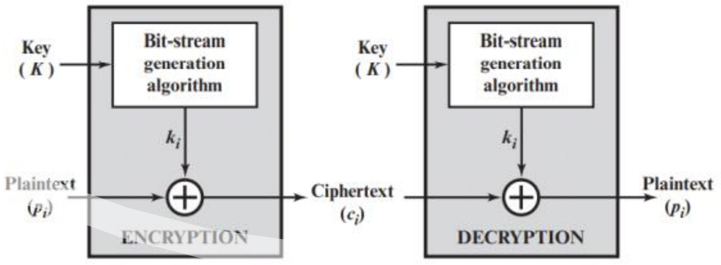
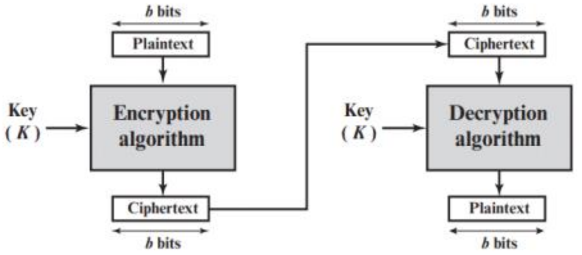
Basic Terminologies

12 February 2021 10:03



(a) Stream cipher using algorithmic bit-stream generator



STREAM CIPHER:

A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. Examples of classical stream ciphers are the Vigenère cipher
and the Vernam cipher.

BLOCK CIPHER:

In the ideal case, a one-time pad version of the Vernam cipher would be used , in which the keystream (ki) is as long as the plaintext bit stream (pi). If the cryptographic keystream is random, then this cipher is unbreakable by any means other than acquiring the keystream.

However, the keystream must be provided to both users in advance via some independent and secure channel. This introduces insurmountable logistical problems if the intended data traffic is very large.

Block Cipher Modes of Operation

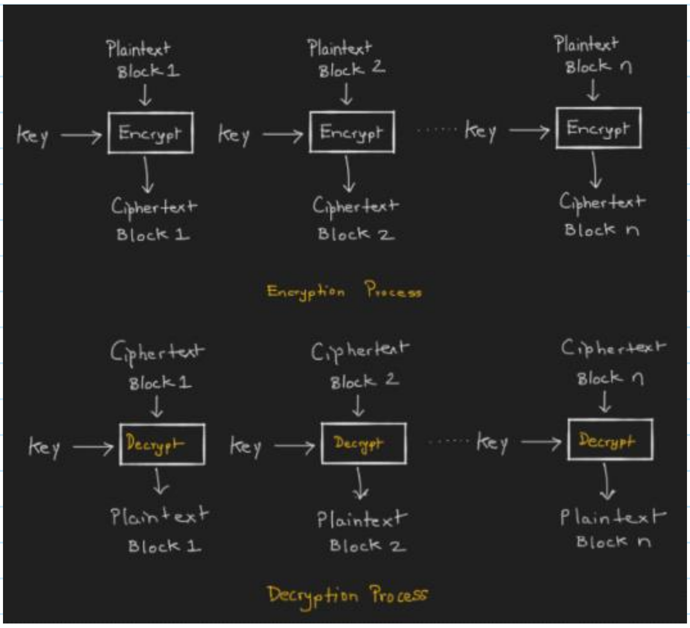
15 February 2021 10:38

There are in total 5 different modes in which the block ciphers work to protect the data. These 5 modes are as follows:

1. Electronic Codebook (ECB) Mode
2. Cipher Block Chaining (CBC) Mode
3. Cipher Feedback (CFB) Mode
4. Output Feedback (OFB) Mode
5. Counter (CTR) Mode

ELECTRONIC CODE BOOK

□



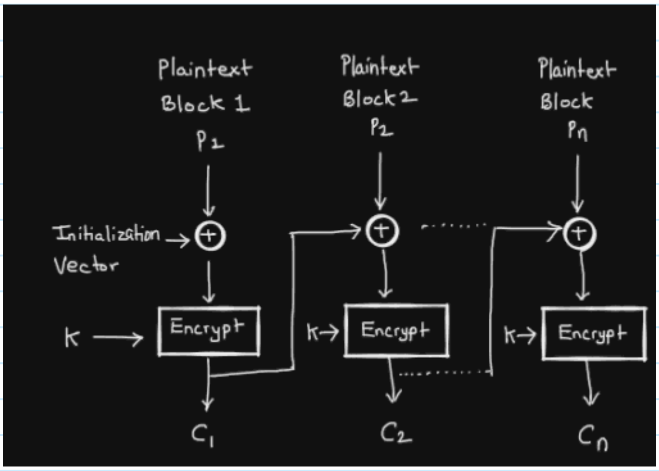
- Plaintext is divided into blocks of 64 bits each.

- **Drawback :**
  Occurrence of more than 1 plaintext block in the input generates same ciphertext block in the output.

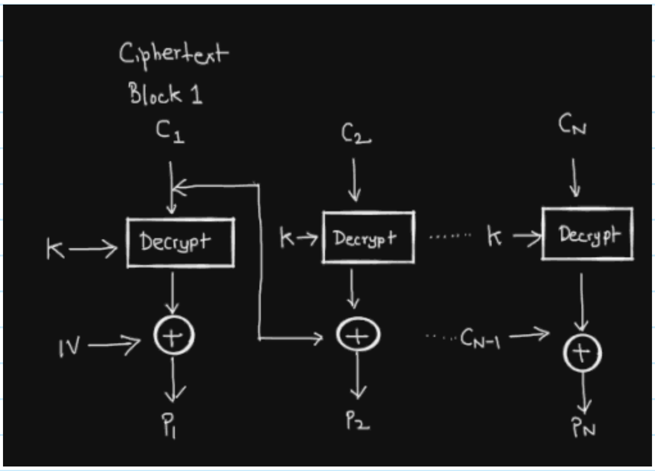
Cipher Block Chaining (CBC)

17 February 2021 12:16

Cipher Block Chaining (CBC)



ENCRYPTION



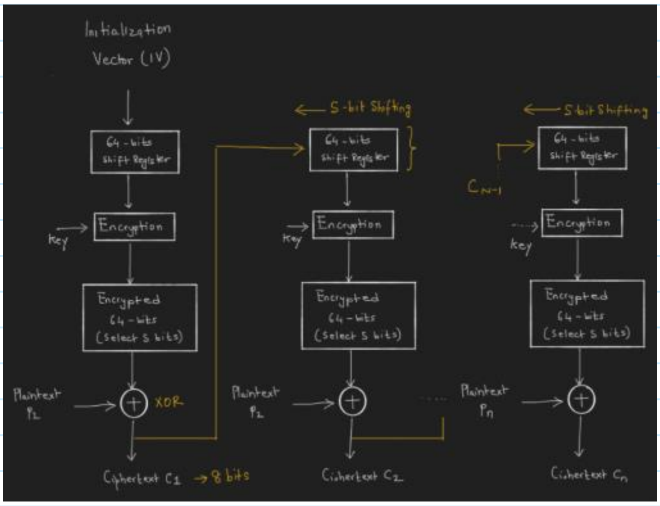
DECRYPTION

- Each block of plaintext is XOR'ed with the previous block of ciphertext.
- Use of Random Initialization Vector.
- Even if Plaintext block repeats in the input, the output of CBC mode yields totally different Ciphertext Blocks.

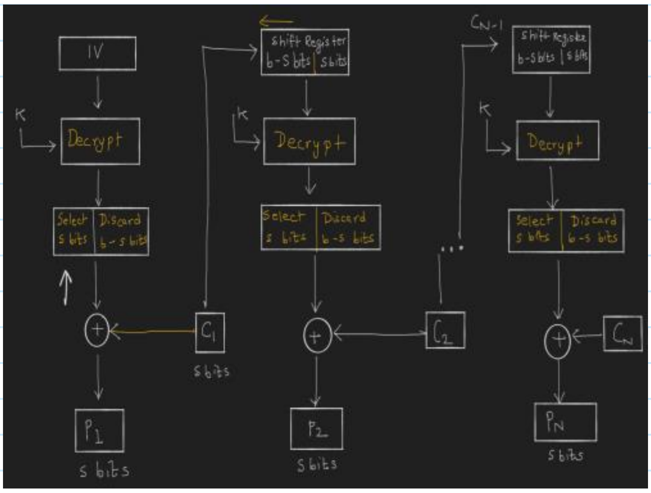
Cipher Feedback Mode (CFB)

15 February 2021 10:38

Cipher Feedback Mode (CFB)



ENCRYPTION



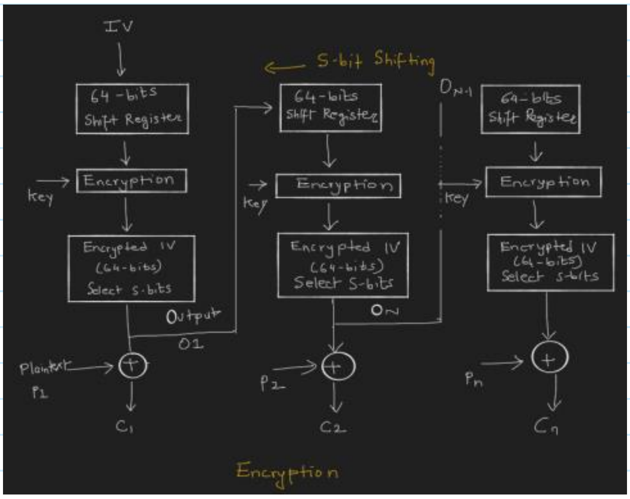
DECRYPTION

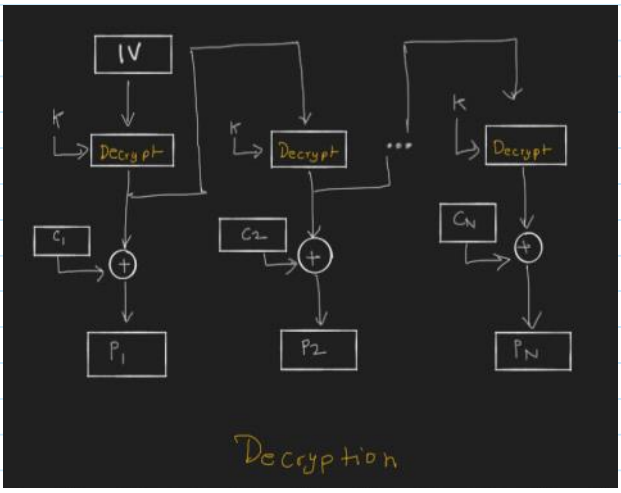
- CFB uses Block Ciphers as Stream Ciphers.
- 64 Bit Initialization Vector (IV) is used which is stored in a Shift Register.
- IV is encrypted and produces a 64 bit encrypted IV.
- 64 bit shift register is shifted left by S bits and C1 is placed in the rightmost S bits of the Shift Register, which again undergoes the encryption process in the next round.
- The process continues untill all the plaintext text is encrypted.

Output FEEDBACK MODE

17 February 2021 12:08

Output FEEDBACK MODE



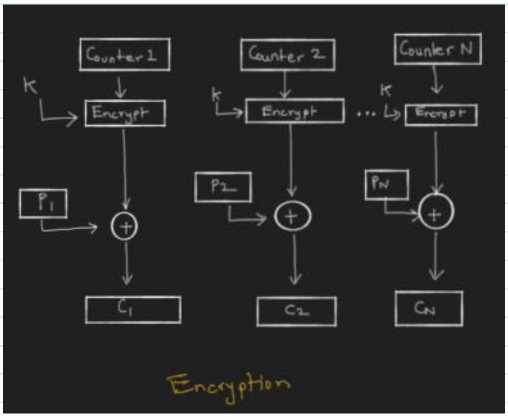


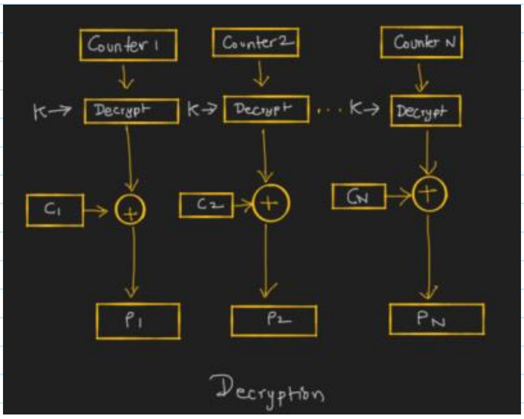
- It is similar to Cipher Feedback Mode.
- The difference lies in the fact is that, the Output O1, instead of the Ciphertext C1 is directly placed in the next stage of the shift register without XOR Operation.
- This ensures that bit erros are avoided during transmission.

Counter Mode

17 February 2021 12:09

Counter Mode





- It is similar to Output Feedback Mode.
- The difference lies in the fact is that it uses counters or sequence numbers as inputs to the algorithm.
- We put a constant value as initial value of counter which will be same size as that of a plaintext block.