Report on different of Blocks Cipher Modes of Operation

Submitted To

Dr. Md. Shariful Islam

Professor

Institute of Information Technology

University of Dhaka

Submitted by

Amran Hossain

BSSE 0917

Date:27-12-2020

Institute of Information Technology

University of Dhaka

Contents

Block Cipher Modes of Operation

Introduction:

Encryption algorithms are divided into two categories based on input type, as block cipher and stream cipher. Block cipher is an encryption algorithm which takes fixed size of input say *b* bits and produces a ciphertext of *b* bits again. If input is larger than *b* bits it can be divided further. A block cipher processes the data blocks of fixed size. Usually, the size of a message is larger than the block size. Hence, the long message is divided into a series of sequential message blocks, and the cipher operates on these blocks one at a time.

Types of Modes of Operation:

For different applications and uses, there are several modes of operations for a block cipher These are:

1. Electronic Code Book (ECB)
2. Cipher Block Chaining (CBC)
3. Cipher Feedback Mode (CFB)
4. Output Feedback Mode (OFB)
5. Counter Mode (CTR)
6. XTS-AES

Electronic Code Book (ECB)

Electronic code book is the easiest block cipher mode of functioning. It is easier because of direct encryption of each block of input plaintext and output is in form of blocks of encrypted ciphertext.

Working Principle:

- The user takes the first block of plaintext and encrypts it with the key to produce the first block of ciphertext.
- He then takes the second block of plaintext and follows the same process with same key and so on so forth.
- The ECB mode is deterministic, that is, if plaintext block P1, P2…, Pn are encrypted twice under the same key, the output ciphertext blocks will be the same.
  In fact, for a given key technically we can create a codebook of ciphertexts for all possible plaintext blocks. Encryption would then entail only looking up for required plaintext and select the corresponding ciphertext. Thus, the operation is analogous to the assignment of

code words in a codebook, and hence gets an official name − Electronic Codebook mode of operation (ECB).

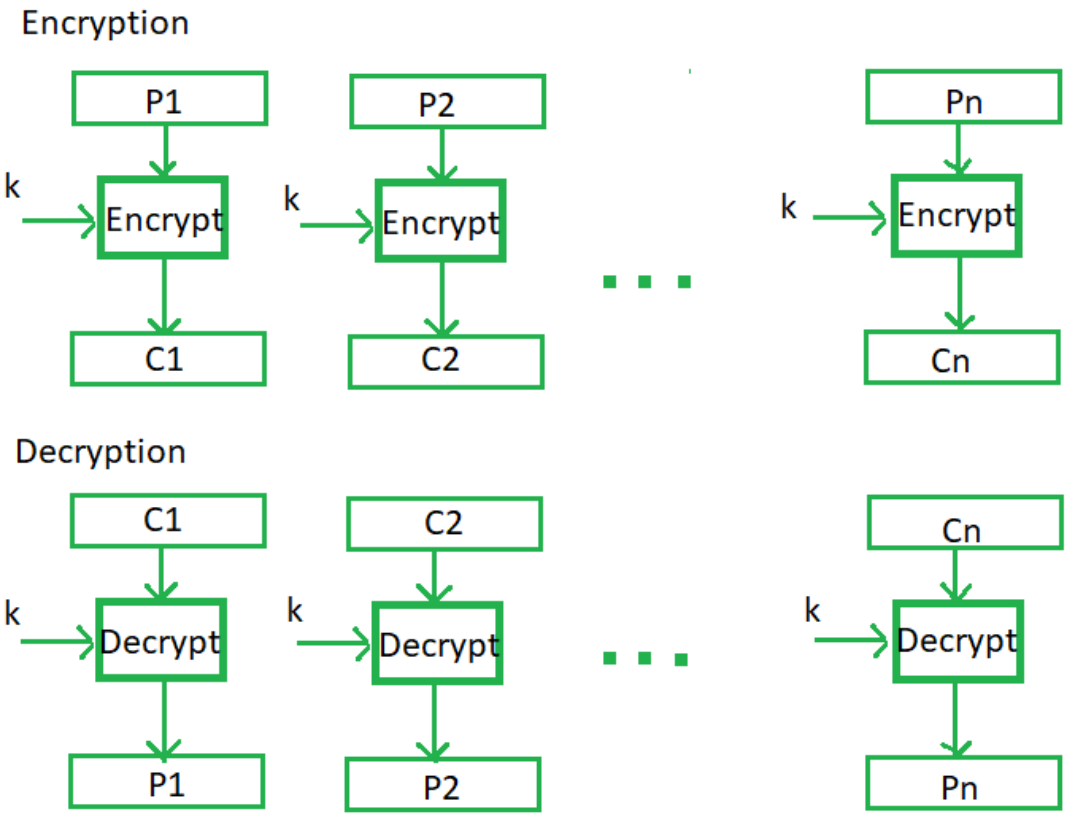

Figure 1: ECB procedure

Advantages

- Parallel encryption of blocks of bits is possible, thus it is a faster way of encryption.
- Simple way of block cipher.

Disadvantages

- Prone to cryptanalysis since there is a direct relationship between plaintext and ciphertext.
- A ciphertext from ECB can allow an attacker to guess the plaintext by trial-and-error if the plaintext message is within predictable.

Application

ECB may also leave plaintext patterns evident in the resulting ciphertext. Bitmap image data encrypted with a key of “Kowalski” using 56-bit DES ECB mode shows obvious patterns.

Cipher Block Chaining (CBC)

Cipher block chaining or CBC is an advancement made on ECB since ECB compromises some security requirements. CBC mode of operation provides message dependence for generating ciphertext and makes the system non-deterministic.

Working Principle:

- Load the n-bit Initialization Vector (IV) in the top register.
- XOR the n-bit plaintext block with data value in top register.
- Encrypt the result of XOR operation with underlying block cipher with key K.
- Feed ciphertext block into top register and continue the operation till all plaintext blocks are processed.
- For decryption, IV data is XORed with first ciphertext block decrypted. The first ciphertext block is also fed into to register replacing IV for decrypting next ciphertext block.

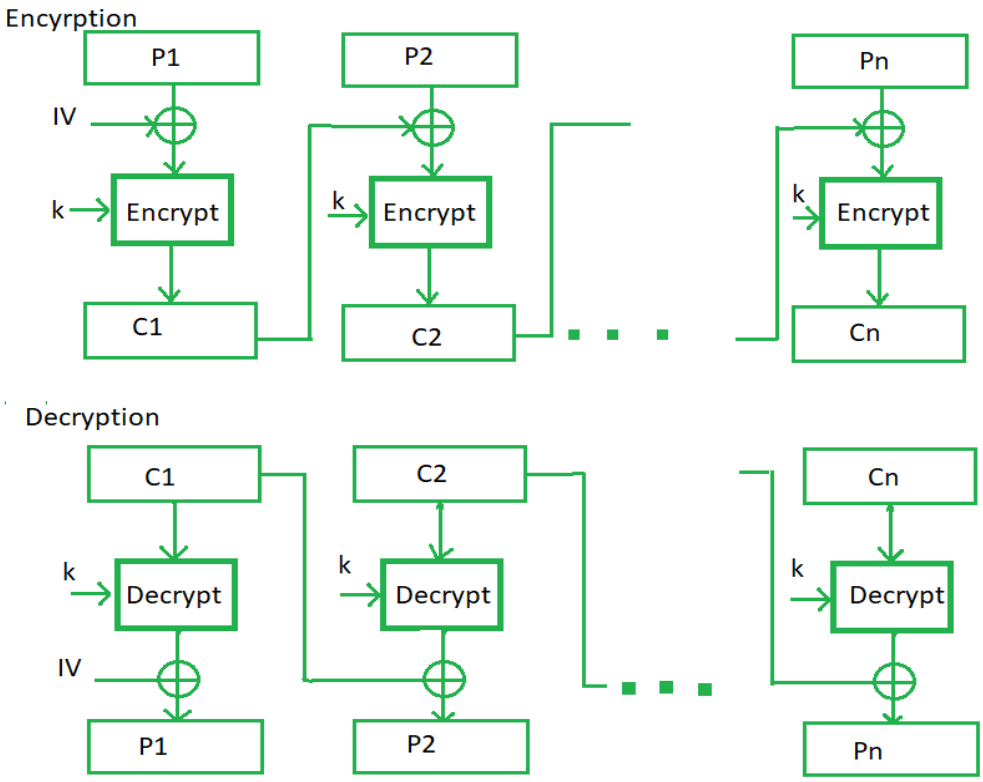

Figure 2: CBC Procedure

Advantages:

- CBC works well for input greater than *b* bits.
- CBC is a good authentication mechanism.
- Better resistive nature towards cryptanalysis than ECB.

Disadvantages:

- Parallel encryption is not possible since every encryption requires previous cipher.
- The error in transmission gets propagated to few further block during decryption due to chaining effect.

Application:

In wireless sensor network we may use this mode. In this model, commands are communicated between new nodes and clusters. Bulk data encryption, authentication.

Cipher Feedback Mode (CFB)

In this mode the cipher is given as feedback to the next block of encryption with some new specifications:

Working Principle

The operation of CFB mode is depicted in the following illustration. For example, in the present system, a message block has a size 's' bit where $1 < s < n$. The CFB mode requires an initialization vector (IV) as the initial random n-bit input block. The IV need not be secret. Steps of operation are −

- Load the IV in the top register.
- Encrypt the data value in top register with underlying block cipher with key K.
- Take only 's' number of most significant bits (left bits) of output of encryption process and XOR them with 's' bit plaintext message block to generate ciphertext block.
- Feed ciphertext block into top register by shifting already present data to the left and continue the operation till all plaintext blocks are processed.
- Essentially, the previous ciphertext block is encrypted with the key, and then the result is XORed to the current plaintext block.
- Similar steps are followed for decryption. Pre-decided IV is initially loaded at the start of decryption.

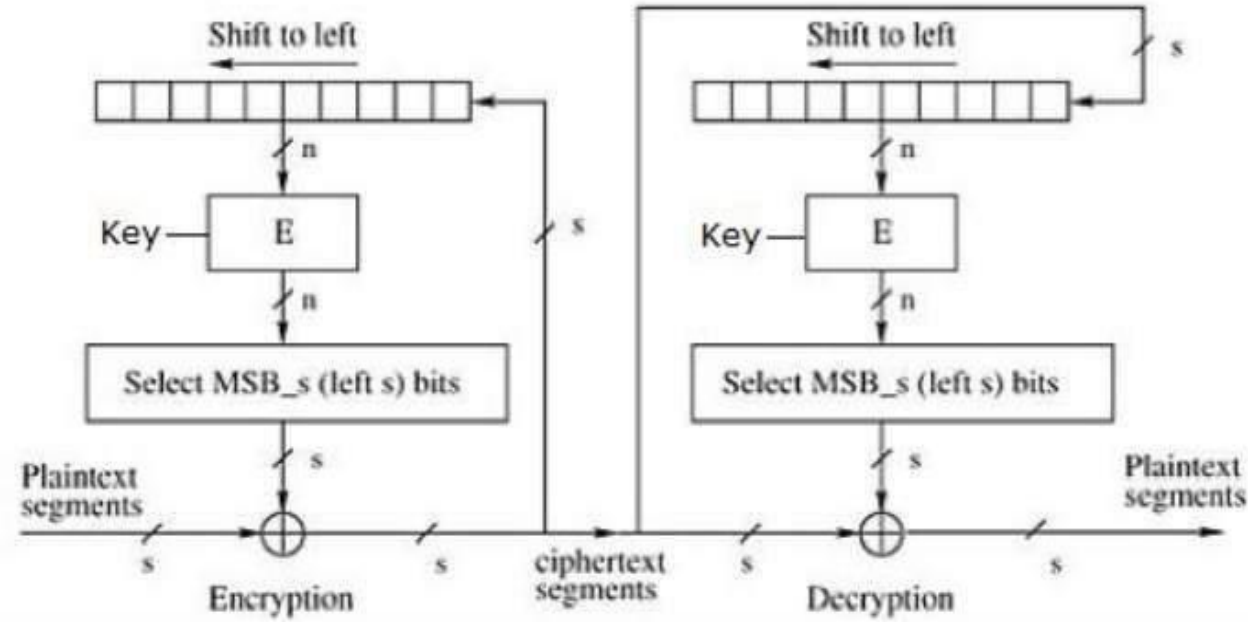

Figure 3: CFB procedure

Advantages:

- Since, there is some data loss due to use of shift register, thus it is difficult for applying cryptanalysis.

- CFB mode is converting a block cipher into a type of stream cipher. The encryption algorithm is used as a key-stream generator to produce key-stream that is placed in the bottom register. This key stream is then XORed with the plaintext as in case of stream cipher.

Disadvantages:

- The error of transmission gets propagated due to changing of blocks.

Application

The entropy calculation can be implemented as a stream cipher. In fact, CFB is primarily a mode to derive some characteristics of a stream cipher from a block cipher. Authentication.

Output Feedback Mode (OFB)

The output feedback mode follows nearly 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.

Working principle

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 dependency or relationship of cipher on plaintext.

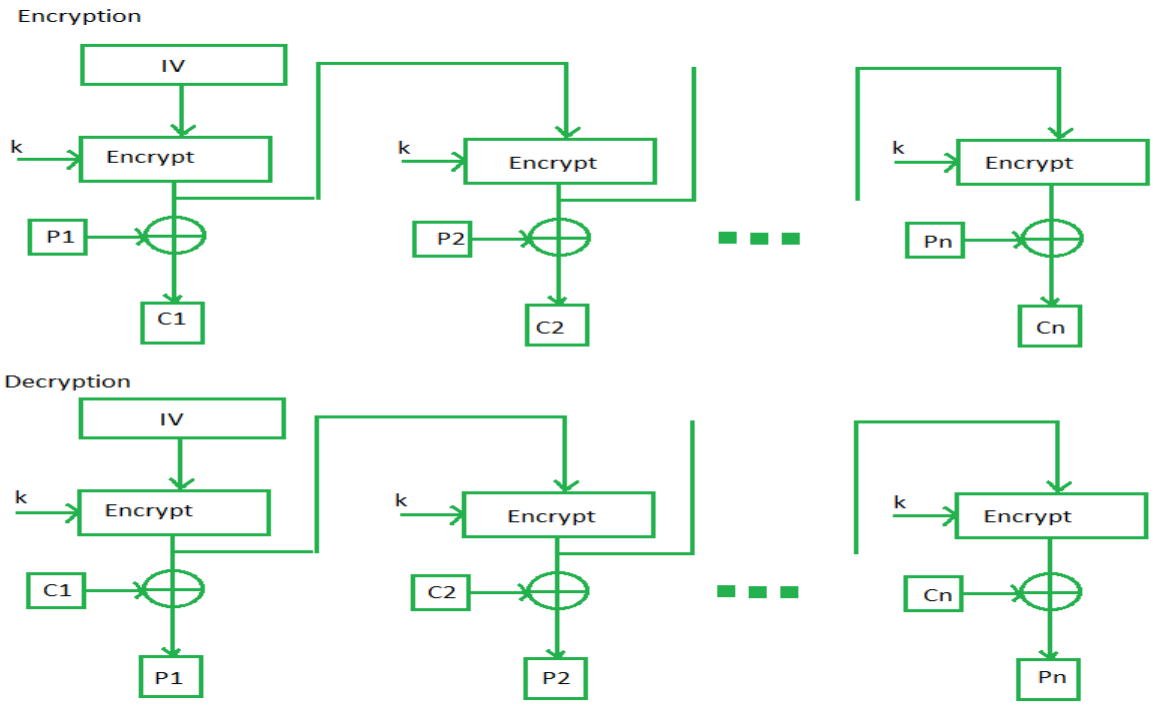

Figure 4: OFB procedure

Advantages

- The main advantage of the OFB method is that bit errors in transmission do not propagate in the encryption.
- For example, if as a bit error occurs in C1 as ciphertext, only the recovered value of P1 as plaintext is affected; subsequent plaintext units are not corrupted. With CFB, C1 as ciphertext also serves as input to the shift register and therefore causes additional corruption downstream in this mode.

Disadvantages

- The disadvantage of OFB is that it is more vulnerable to a message stream modification attack than is CFB in the modes of operation.

Application

Stream encryption on noisy channels.

Counter Mode (CTR)

The Counter Mode or CTR is a simple counter-based block cipher implementation. In this mode, both the sender and receiver need to access to a reliable counter, which computes a new shared value each time a ciphertext block is exchanged. This shared counter is not necessarily a secret value, but challenge is that both sides must keep the counter synchronized.

Working Principle

Both encryption and decryption in CTR mode are depicted in the following illustration. Steps in operation are −

- Load the initial counter value in the top register is the same for both the sender and the receiver. It plays the same role as the IV in CFB (and CBC) mode.
- Encrypt the contents of the counter with the key and place the result in the bottom register.
- Take the first plaintext block P1 and XOR this to the contents of the bottom register. The result of this is C1. Send C1 to the receiver and update the counter. The counter update replaces the ciphertext feedback in CFB mode.
- Continue in this manner until the last plaintext block has been encrypted.
- The decryption is the reverse process. The ciphertext block is XORed with the output of encrypted contents of counter value. After decryption of each ciphertext block counter is updated as in case of encryption.

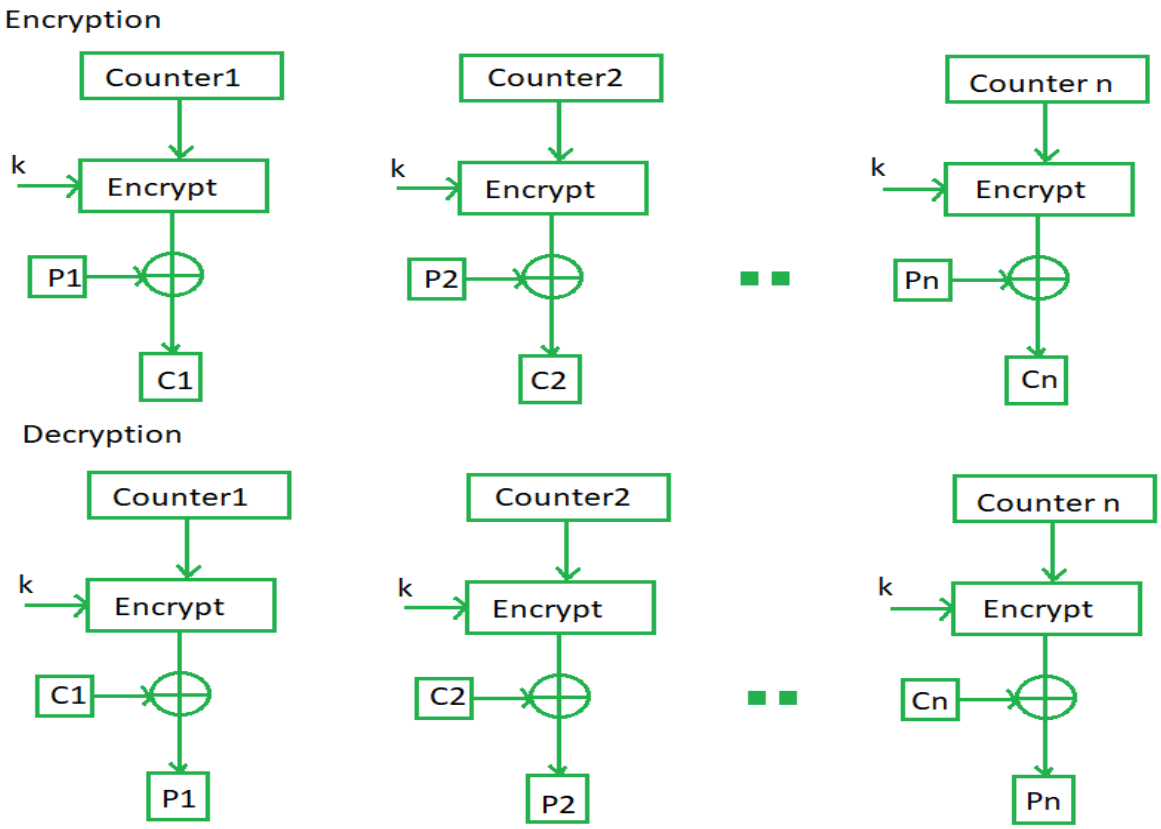

Figure 5: CTR procedure

Advantages

It does not have message dependency and hence a ciphertext block does not depend on the previous plaintext blocks.

Like CFB mode, CTR mode does not involve the decryption process of the block cipher. This is because the CTR mode is really using the block cipher to generate a key-stream, which is encrypted using the XOR function. In other words, CTR mode also converts a block cipher to a stream cipher.

Disadvantages

The serious disadvantage of CTR mode is that it requires a synchronous counter at sender and receiver. Loss of synchronization leads to incorrect recovery of plaintext.

Application

High speed network encryption.

XTS-AES

It is the newest block cipher mode and is the cipher mode used by Data Traveler 4000G2 and Data Traveler Vault Privacy 3.0. It is designed as a stronger alternative to other block cipher models.

Working Principle

XTS uses two AES keys. One Key is used to performed the AES block encryption; the other is used to encrypt what is known as “Tweak value”. This encrypted tweak is further modified with Galois polynomial function and XOR with both the plain text and the cipher text of each block. The GF function provides further diffusion and ensures that blocks of identical data will not produce identical cipher text. This achieves the goal of each block producing unique cipher text given identical plain text without the use of initializing vectors and chaining. In fact, the text is almost double encrypted using two independent keys. Decryption of the data is accomplished by reversing this process. Since each block is independent and there is no chaining, if the stored cipher data is damaged and becomes corrupted, only the data for that particular block will be unrecoverable. With the chaining modes, these errors can propagate to other blocks when decrypted.

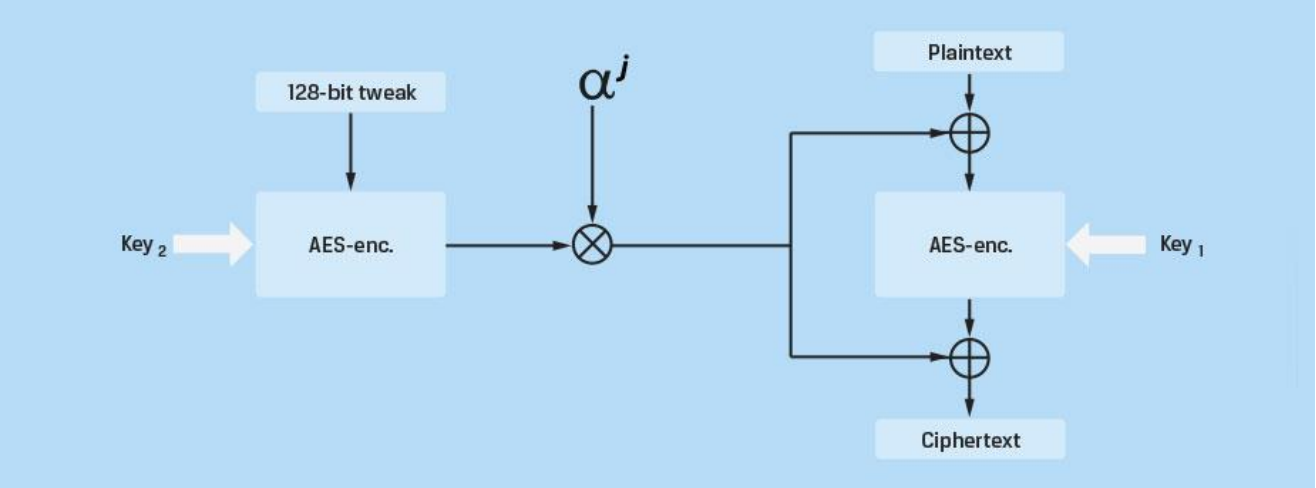

Figure 6: XTS-AES procedure

Advantages

It is stronger than any other modes. It eliminates potential vulnerabilities associated with some of the more sophisticated side channel attacks that could be used to exploit weaknesses within over modes.

Disadvantages

Error can be propagated to other blocks when decrypted.

Application

Validation system. Sophisticated HDL Testbench(self-checking) and test vector generator.

References

1. https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
2. https://en.wikipedia.org/wiki/Disk_encryption_theory
3. https://www.cast-inc.com/security/encryption-primitives/aes-xts/
4. https://www.tutorialspoint.com/cryptography/block_cipher_modes_of_operation.htm
5. https://www.geeksforgeeks.org/block-cipher-modes-of-operation/
6. https://www.sciencedirect.com/topics/computer-science/electronic-code-book