**NAME:** Aditya Jethani

**ROLL NO:** 21BCP166

**DIV-3 G-5**

**INFORMATION SECURITY ASSIGNMENT**

**TOPIC:** Comparative study of merits and demerits of 5 block cipher modes of operations

**Introduction:**

**What is a block cipher?**

A block cipher is a method of encrypting data in blocks to produce ciphertext using a cryptographic key and algorithm. The block cipher processes fixed-size blocks simultaneously, as opposed to a stream cipher, which encrypts data one bit at a time.

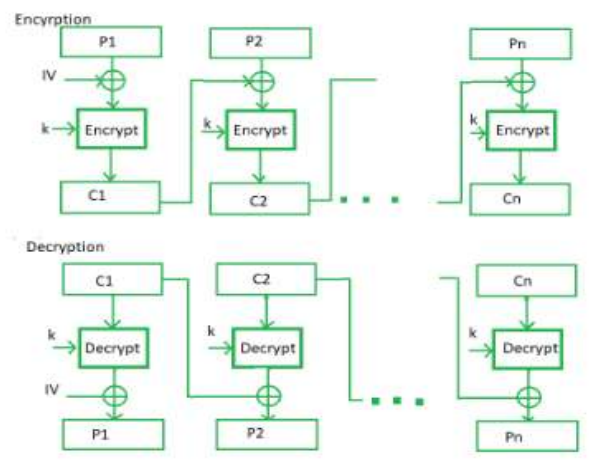
**What are the different modes of operation in block cipher?**

Block ciphers only encrypt messages that are the same size as their block length, so each block of plaintext with more or less blocks needs to be encrypted separately. The following block cipher modes of operation define how these blocks are encrypted:

1. **Electronic codebook (**[**ECB**](https://www.techtarget.com/searchsecurity/definition/Electronic-Code-Book)**) mode**
2. **Cipher block chaining (**[**CBC**](https://www.techtarget.com/searchsecurity/definition/cipher-block-chaining)**) mode**
3. **Ciphertext feedback (**[**CFB**](https://www.techtarget.com/searchsecurity/definition/ciphertext-feedback)**) mode**
4. **Output feedback (OFB) mode**
5. **Counter (CTR) mode**

**ELECTRONIC CODE BOOK MODE:**

* **ECB mode is used to electronically code messages as their plaintext form.**
* **It is the simplest of all block cipher modes of operation. It does not add any randomness to the key stream, and it is the only mode that can be used to encrypt a single-bit stream.**
* **This means that each plaintext symbol, such as a character from the plaintext alphabet, is converted into a ciphertext symbol using the cipher's key and a substitution alphabet.**

****

**Advantages of ECB:**

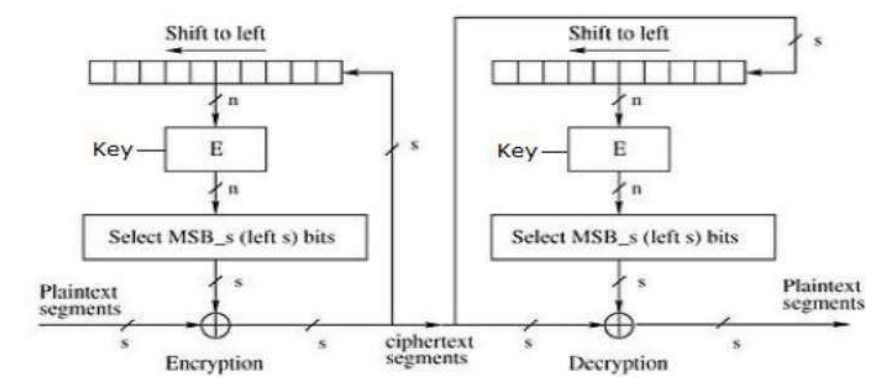
1. The most obvious advantage of using the ECB mode is how simplistic it is.
2. ECB can tolerate the loss of blocks without affecting other available blocks.
3. Parallel encryption of bits is possible making the process faster.

**Disadvantages of ECB:**

1. Vulnerability to certain types of attacks due to the deterministic nature of the encryption.
2. Identical plaintexst blocks result in identical ciphertext blocks, making it easier for attackers to identify patterns in the encrypted data.

**CIPHER BLOCK CHAINING:**

* CBC mode is a method of encrypting data that ensures that each block of plaintext is combined with the previous ciphertext block before being encrypted.
* The symmetric key algorithm creates a ciphertext that depends on all plaintext blocks processed before it in a data stream. This is done to ensure that each block of the ciphertext is dependent on all of the previous blocks.
* Each plaintext block is XOR-ed (exclusive OR) with the previous ciphertext block before being encrypted with the cipher algorithm.
* CBC mode is used in a variety of security applications. For example, Secure Sockets Layer/Transport Layer Security uses CBC mode to encrypt data that is transferred over the internet.



**ADVANTAGES OF CBC:**

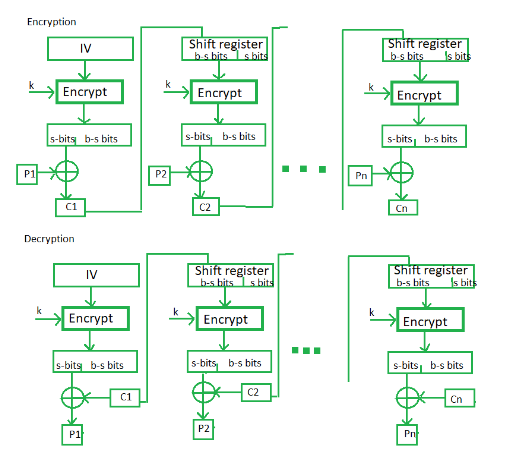
1. CBC has the advantage over the ECB mode in that the XORing process hides plaintext patterns.
2. CBC is resilient to tampering with the ciphertext. Altering a single ciphertext block affects not only that block but also the decryption of subsequent blocks, making it easier to detect unauthorized changes in the data.
3. CBC is widely supported and used in various cryptographic protocols, making it a practical choice for many encryption applications.

**DISADVANTAGE OF CBC:**

1. Both block losses and concurrent encryption of several blocks are not supported by the encryption.
2. In CBC mode, each ciphertext block depends on the previous one. If a single block is lost or corrupted during transmission, it can lead to a cascade effect, rendering the decryption of subsequent blocks incorrect.
3. Using strong encryption algorithms like AES-256 in CBC mode can have a performance impact due to the high level of encryption.

**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.



**ADVANTAGE OF CFB:**

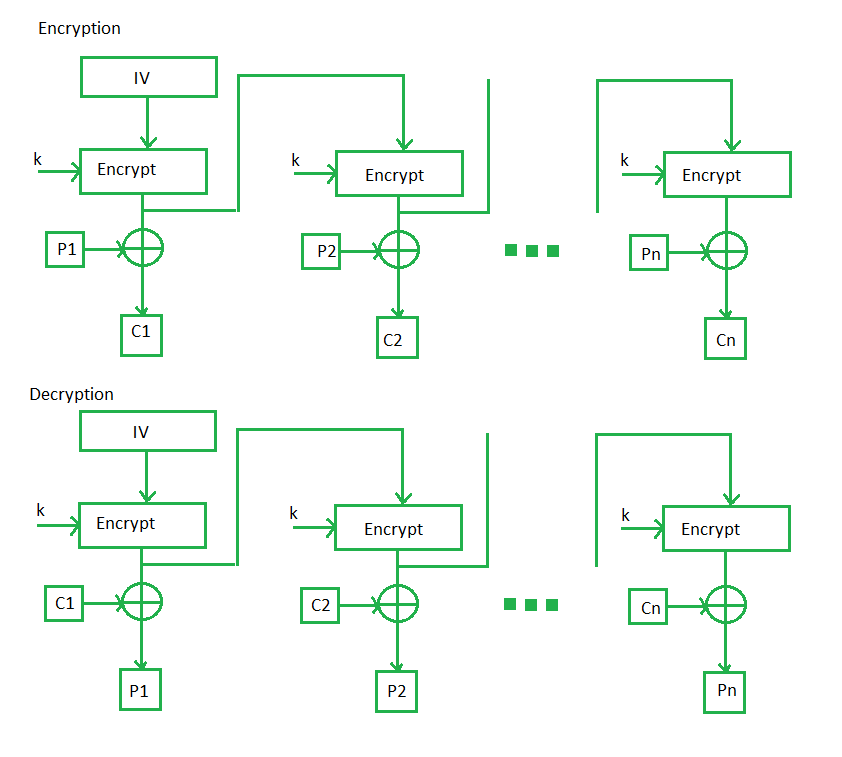
1. It doesn't use a decryption algorithm, it is generally faster than the CBC mode.
2. CFB mode encrypts data in smaller units (usually bits or bytes) rather than entire blocks, making it suitable for encrypting data of varying lengths.
3. Unlike some other modes, CFB mode limits the propagation of errors. If an error occurs in one block, it generally affects only that block, reducing the risk of widespread data corruption.

**DISADVANTAGE OF CFB:**

1. The encryption cannot tolerate block losses, nor can multiple blocks be encrypted in parallel.
2. CFB mode is more complex than some other modes like Electronic Codebook (ECB) mode, which can make it harder to implement correctly and securely.

**OUTPUT FEEDBACK MODE:**

* OFB mode can be used with any block cipher and is similar in some respects to CBC mode.
* It uses a feedback mechanism, but instead of XORing the previous block of ciphertext with the plaintext before encryption, in OFB mode, the previous block of ciphertext is XORed with the plaintext after it is encrypted.
* 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.



**ADVANTAGES OF OFB:**

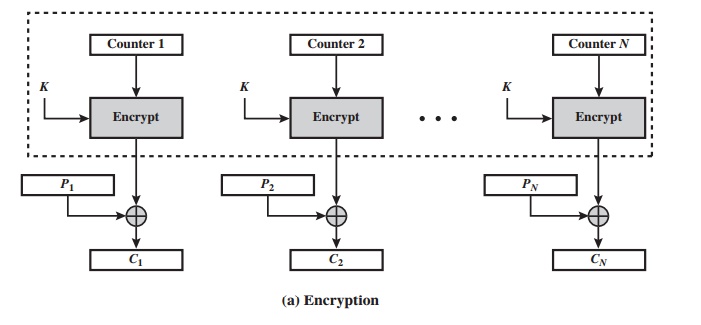
1. In the case of CFB, a single bit error in a block is propagated to all subsequent blocks. This problem is solved by OFB as it is free from bit errors in the plaintext block.
2. Holds great resistance towards bit transmission errors.
3. One significant advantage of OFB is its ability to isolate errors. Bit errors that occur during data transmission do not propagate through the encryption.

**DISADVANTAGE OF OFB:**

1. The disadvantage of OFB is that it is more vulnerable to a message stream modification attack than is CFB in the modes of operation.
2. OFB doesn't have interdependency between blocks, which means the encryption of one block doesn't depend on the previous block's ciphertext.

**COUNTER MODE:**

* CTR mode uses a block chaining mode of encryption as a building block.
* The process of encrypting data is performed by XORing the plaintext with a sequence of [pseudorandom](https://www.techtarget.com/whatis/definition/pseudo-random-number-generator-PRNG) values, each of which is generated from the ciphertext using a feedback function.
* The CTR encryption process can be visualized as a series of XORs between blocks of plaintext and corresponding blocks of ciphertext.



**ADVANTAGES OF CTR:**

1. The Counter Mode component provides data privacy, while CBC-MAC provides data integrity and authentication.
2. CTR mode is known for its efficiency. It doesn't require complex mathematical operations like some other modes, making it faster and less resource intensive.
3. CTR mode is independent of feedback use, allowing for parallel encryption and decryption processes. This means that multiple blocks of data can be encrypted or decrypted simultaneously, enhancing processing speed and efficiency.

**DISADVANTAGE OF CTR:**

1. The serious disadvantage of CTR mode is that it requires a synchronous counter at sender and receiver.
2. Loss of synchronization leads to incorrect recovery of plaintext.
3. One of the significant disadvantages of CTR mode is that it lacks built-in integrity and authentication mechanisms.