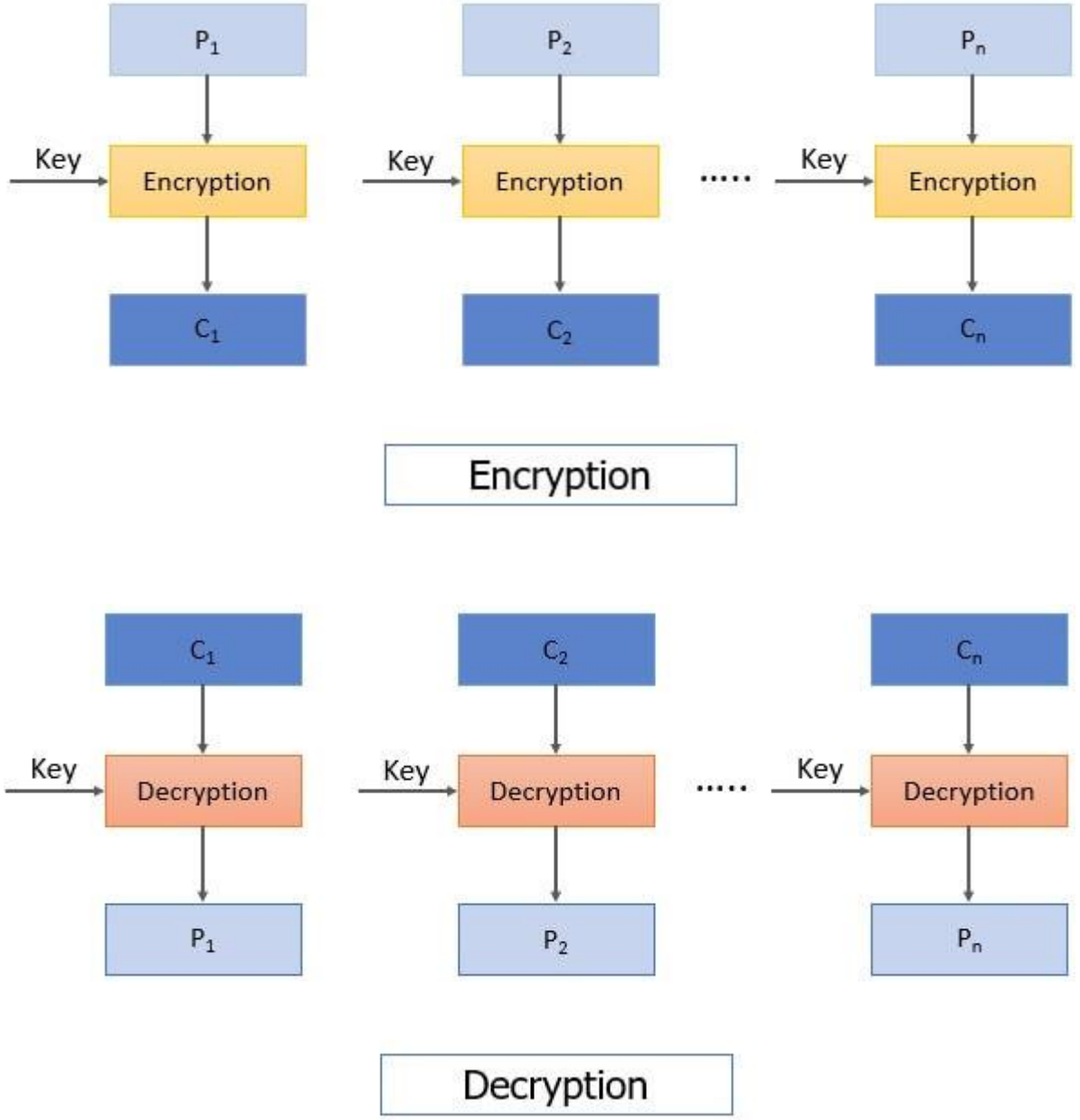
5 MODE OF OPERATION IN BLOCK CIPHER (Part 2)

1. Electronic Code Book (ECB) Mode



1. Electronic Code Book (ECB) Mode

- Electronic Code Book (ECB) is the simplest block cipher mode of operation.
- In this mode, each block of plaintext is encrypted separately.

or

- Every block gets encrypted one at each time to form the cipher block.
- The same key is used to encrypt /decrypt each block.
- ECB is considered for encrypting the small messages which have a rare possibility of repeating text.

The main disadvantage to this mode is that identical plaintexts encrypted with the same key create identical ciphertexts, which allows an attacker to learn some information about the encrypted message based solely on the ciphertext.

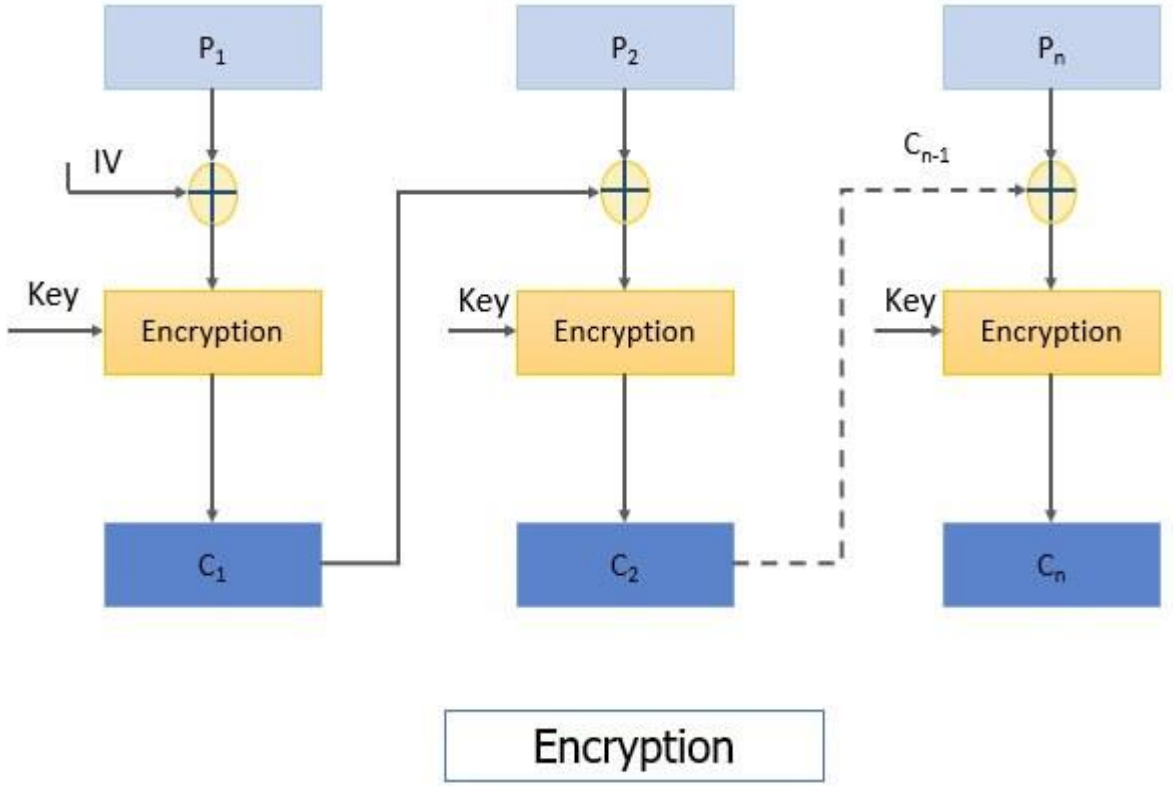
2. Cipher Block Chaining Mode

This overcomes the ECB limitations. Here, even if the plain text has many repeating blocks, its encryption does not produce a similar cipher block. This is done by adding chaining to it, which gets the ciphertext block obtained depending on the current and any previous plain text block input.

i.e To overcome the limitation of ECB i.e. the repeating block in plain text produces the same ciphertext, a new technique was required which is Cipher Block Chaining (CBC) Mode. CBC confirms that even if the plain text has repeating blocks its encryption won't produce same cipher block.

NOTE: Initialization vectors (IVs) are **used** to prevent a sequence of text that is identical to a previous sequence from producing the same exact ciphertext when encrypted.

➢ **encryption steps of CBC**

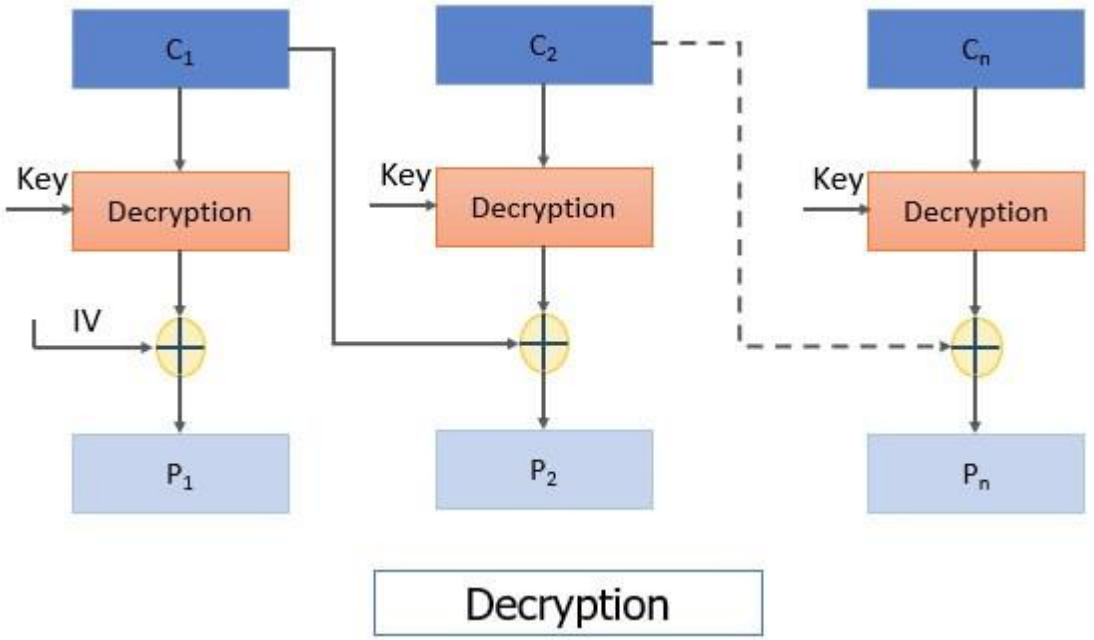


Step 1: The initialization vector and first plain text block are XORed and the result of XOR is then encrypted using the key to obtain the first ciphertext block.

Step 2: The first ciphertext block is fed to the encryption of the second plain text block. For the encryption of second plain text block, first ciphertext block and second plain text block is XORed and the result of XOR is encrypted using the same key in step 1 to obtain the second ciphertext block.

Similarly, the result of encryption of second plain text block i.e. the second ciphertext block is fed to the encryption of third plain text block to obtain third ciphertext block. And the process continues to obtain all the ciphertext blocks.

Decryption steps of CBC:



Step 1: The first ciphertext block is decrypted using the same key that was used for encrypting all plain text blocks. The result of decryption is then XORed with the initialization vector (IV) to obtain the first plain text block.

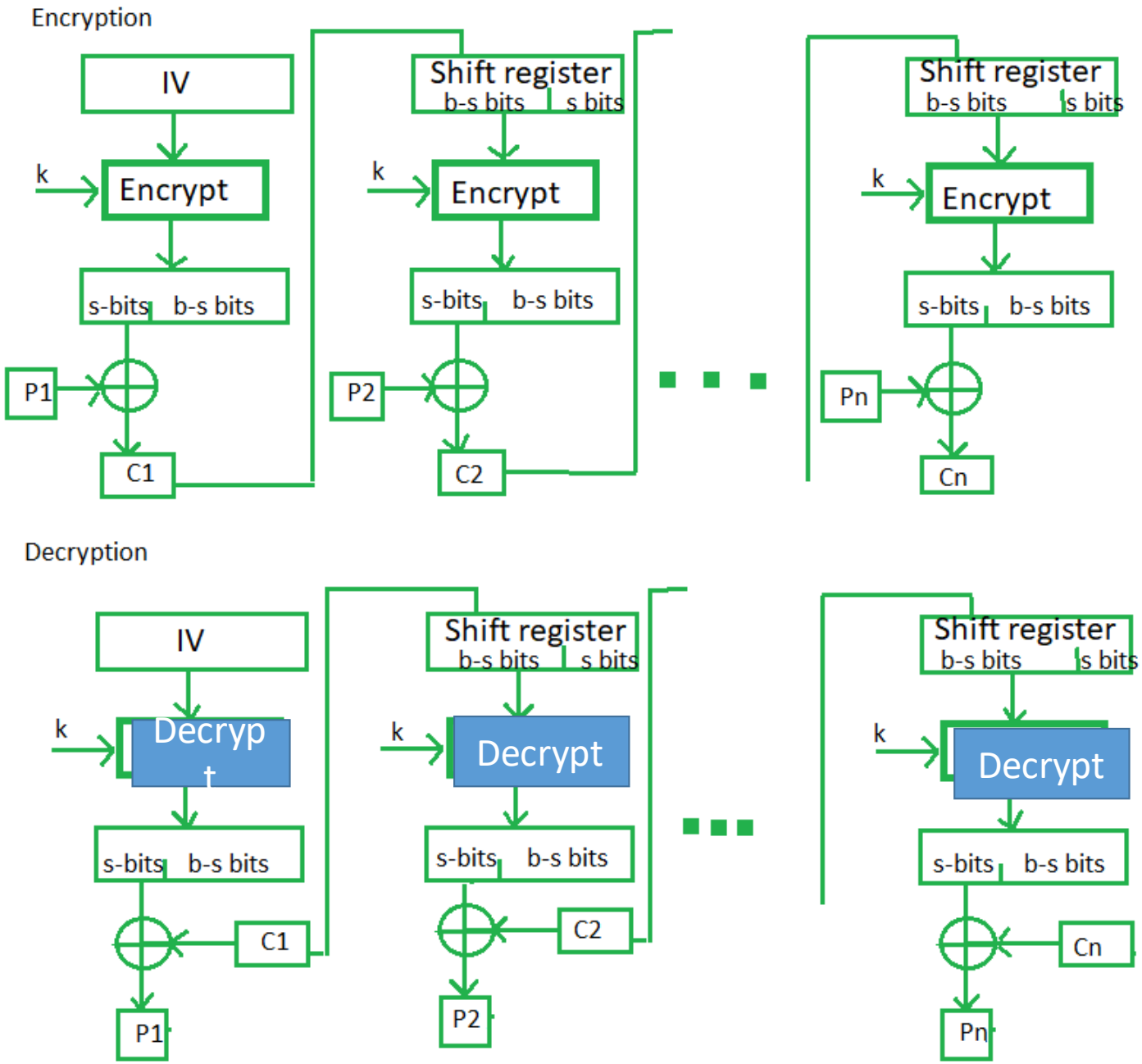
Step 2: The second ciphertext block is decrypted and the result of decryption is XORed with the first ciphertext block to obtain the second plain text block. And the process continues till all plain text blocks are retrieved.

NOTE: There was a limitation in CBC that if we have two identical messages and if we use the same IV for both the identical message it would generate the same ciphertext block.

3.Cipher Feedback (CFB) Mode

This is Ciphertext feedback (CFB) which is also a mode of operation for a block cipher. In contrast to the cipher block chaining(CBC) mode, which encrypts a set number of bits of plaintext or original text at a time, it is at times desirable or sensible to encrypt and transfer or exchange some plaintext or original text values instantly one at a time, for which ciphertext feedback is a method in cryptography. Like cipher block chaining(CBC), ciphertext feedback(CFB) also makes use of an initialization vector (IV) in the blocks..

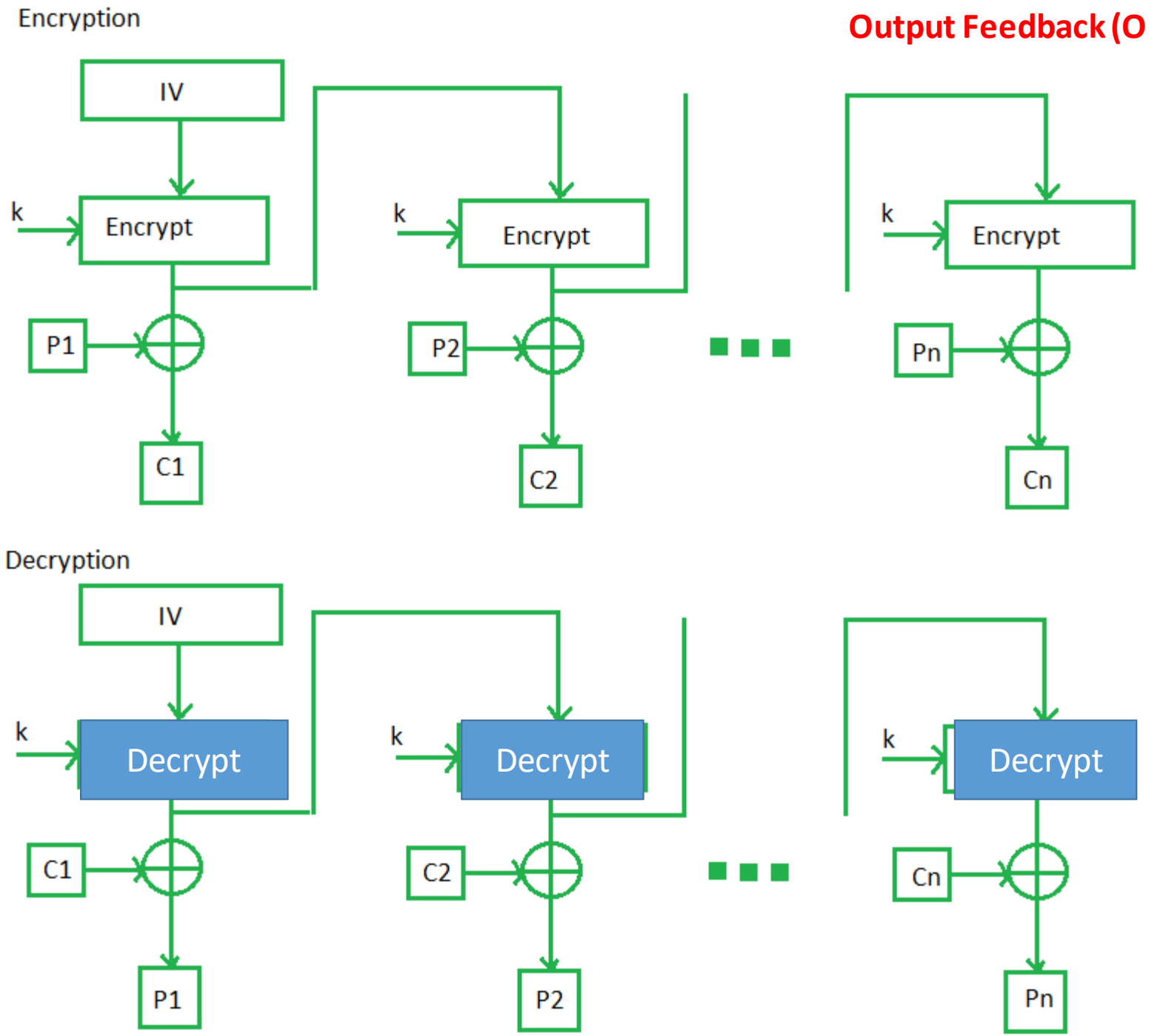
3.Cipher Feedback (CFB) Mode



4. Output Feedback (OFB) Mode

The output feedback (OFB) mode is almost similar to the CFB. The difference between CFB and OFB is that unlike CFB, in OFB the encrypted IV is fed to the encryption of next plain text block. The other difference is that CFB operates on a stream of bits whereas OFB operates on the block of bits.

Output Feedback (OFB) Mode



5. Counter Mode

The Counter Mode or CTR is a simple counter based block cipher implementation. Every time a counter initiated value is encrypted and given as input to XOR with plaintext which results in ciphertext block. The CTR mode is independent of feedback use and thus can be implemented in parallel.