A Pros and Cons of Block Cipher Modes for Symmetric Key Algorithms

Prashant P. Pittalia

Abstract— **Symmetric encryption algorithms must be used with the cipher block mode operation in real applications. The cipher block mode chosen is influenced by security and performance of the mode. This paper discusses ECB (Electronic Codebook), CBC (Cipher Block Chaining), CFB (Cipher FeedBack), OFB (Output FeedBack) and CTR (Counter) cipher modes. To provide security and proper implementation of symmetric key algorithms cipher modes are more important. This paper describes the details of cipher modes operation, their parameters as well as their strengths and weaknesses. The Counter mode of operation has been found generally superior to the other four modes of operation in terms of performance especially when increasing the input size.**

Index Terms— **AES, Cipher Mode, Encryption, Symmetric Key Algorithm**

I. INTRODUCTION

The block ciphers are schemes for encryption or decryption where a block of plaintext is treated as a single block and is used to obtain a block of cipher text with the same size [1]. In symmetric key cryptography the sender uses the key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. In Symmetric key encryption/decryption, the algorithm used for decryption is the inverse of the algorithm used for encryption. This means that if the encryption algorithm uses a combination of addition and multiplication, the decryption algorithm uses a combination of division and subtraction. Symmetric key encryption schemes are very important for bulk data encryption. The symmetric key encryption algorithms like DES, Triple DES, IDEA, AES and Blowfish Today, In symmetric key algorithms, AES (Advanced Encryption Standard) is one of the most used algorithms for block encryption. Earlier to AES, DES (Data Encryption Standard),

3-DEC (Triple Data Encryption Standard) was used for encryption and decryption of the information. Data Encryption Standard maps a 64-bit data block into the same block length using the key split over multiple rounds. Tripple DES uses the DES cipher three times to overcome the shortcomings associated with the shorter keys of simple DES. The basic form of 3DES is DES (k3; DES (k2, DES (k1, M))) where M is the message and k1, K2, k3 are the keys. It can be made interoperable with simple DES by making k1 = k2 = k3 = k and replacing the middle DES encryption operation with decryption operation DES (k3, DES-1(k2, DES (k1, M))). The choice of the keys k1, K2 and k3 greatly changes the amount of security offered by 3DES; for example if k1=k2 then it is equivalent to 112 bits key length but if all three keys are different then it provides maximum security of the key length 168 bits. IDEA uses 8.5 rounds with a key length of 128 bits. Also it uses same block length of 64 bits. 3DES is equivalent to IDEA but their architectures are very different. 3DES uses a Feistel network while IDEA uses a substitution-permutation network.

AES (Advanced Encryption Standard) is a standard adopted by the US Government for data with extremely high security requirements. The cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen and submitted to the AES selection process with the name of "Rijndael", a portmanteau of the names of the creators. . It consist of 10, 12 or 14 rounds depending on the key length 128, 192 or 256 bits. The block length of the plain text is 128 bits. In fact, the block length may be any multiple of 32 bits not less than 128 and not more than 256 bits. The algorithm consists of four steps, namely ByteSub Transformation (BS), ShiftRow Transformation (SR), MixColumn Transformation and AddRoundKey. The key lengths with respective rounds are very much sufficient for known attacks to the date.

II. BLOCK CIPHER MODES

In Block cipher is an encryption algorithm which takes fixed size of input and fixed size of output. The N bits as input and N bit as output. If input is larger than N bits it can be divided further. There are several modes of operations for a block cipher for different applications and uses. A mode of operation describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block [2].

Some cipher modes require a unique binary sequence that is called an initialization vector (IV), for each encryption operation. The initialization vector has to be non-repeating and random. The initialization vector is used to ensure distinct cipher texts are produced even when the same plaintext is encrypted multiple times independently with the same key.[3] Block ciphers may be capable of operating on more than one block size, but during transformation the block size is always fixed. Block cipher modes operate on whole blocks and require that the last part of the data be padded to a full block if it is smaller than the current block size. [4]

A. ECB Mode of Operation

The ECB (Electronic Code Book) mode of operation is presented in Fig. 1.The plaintext message is divided in blocks called P1, P2, PN and each block is encrypted separately with the same key (K). The output of the encryption is the cipher text as C1, C2 and CN respectively. If the size of the message is larger than n blocks, the last block is filled with padding.

Manuscript received June 21, 2019

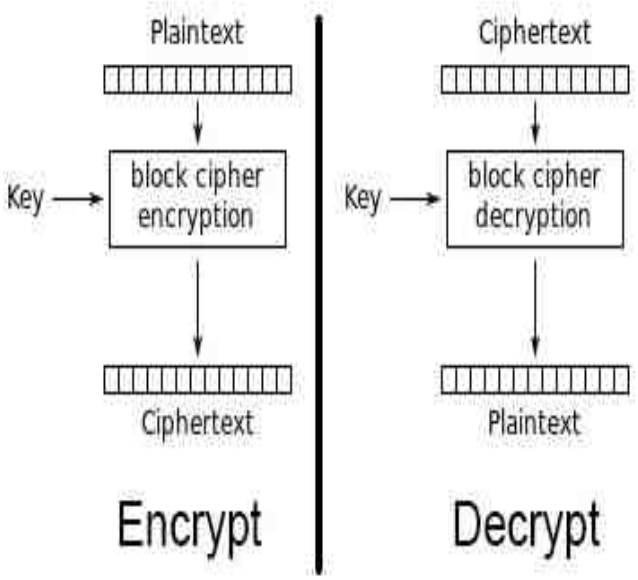

Fig -1: Electronic Code Book Mode [5]

In this mode, if any one block is affected during the transmission it could not affect the other blocks. But if the same plain text P is used the output cipher text C is also the same. During the transmission of the cipher text blocks, if attacker exchange the blocks, it is very difficult to find out such attacks. E.g., if in the plaintext every 4th block is store the value of salary. If attacker comes to know about the block positions and if it just swap the cipher text blocks at the position in multiple of 4, the salary data is affected and at the same time the payroll calculation will be affected. This mode is recommended only for the block size = 1. The advantage of this mode is that all the blocks are independent. It means that the each block is encrypted separately and decrypted separately. During transmission if any cipher block is affected with the errors than it could affect only that block, other blocks can easily converted into original plain text. In this mode protection against deletion or addition of block

B. CBC Mode of Operation

In this CBC (Cipher Block Chaining) mode operation, if the plaintext input P is same at multiple places than the output cipher text C is also different. Here the initialization vector – IV is used. Its size is same as block size. As a start of operation plaintext block P1 is XOR with the IV, then the resultant output is encrypted with the key K and get the final output C1. Here the result of encryption of previous block is XOR with the next plain text block. As a result for the same plaintext, encrypted output is totally different. In this mode both sender and receiver must know the value if initialization vector (IV). If it is sent in clear text attacker may change a bit or bytes init to do malicious task. The better way is that to send IV encrypted with the Electronic code book mode and send to the other side.

Every time the new IV is used if the same message encrypted again and again output is different. Here the same key is used for each encryption block. If one of the cipher text block is affected with the error than all the subsequent blocks are wrong.

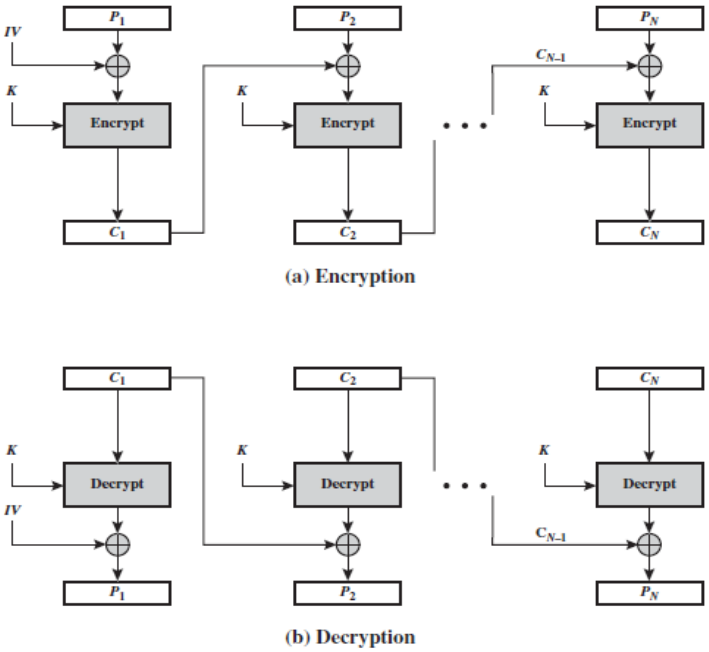

Fig -2: Cipher Block Chaining Mode [6]

C. CFB Mode of Operation

In CFB (Cipher FeedBack) mode of operation used the stream cipher to encrypt the block.

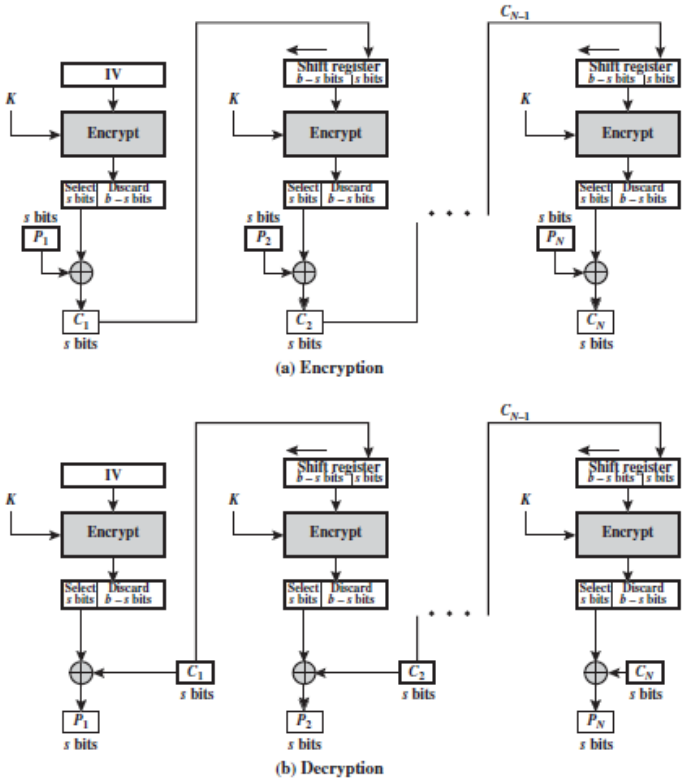

Fig -3: Cipher Feedback Mode [6]

It starts with encrypting the initialization vector (IV) is encrypted with the key K. After that, the output is XOR with the first plain text block P1For all subsequent operation, the previous block output C1, C2,....Cn-1is encrypted with the key K and that cipher text is XOR with the plaintext block P2.... PN. Initilization vector (IV) is kept in the shift register of size 64 bits. When the IV is encrypted with key K, the output is again 64 bits. Only few bits (s = 8 bits) of the encrypted IV is XOR with the plain text block P1 with size of

(s = 8 bits). The least significant bits (s = 8 bits) from the IV are discarded. The result C1from the XOR operation is then placed at the rightmost position in the shift register and the operation is repeated in the same manner.

If any one block is affected with the error, it may be propagate for all the subsequent block till that block is remains in the shift register.

D. Stream Cipher Mode

In Stream cipher mode, the Initialization vector (IV) is encrypted with the key K. The output is again encrypted with the same key K for getting the second output block. This output block is encrypted to get third output block and so on. The sequence of output blocks is known as key stream. It is one time pad and XOR with the plain text to get the cipher text. Here the IV is used only in the first step. Also the key stream is independent of the data stream so it may be calculated in advance. If any block is affected with error during the transmission than it could affect only that block the subsequent blocks are properly received at the receiver side.

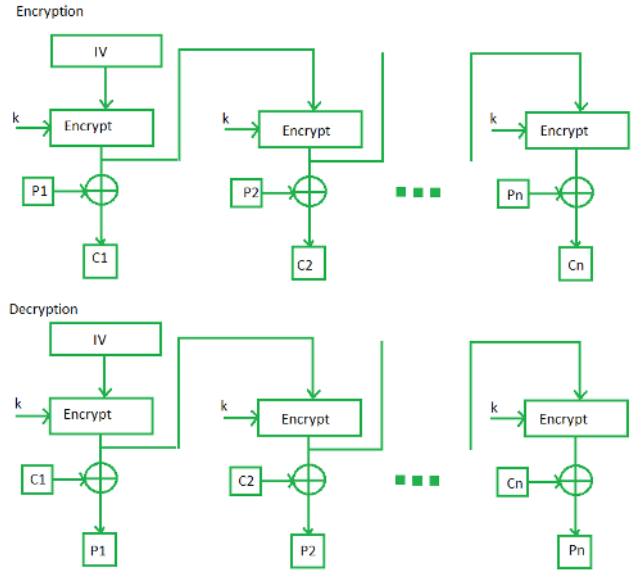

Fig -4: Stream Cipher Mode [7]

If IV and key is used multiple times, than it could be possible that attacker can analysis the cipher text and come to know about the plain text.

E. Counter Mode

In counter mode, the Initialization vector (IV) plus a constant is encrypted with the key K. The resulting output is XOR with the plain text. Every time the initialization vector (IC) is added by 1 for each new block.

It is helpful in decryption of any block of the cipher text without the prior block detain on the receiver side. It is helpful to randomly access any block of plain text. If the IV and key K is same for multiple times than it may be possible that the attacker crack the cipher text easily. The IV and the key K both should be selected randomly in such a way that pair of IV and key should be unique, so that attacker could not break the code.

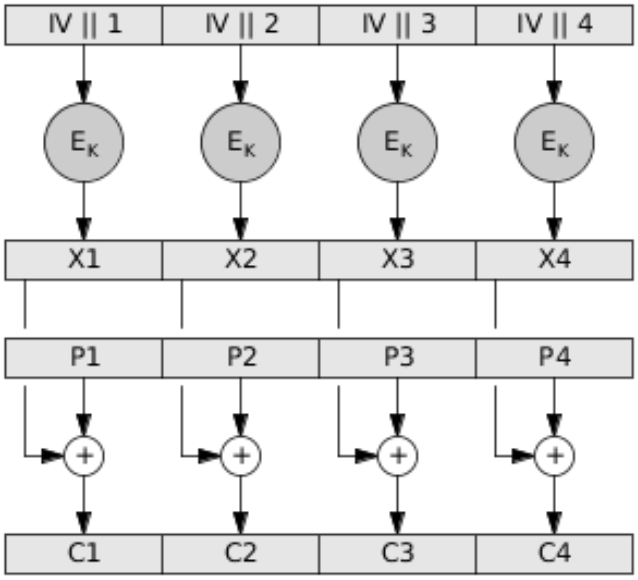

Fig -5: Counter Mode [8]

- Hardware efficiency: Unlike the other modes, encryption and decryption in CTR mode can be done in parallel on multiple blocks of plaintext or cipher text. In other mode, the operation of one block should be completed before starting of the next block. This makes the maximum time for encryption and decryption of the data. In CTR mode, the throughput is only limited by the amount of parallelism that is achieved.
- Software efficiency: Processor that supports the parallel features may effectively utilize for parallel execution in counter mode
- Preprocessing: If enough memory with the device, the preprocessing can be used. The execution of the underlying encryption algorithm does not depend on input of the plaintext or ciphertext. When the plaintext or ciphertext input is presented, then the only computation is a series of XORs. It greatly enhances the throughput.
- Random access: The ith block of plaintext or ciphertext can be processed in random-access fashion.There may be applications in which a ciphertext is stored, and it is desired to decrypt just one block; for such applications, the random access feature is attractive.
- Provable security: counter mode is at least as secure as the other modes discussed in this section.

CONCLUSION

The symmetric key algorithms same input plain text converted into the same cipher text. Attackers may easily identify the key of secret message. To protect against such attack the cipher block modes are used. It helps in secret the message throughout the communication between sender and the receiver. To Convert block cipher into stream cipher

1. Cipher feedback (CFB) mode
2. Stream cipher mode
3. Counter (CTR) mode

Electronic code book mode is not secure mode, but the stream cipher mode and counter mode are vary useful for the several applications.

REFERENCES

[1] J.A. Buchmann. Introduction to Cryptography. NY, Springer, 2001

[2] https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

[3] Kuo-Tsang Huang, Jung-Hui Chiu, and Sung-Shiou Shen (January 2013). "A Novel Structure with Dynamic Operation Mode for Symmetric-Key Block Ciphers" (PDF). International Journal of Network Security & Its Applications (IJNSA). 5 (1): 19. Archived (PDF) from the original on 2015-11-22.

[4] Cryptography Engineering: Design Principles and Practical Applications. Ferguson, N., Schneier, B. and Kohno, T. Indianapolis: Wiley Publishing, Inc. 2010. pp. 63, 64. ISBN 978-0-470-47424-2.

[5] https://www.codeproject.com/Articles/1016357/OpenSSL-Tour-for-Win-Developer

[6] W. Stallings. Cryptography and Network Security : Principles and Practices. Fourth Edition. NJ, Prentice Hall, 2005

[7] https://www.geeksforgeeks.org/computer-network-block-cipher-modes-of-operation/

[8] https://www.cs.rit.edu/~ark/462/module05/notes.shtml

[9] Neelima Saini &Sunita Mandal, “Review paper on cryptography”, International Journal of Research (IJR), e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015