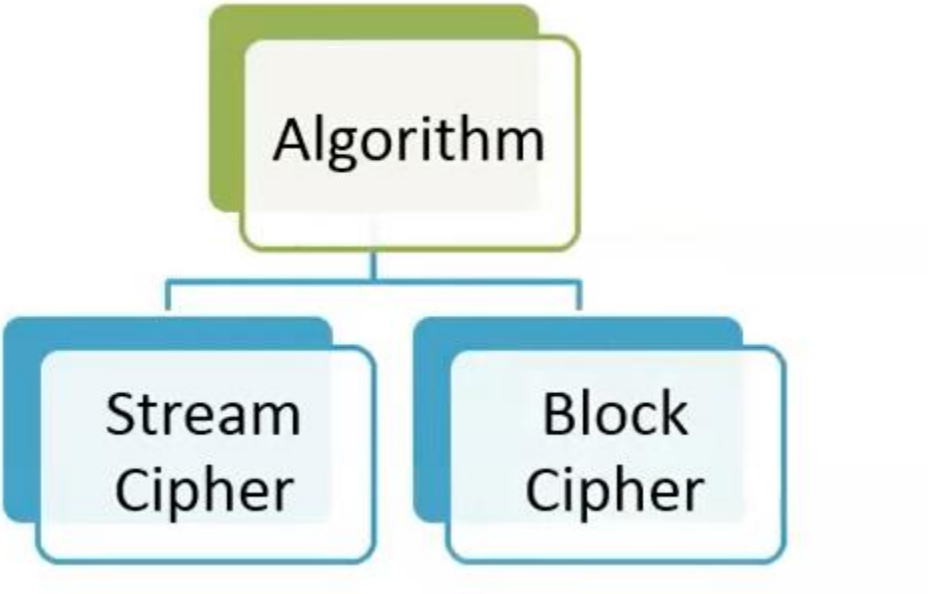
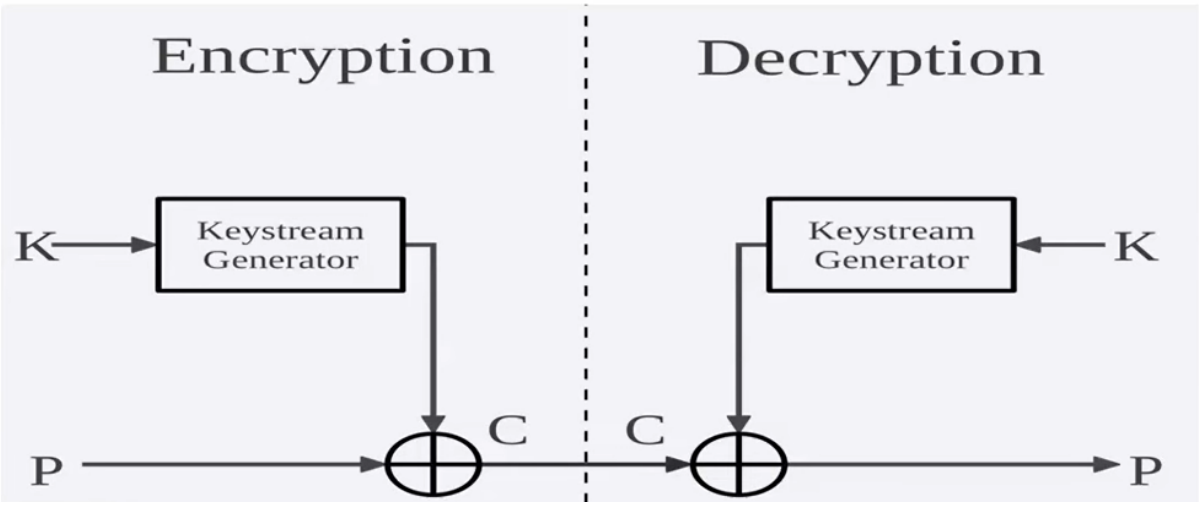
## Cryptographic Algorithm

- Basically, a cryptographic algorithm is used for the transformation of plaintext into ciphertext.
- There are basically two methods on which cryptographic algorithms work:




## Stream Cipher

- In stream cipher, keys and algorithms are applied to each binary digit in a data stream, one bit at a time, rather than encrypting a block of data.
- A stream cipher operates on plaintext accepting only one bit at a time.
- A stream cipher in which each bit of plain text message XORs with each bit of key to obtain a cipher text message.




- There is a key stream generator which outputs a stream of bits: k1, k2, k3, ... ki and XORed with a stream of plaintext bits p1, p2, ..., pi to produce the stream of cipher text bits.

$$Ci=Pi \oplus Ki$$

- During decryption, the cipher text bits are XORed with the same key stream to recover the plain text bits.

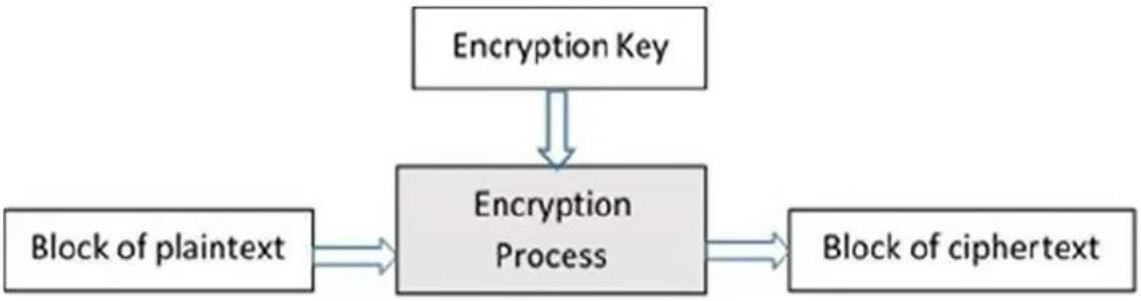
$$Pi=Ci \oplus Ki$$

❖ list of common encryption algorithms categorized under stream ciphers

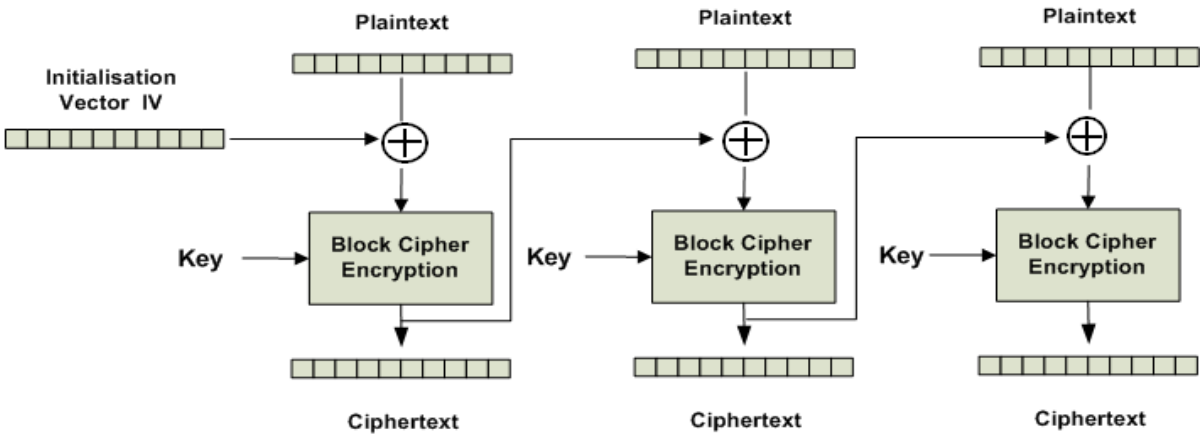
- RC4 (Rivest Cipher 4)
- Salsa20
- ChaCha20
- A5/1 and A5/2
- Trivium
- Grain

# Block Cipher

- In Block cipher, plain text message is divided into fixed-size blocks and each block is encrypted with some fixed-size key.
- Divide each plain text message into blocks of 64, 128, 256 bits and apply key sizes 40, 56, 64, 80, 128, 168, 192 and 256 bits which generates cipher text blocks same as the size of plain text blocks.
- Data Encryption Standard (DES) is the best example of block cipher in which each block of 64-bit gets encrypted using 56-key bit and cipher text of 64-bit gets generated.



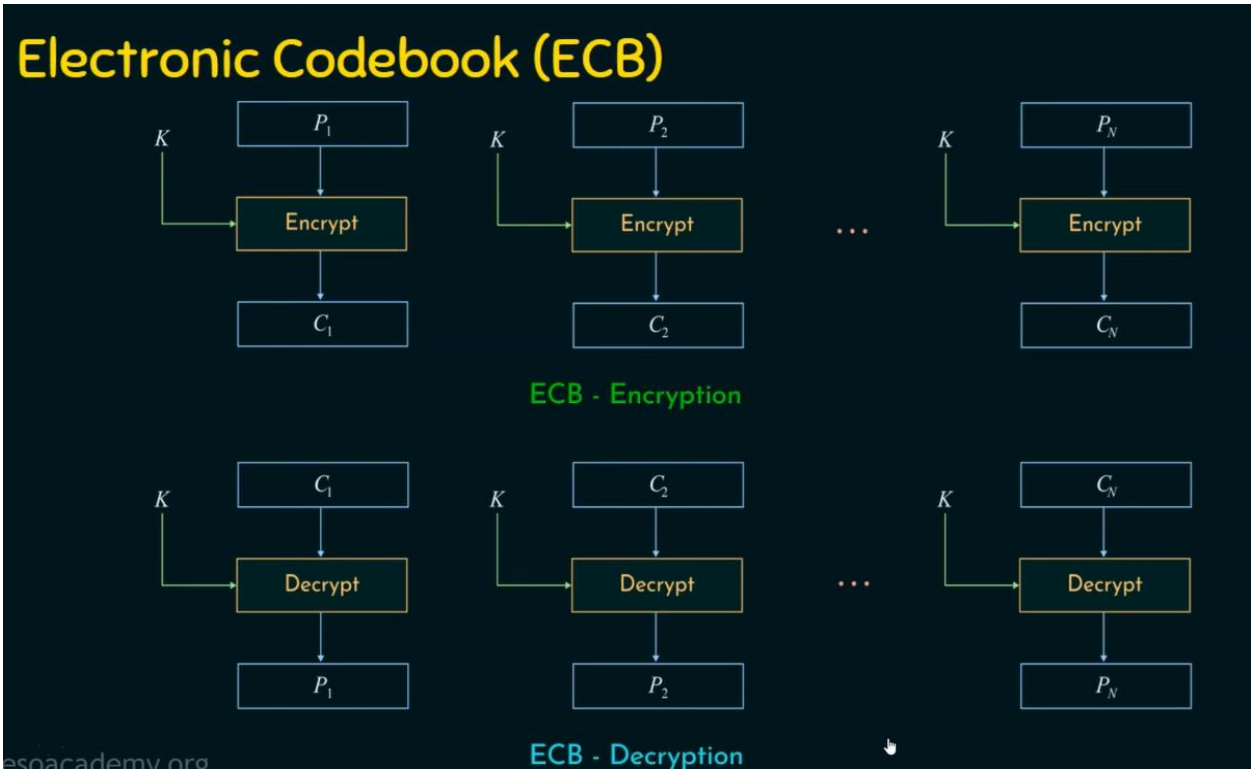

- A receiver-side decrypts messages with the same key to generate plaintext.
- Block cipher also uses the concept of a key generator.
- Block ciphers use chaining mode; this is because for repeating text patterns, the same cipher block will be generated which can give a clue to cryptanalysts regarding what the original plaintext is.
- As a chaining mode, the previous block is mixed with the current block to avoid repeats in patterns. It is more secure.

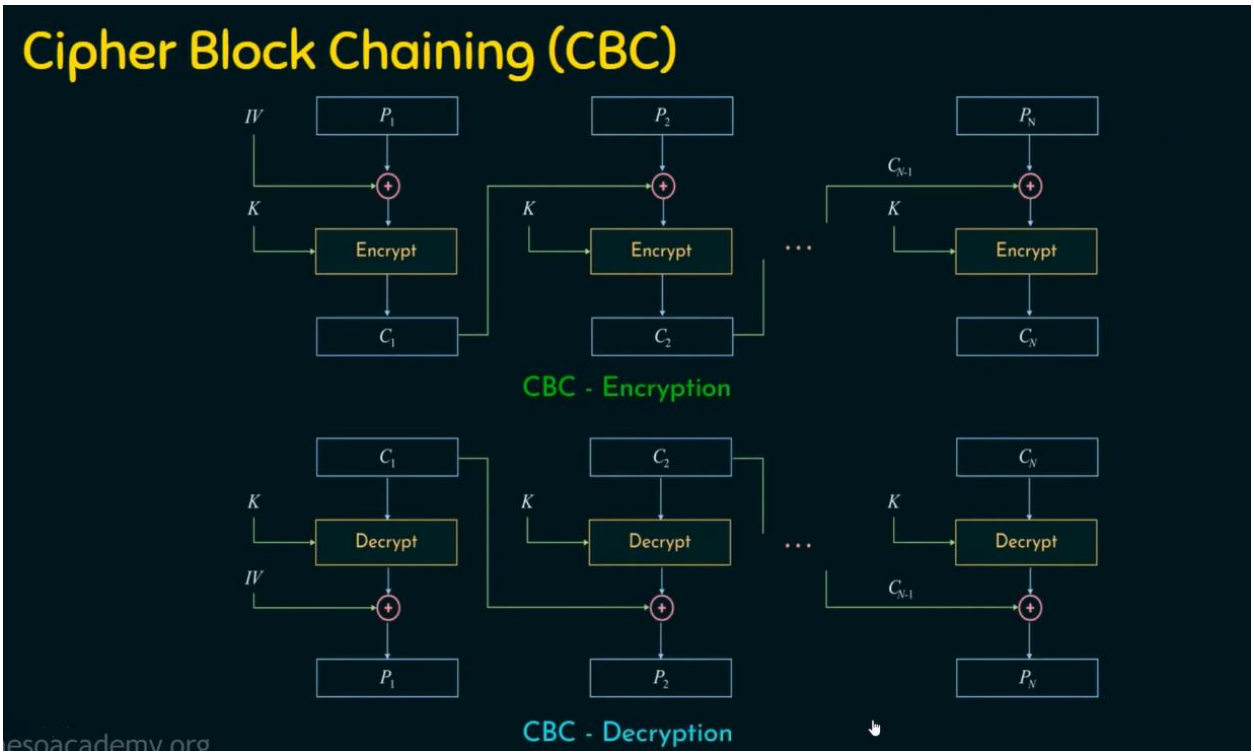



❖ list of common encryption algorithms categorized under block ciphers

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard):
- 3DES (Triple DES)
- Blowfish
- Twofish
- Serpent
- IDEA (International Data Encryption Algorithm)

## ❖ Assignment of ECB and CBC



# Difference between block and stream cipher

| No. | Stream Cipher | Block Cipher |
|---|---|---|
| 1 | Key and algorithm applied on each binary digit. | Key and algorithm applied on block of data. |
| 2 | Less time consuming in compare to block cipher. | More time consuming in compare to stream cipher. |
| 3 | Only one bit encrypting at a time, it is faster than block cipher. | Block of data is encrypting at a time block cipher is slower than stream cipher. |
| 4 | It doesn't used chaining mode. | It uses chaining mode. |
| 5 | Hardware implementation is easy using stream cipher. | Software implementation is easy using block cipher. |
| 6 | One time pad is the best example of stream cipher. | DES is the best example of block cipher. |
| 7 | Less Secure in compare to Block cipher. | More secure in compare to stream cipher. |