SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING(IoT and Cybersecurity Including BCT)

COURSE NAME : FUNDAMENTALS OF CRYPTOGRAPHY 19CS301

II YEAR / III SEMESTER

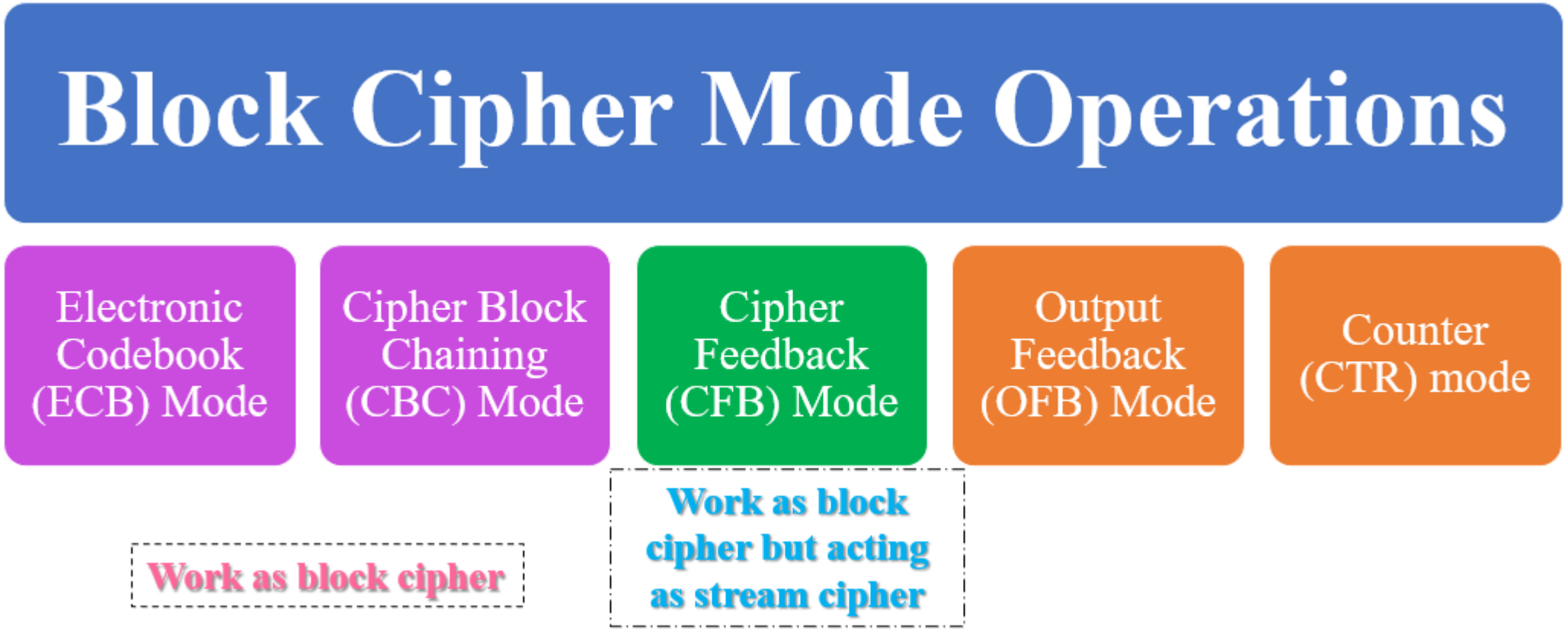
Unit II-

Topic :Modes of operations

Modes Of Operations

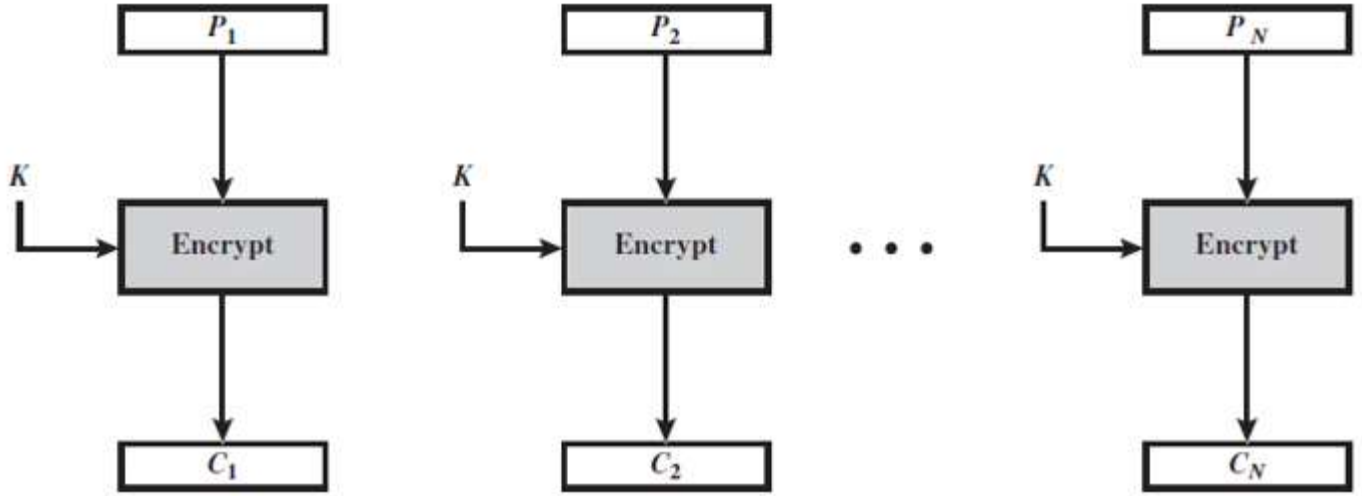
- Cryptographic algorithm works on main two techniques: block and stream ciphers.
- In a stream cipher, the plaintext is encrypted one bit at a time. In a block cipher, the plaintext is broken into blocks of a fixed length and the bits in each block are encrypted together. One of the main issues with block ciphers is that they only allow you to encrypt messages the fixed size as their block length
- If plaintext, which has a block size 64 bits easily encrypt. But encrypt a 65-bit message, you need a way to define how the second block should be encrypted.
- The solution to this is called block cipher modes of operation. Need of block cipher mode is basic building block for providing data security. In block cipher rather than encrypting one bit at a time, block of bits is encrypted at a time.
- There are 5 modes of operation for block cipher that may be used in a wide variety of applications like symmetric key cryptographic algorithm. These modes define how data encrypted and decrypted.

Modes Of Operations

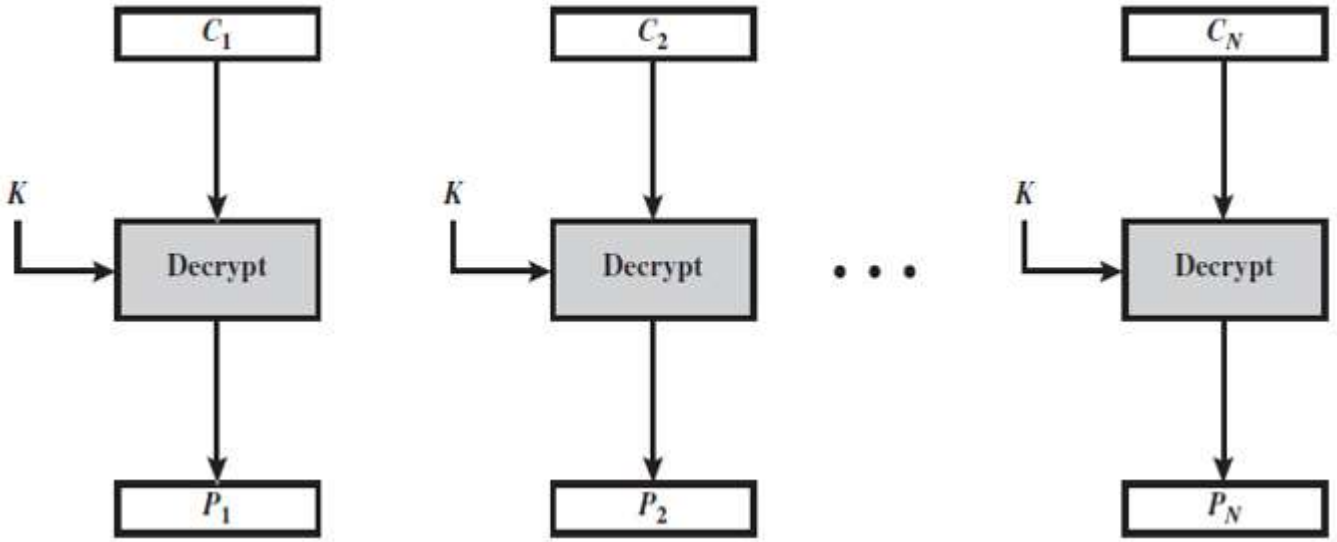


Electronic codebook(ECB)

- In ECB (Electronic Code Book) mode the given plain text message is divided into blocks of 64 bits each and each 64 bits blocks gets encrypted independently. The plaintext box produces cipher text of same size. All blocks of plaintext are encrypted using same key. Cipher text is decrypted using same key of encryption key
- Figure shows the encryption and decryption process of ECB mode.



Electronic codebook(ECB)



- The drawback of ECB mode is that for occurrence of more than one plaintext block in the input generates the same cipher text block in the output, which gives clue to the attacker.
- For example, “ABC” plain text convert into 64-bit block and it generates 64-bit cipher text “XYZ”.

Applications of Electronic codebook(ECB)

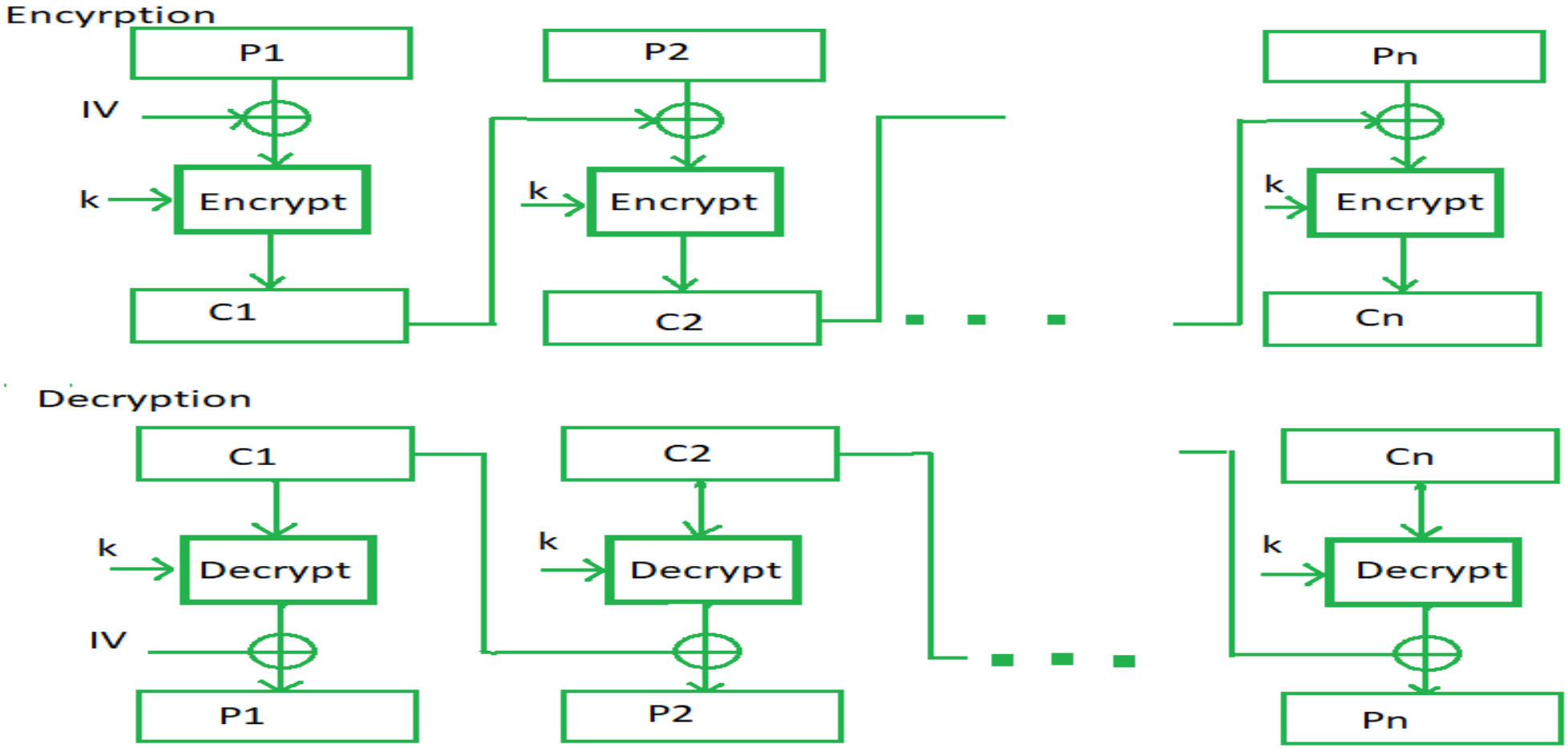
Only small messages can be encrypted to using ECB mode of operation.
Mostly ECB mode used, transmitting a single value in secure fashion. Ex. Password or key used for encryption.

Disadvantages of using ECB

Prone to cryptanalysis since there is a direct relationship between plaintext and ciphertext

Cipher block chaining (CBC)

- In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.



Advantages of CBC –

CBC works well for input greater than *b* bits.

CBC is a good authentication mechanism.

Better resistive nature towards cryptanalysis than ECB.

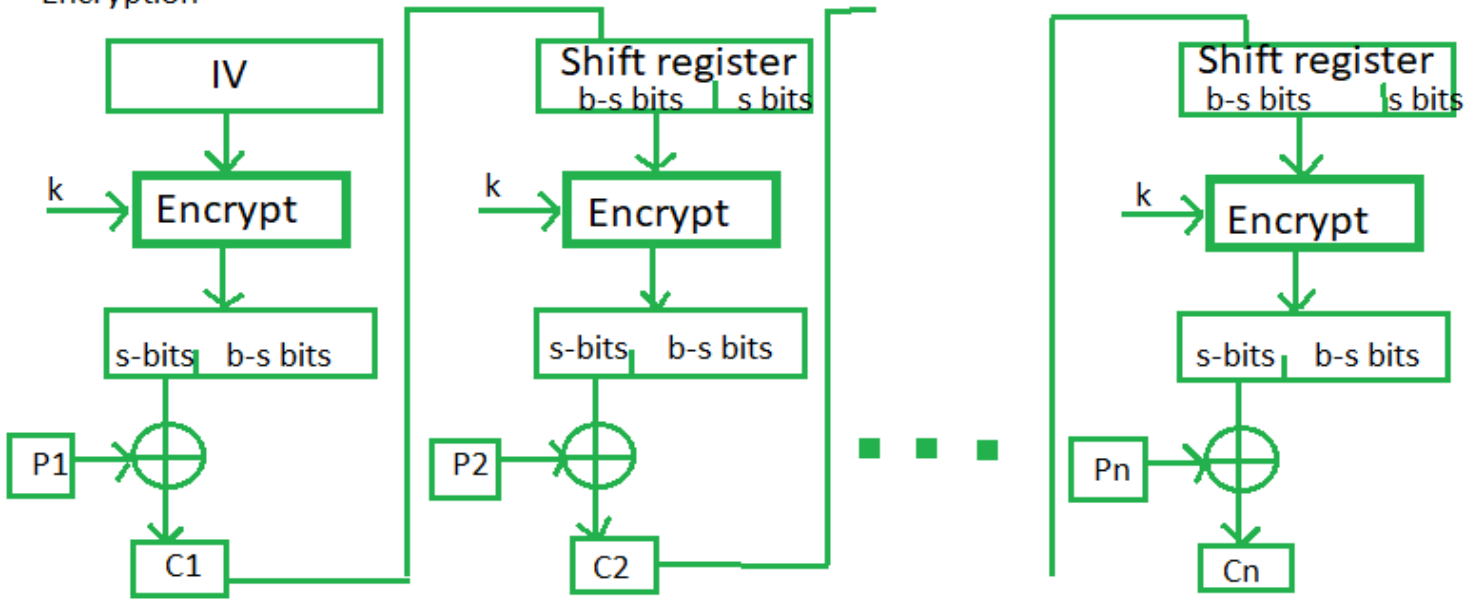
Disadvantages of CBC –

Parallel encryption is not possible since every encryption requires a previous cipher.

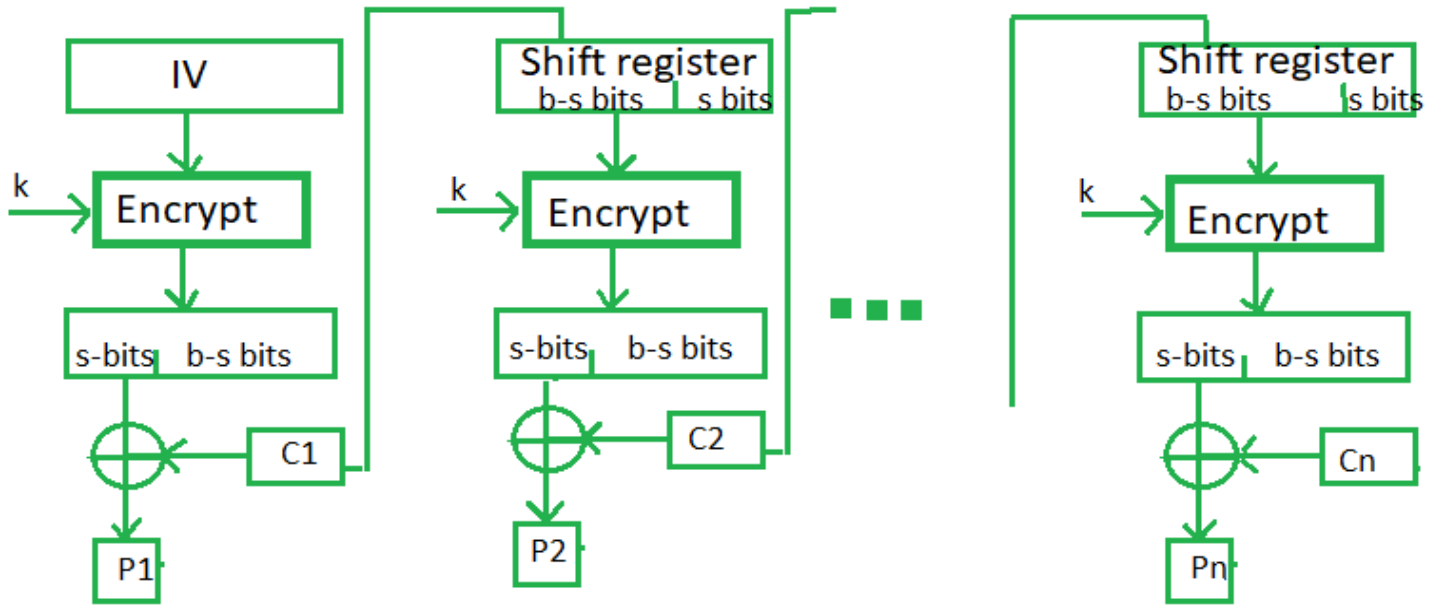
Cipher Feedback Mode (CFB)

In this mode the cipher is given as feedback to the next block of encryption with some new specifications: first, an initial vector IV is used for first encryption and output bits are divided as a set of *s* and *b-s* bits. The left-hand side *s* bits are selected along with plaintext bits to which an XOR operation is applied. The result is given as input to a shift register having b-s bits to lhs, s bits to rhs and the process continues. The encryption and decryption process for the same is shown below, both of them use encryption algorithms.

Encryption



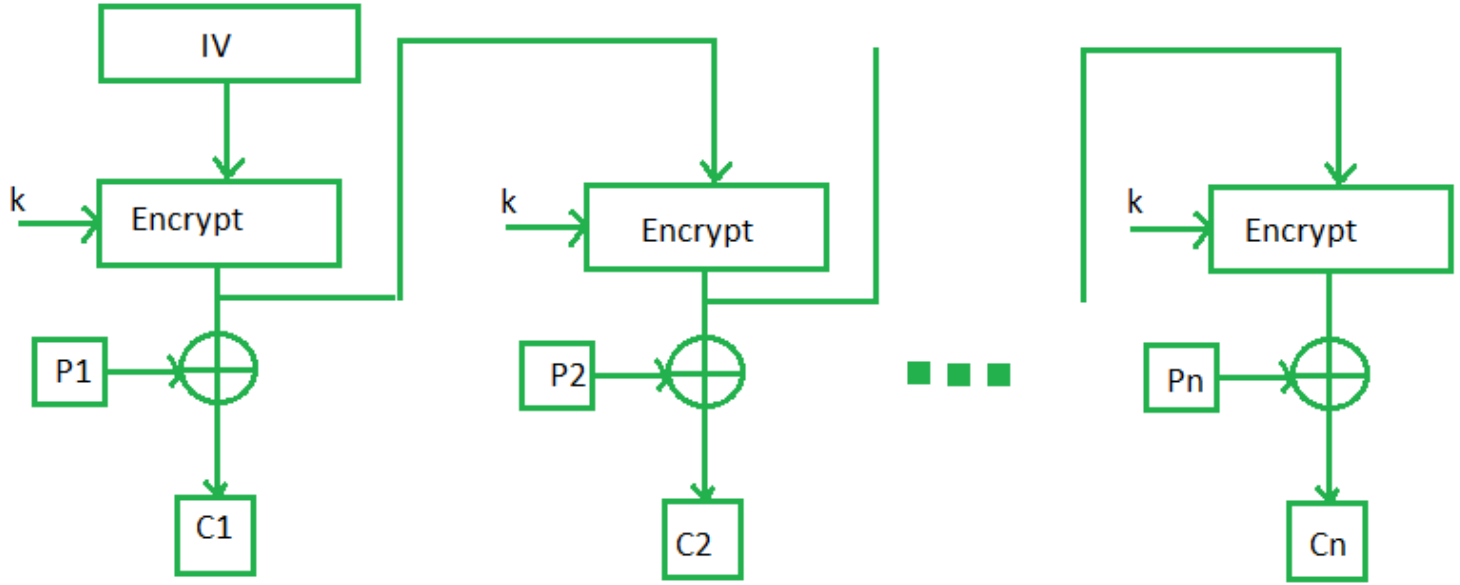
Decryption



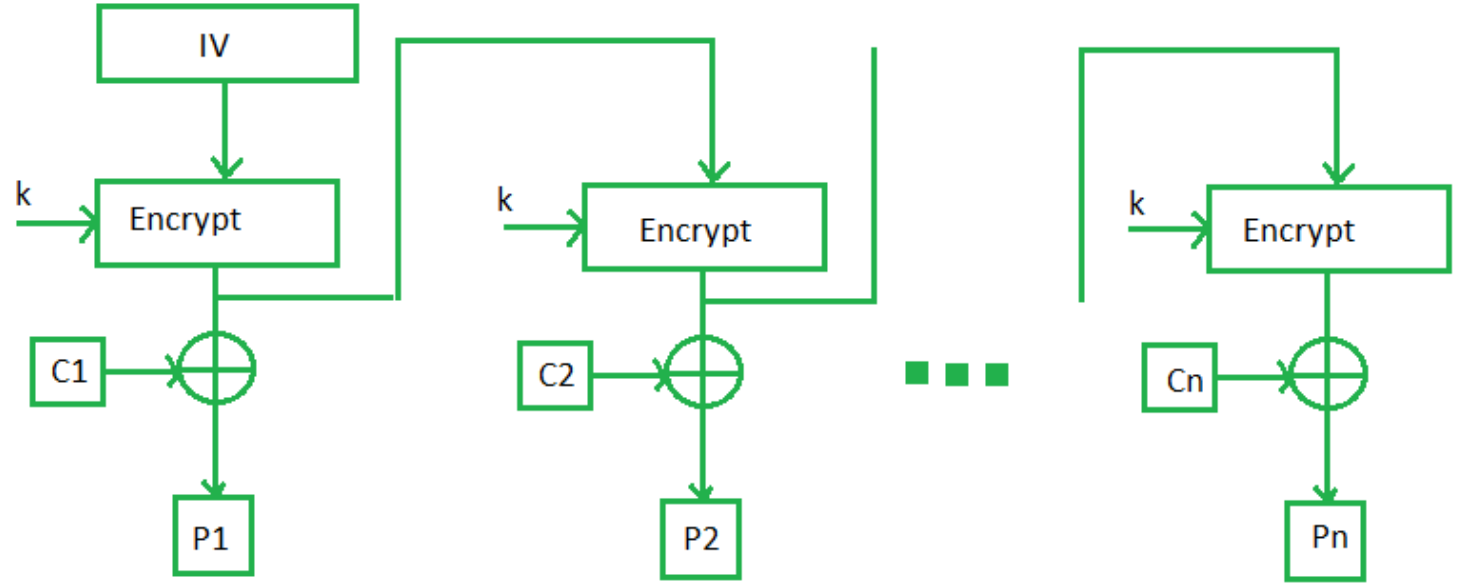
Output Feedback Mode

The output feedback mode follows nearly the same process as the Cipher Feedback mode except that it sends the encrypted output as feedback instead of the actual cipher which is XOR output. In this output feedback mode, all bits of the block are sent instead of sending selected *s* bits. The Output Feedback mode of block cipher holds great resistance towards bit transmission errors. It also decreases the dependency or relationship of the cipher on the plaintext.

Encryption



Decryption



Advantages of OFB

In the case of CFB, a single bit error in a block is propagated to all subsequent blocks. This problem is solved by OFB as it is free from bit errors in the plaintext block.

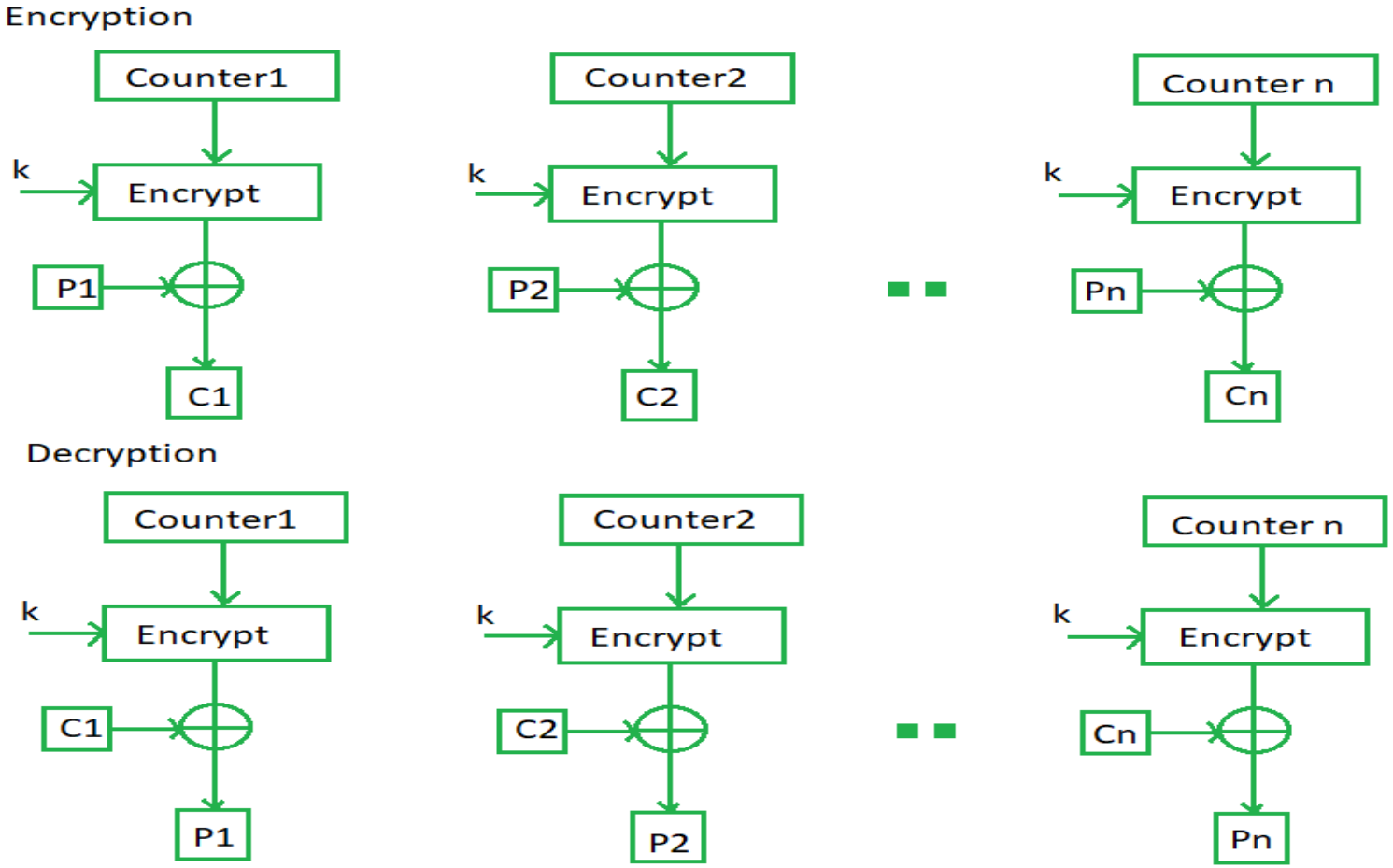
Disadvantages of OFB

The drawback of OFB is that, because to its operational modes, it is more susceptible to a message stream modification attack than CFB.

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.

Its simple implementation is shown below:



Advantages of Counter

Since there is a different counter value for each block, the direct plaintext and ciphertext relationship is avoided. This means that the same plain text can map to different ciphertext.
Parallel execution of encryption is possible as outputs from previous stages are not chained as in the case of CBC.

Disadvantages of Counter

The fact that CTR mode requires a synchronous counter at both the transmitter and the receiver is a severe drawback. The recovery of plaintext is erroneous when synchronisation is lost.

Applications of Block Ciphers

1.Data Encryption: Block Ciphers are widely used for the encryption of private and sensitive data such as passwords, credit card details and other information that is transmitted or stored for a communication. This encryption process converts a plain data into non-readable and complex form. Encrypted data can be decrypted only by the authorised person with the private keys.

2.File and Disk Encryption: Block Ciphers are used for encryption of entire files and disks in order to protect their contents and restrict from unauthorised users. The disk encryption softwares such as BitLocker, TrueCrypt aslo uses block cipher to encrypt data and make it secure.

3.Virtual Private Networks (VPN): Virtual Private Networks (VPN) use block cipher for the encryption of data that is being transmitted between the two communicating devices over the internet. This process makes sure that data is not accessed by unauthorised person when it is being transmitted to another user.

4.Secure Sockets Layer (SSL) and Transport Layer Security (TLS): SSL and TLS protocols use block ciphers for encryption of data that is transmitted between web browsers and servers over the internet. This encryption process provides security to confidential data such as login credentials, card information etc.

5.Digital Signatures: Block ciphers are used in the digital signature algorithms, to provide authenticity and integrity to the digital documents. This encryption process generates the unique signature for each document that is used for verifying the authenticity and detecting if any malicious activity is detected.