2. CBC Operation Mode.

CBC stands **for Cipher-Block Chaining** The previous cipher text block is XORed with the clear text block before applying the encryption mapping.

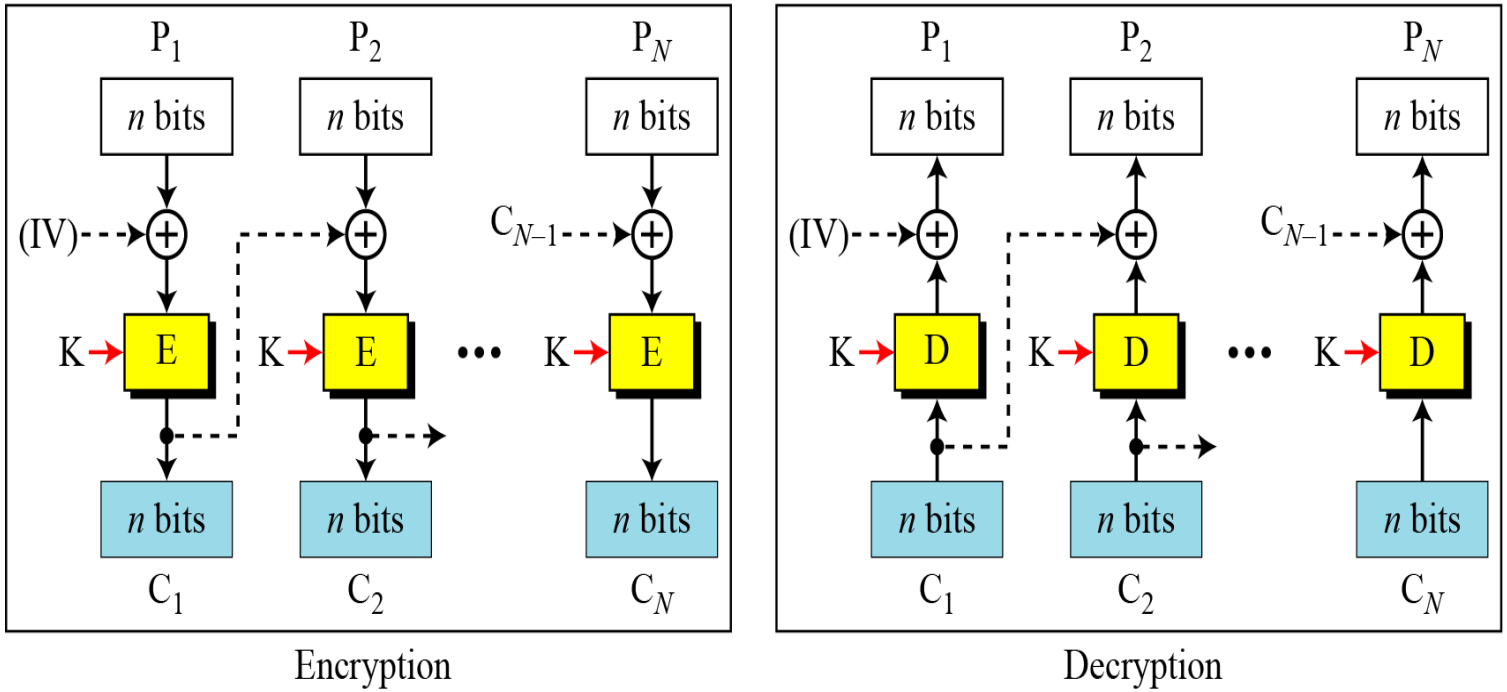
Solve security deficiencies in ECB where Repeated same plaintext block result different ciphertext block

Use Initial Vector (IV) to start process

$C_i = EK (P_i \text{ XOR } C_{i-1})$

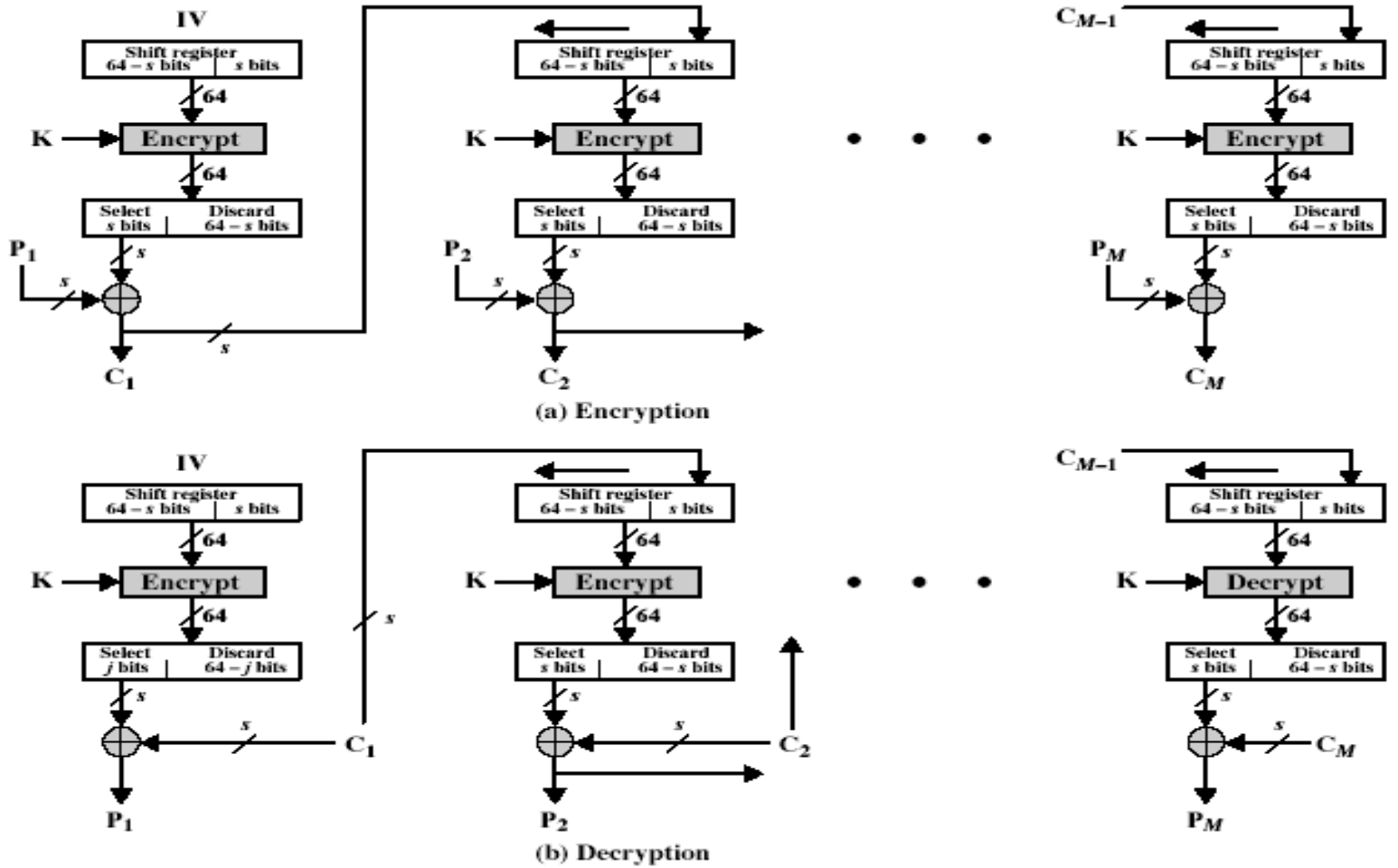
$C_0 = IV$

E: Encryption D : Decryption
P_i: Plaintext block *i* C_i : Ciphertext block *i*
K: Secret key IV: Initial vector (C_0)



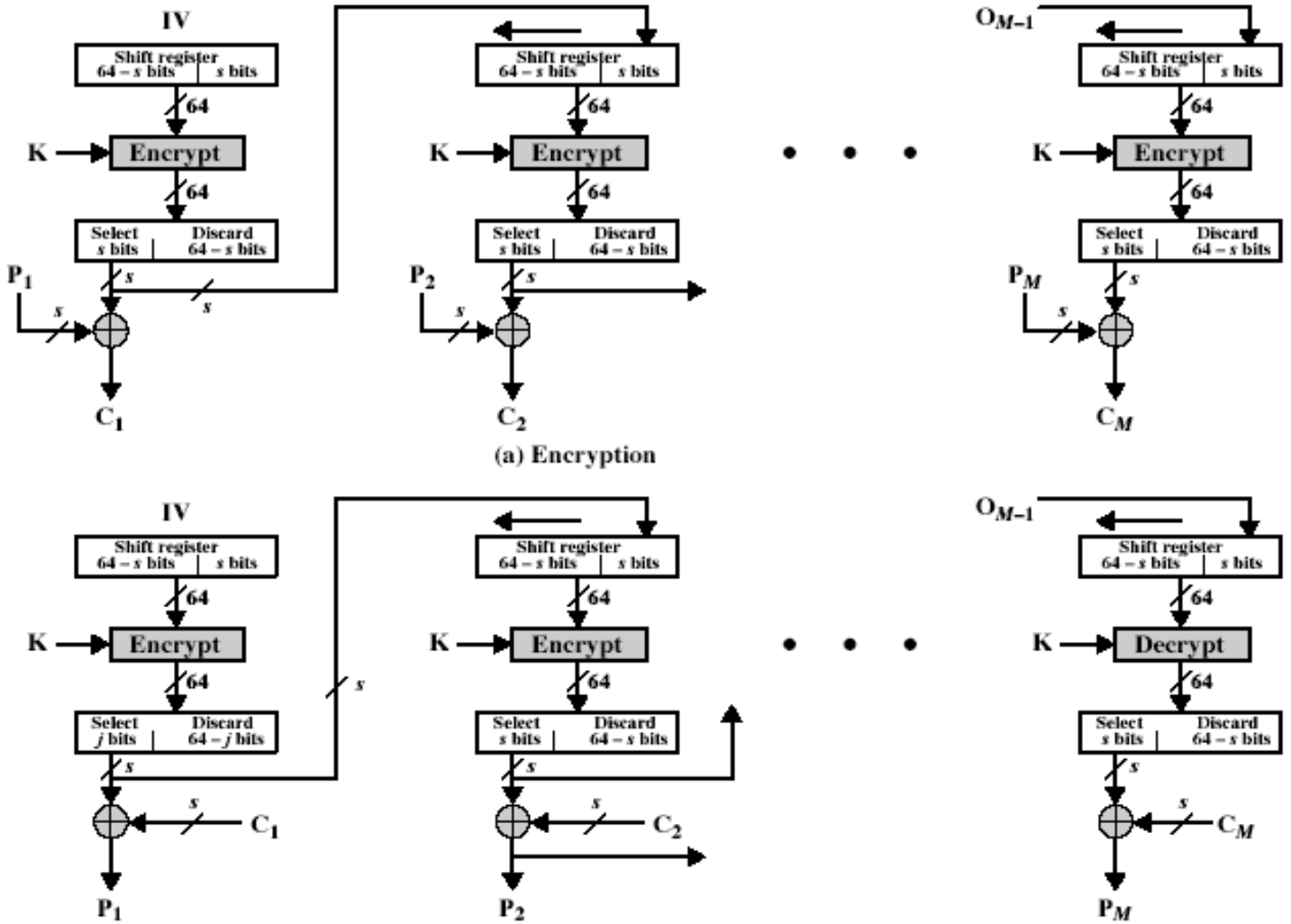
3. Cipher FeedBack (CFB).

- Message is treated as a stream of bits , Bitwise-added to the output of the block cipher , Result is feedback for next stage (hence name).its Uses for stream data encryption, authentication
- Use Initial Vector to start process.
- Plaintext is treated as a stream of bits. Any number of bit (1, 8 or 64 or whatever) to be feed back (denoted CFB-1, CFB-8, CFB-64)



4. Output Feedback Mode (OFM).

- The block cipher is used as a stream cipher, it produces the random key stream.
- Very similar to CFB But output of the encryption function output of cipher is fed back (hence name), instead of ciphertext.



- **Product Cipher** - An encryption scheme that "uses multiple ciphers in which the cipher text of one cipher is used as the clear text of the next cipher". Usually, substitution ciphers and transposition ciphers are used alternatively to construct a product cipher.
- **Iterated Block Cipher** - A block cipher that "iterates a fixed number of times of another block cipher, called round function, with a different key, called round key, for each iteration".
- Most symmetric block ciphers are based on a **Feistel Cipher Structure.**
- **Feistel Cipher** - An iterate block cipher that Process through multiple rounds which
  - partitions input block into two halves
  - perform a substitution on left data half
  - based on round function of right half & sub key
  - then have permutation swapping halves

Feistel Cipher Structure