Study of Block Ciphers- Counter Mode and Output Feedback Mode

Avinash Kaur
Department of Computer Engineering,
Lovely Professional University,
Phagwara, India.

Harwant Singh Arri
Department of Computer Engineering,
Lovely Professional University,
Phagwara, India.

***Abstract*—Modes of operations play a vital role in network security. Counter mode and output feedback mode are the mostly used because of their prominent attributes. Encryption and Decryption are done with Rijndael AES algorithm. X-OR operation is one of the major factors by which modes of operation works. Counter mode and output feedback mode are block cipher. But it uses a block cipher as a stream cipher. Operation modes have main features of data security and give surety of data integrity.**

***Keywords*—OFB;Counter Mode;AES;X-OR**

I. Introduction

To secure our information from malicious activity cryptography is done. In simple manner cryptography is secret writing. Encryption and decryption is the main feature that is used with a key to secure any application. It provides privacy to our information and protected it from unknown sources. It is very important task in cryptography that the data which is encrypted at the sender side must be same after decryption at the receiver side. Now a day's number of algorithms are designed which proved the concept of cryptography and ensures the confidentiality, integrity, authentication of data [1]. The main terms used in these algorithms are plaintext which is the original form of message, ciphertext which is the secret writing words. Some substitution and permutation techniques are applied on that particular algorithm.

II. Security in WLAN

Cryptography provides the facility to camouflage our data so that transmitted information can not reveal by eavesdropper. Cryptography means switch information into ostensible unintelligible way that permit a secret method of witching. In this plain text is our well known original message. The switched words or text is converted text called cipher text. No one can understand the format of cipher text .The main reason to hide the characters are to protect it from unauthorized use.This cryptography technique reduces the vulnerabilities issues and protect our data from malicious activities [2]. Cryptography systems manage both an algorithm with a secret quantity with the different cryptographic primitives are:

I. Encryption

It means taking a plain text and transforms it into a special as cipher text. The cipher text is scrambled message produced as output. Message produces by encryption cannot be easily inferred by unauthorized persons.

II. Decryption

It is the conversion of encryption technique. A cipher text is reconverting into its original form. So the text in decryption is what the sender writes at first time to the authorized receiver.

III. AES ALGORITHM

Advanced Encryption Standard is a block cipher.AES use same key for encryption and decryption. AES is a symmetric algorithm. This algorithm is quite different from DES algorithm. It is not feistel type of structure. This algorithm is well known by Rijndael algorithm. In this algorithm three different types of block size can be choose which is of 128,192,256 bits [3]. The key size depends upon the block size. Mainly 128 bits block size is used with 128 bit length of key. Encryption is done by processing number of rounds. For 128 bit key total 10 number of rounds are processed. Similarly for 192 bits total numbers of rounds are 12 and for 256 total numbers of rounds are 14. Working of all rounds are identical except the last round. Each round has substitution and permutation to make data more secure. In total encryption procedure four steps are repeated according to rounds in algorithm.

1.Add Round Key

2.Byte Sub.

3.Shift Row

4.Mix Column

The 4th step is not being used in last round of encryption. For encryption key is divided into various subkeys for each round, this process is called key expansion.

1. Add Round Key

It begins the encryption followed by nine rounds. A bitwise XOR of the current block with the portion of the expanded key is used. Only the Add Round Key step uses the key. Any other step is reversible without knowledge of the key. Decryption is not same to encryption. Decryption uses the same keys but in the reverse order.

2. Byte Sub

In this s-box is used for byte substitution of block. S-Box consists of matrix having byte values. Each indiviual byte of state is mapped into new byte.

3. Shift row

As the name describes rows are shifted in this stage but the first row of state is not altered. For second row,1 byte circular shift is performed. For 3rd row 2-byte and for 4th row 3-byte shift is performed.

4.Mix column

On each column this operation is performed individually. Each byte of column is mapped into new value.

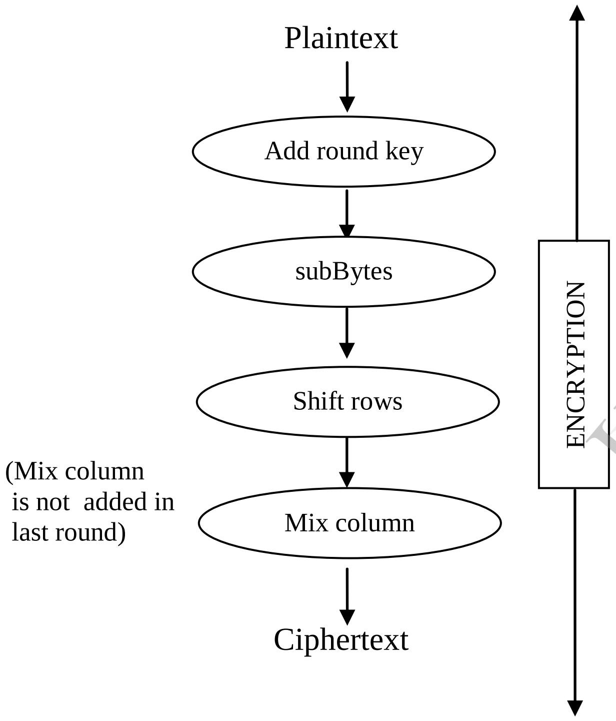

Fig.1. Encryption of AES Algorithm

AES algorithm is highly secure. As the number of rounds are more complex than DES algorithm. Substitution and permutation in each round give the better performance for securing a plaintext. In a state of two dimensional array all the operations are performed.AES algorithm composite of three kinds of layers linear diffusion, non linear diffusion and key mixing[4]. Decryption of AES algorithm is not same as that of encryption whether key scheduling is same as it is symmetric algorithm. For security of our plaintext from sender to receiving side AES algorithm play important role because the use of identical keys, fast processing, use of less computer resources, high performance. The main feature is against brute force attack. Now a days it is enough secure to use in real time applications.

IV. OPERATION MODES

There are various block cipher mode of operations in variety of applications. These block cipher modes are used with AES algorithm to provide more security to sensitive data. A mode of operation defines a cipher's single-block operation which is repeatedly applied to securely transform amounts of data more than a block. All the operation modes are operated using X-OR function [5]. These operation modes are added without any extra cost to AES algorithm. Operation modes are approved by National Institute of Standards and Technology. Most common modes are Electronic Code Book, Cipher block Chaining, Propagating Cipher Block Chaining, Cipher Feedback and Counter Modes. In this paper, we will mainly focus on Output Feedback Mode and Counter Mode because of its eminent nature.

Output feedback mode

It is a block cipher mode of operation. This block cipher is always compared with Cipher Feedback Mode[6]. As the working of both modes are somewhat same. The key difference is at the time of X-OR operation.

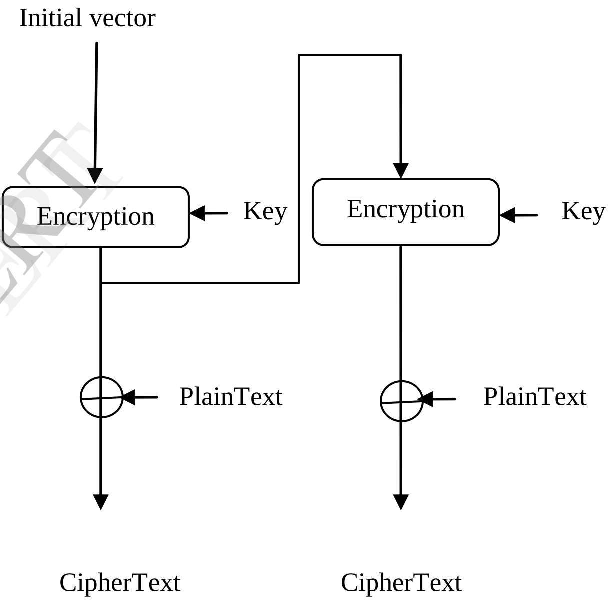

Fig.2. Output Feedback Mode

Output feedback is initially works with initial vector as an input. Then block cipher encryption is performed with key on initial vector. The resultant encryption is X-ORED with the plain text and we obtain the ciphertext .This is the first part of the encryption. The resultant,we obtained before X-OR function with plain text, the second part of encryption is performed with it. The second encryption is performed with same key on resultant then the same procedure is followed. The plain text is X-OR with second resultant. All the operation will be repeated until the block size will over. Initial vector is also called starting variable of fixed size data which is pseudo random. It is used single time in encryption. As intruder has no knowledge of this initial vector[7]. So it is not easy to break the encryption text. Initial vector is also called nonce i.e. number used once.

E_1=Encryption $_{\text{key}}$ (initial vector) $\oplus$ Plain Text

E_i=Encryption $_{\text{Key}}$ (Y_{i-1}) $\oplus$ Plain Text

Where, Yi-1 is the encryption after first stage

.

V. FEATURES OF OUTPUT FEEDBACK MODE

1. Any bit errors that occur at the transmission do not propagated to affect the decryption following blocks [8].
2. Initial vector which is unique in nature make it more secure to prevent from vulnerable activity.
3. It is used to build synchronous stream cipher from a block cipher.
4. It is applicable for bulk encryption for transmission.

VI. COUNTER MODE

It is another type of block cipher operation mode. It is somewhat identical to output feedback mode [9] but it encrypts counter value instead of feedback value. It generates stream cipher turns from block cipher. In this initial value or we can say nonce is concatenate with counter value. Counter value is not same and changes every time. Then combine value is encrypted with the key. After that resultant value is further X-ORED with plaintext to get final cipher text of that value. For each block counter value should be increased and not be same as that of previous value. There is no need to Nonce value to keep secret as it is unpredictable value [8]. In the last blocks bits may not be completely fill, still encryption is possible in that case also.

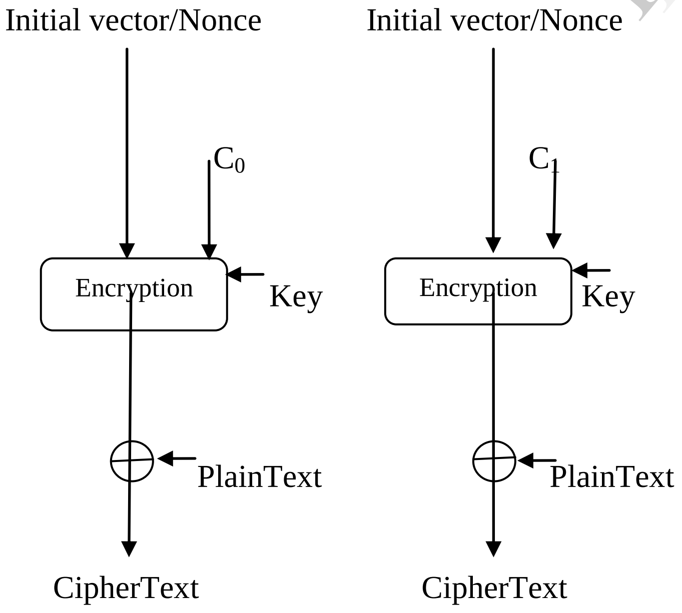

Fig. 3. Counter mode Encryption.

VII. FEATURES OF COUNTER MODE

1. It converts block cipher into stream cipher.
2. It encrypts the entire block at a time. So performance for output is automatically increased.
3. It provides data confidentiality and data integrity which is missing in case of some stream cipher [10].
4. It is a random value which may be set to zero or other vale then every time increment of one is done.
5. The computation can be done in parallel.
6. It takes significant advantage of the efficiency over other ciphers.

Conclusion

Operations modes play important role in network security. The two operation modes i.e. Output Feedback Mode and counter modes are mostly used because of its simple but strong working for security. It takes the advantage of block cipher for high speed requirements. The software and hardware efficiency supports more because of its parallel execution. Counter mode is simpler and less dependent on previous value. Unlike Output Feedback Mode it can compute encryption even when the block size is less than n.So Counter mode take more advantages because of its eminent features. However output feedback is useful in various applications.

REFERENCES

[1] Phillip Rogaway,Mihir Bellare,John Black ,"OCB: A block-cipher mode of operation for efficient authenticated encryption" ,TISSEC, August 2003,Vol. 6 Issue 3, pp. 365-403.

[2] Zirra Peter Buba ,Gregory Maksha Wajiga," Cryptographic Algorithms for Secure Data Communication",IJCSS, 2011,vol.5,no.2,pp.227-243.

[3] C. Parikh,P.Patel,"Performance Evaluation of AES Algorithm on Various Development Platforms" ISCE 2007,pp.1-6.

[4] https: //www.lri.fr/fmartignon/documenti/systemesecurite/5-AES

[5] Phillip Rogaway,"Evaluation of Some Blockcipher Modes of Operation", Evaluation carried out for the CRYPTREC, February , 2011.

[6] Yi-Li Huang, Fang-Yie Leu, Jung-Chun Liu, Jing-Hao Yang," A Block Cipher Mode of Operation with Two Keys",Lecture Notes in Computer Science and information and Communication Technology,2013,Vol. 7804, pp 392-398.

[7] http: // highered.mcgrawhill.com /sites/dl/free/0072870222/385981 /Student_Solution_Chap_08.

[8] Kinga Marton ,Alin Suciu ,Christian Sacarea, Octavian Cret,"Generation and Testing of random numbers for cryptographic applications" ,proceedings of the romanian academy vol. 13, no. 4,2012, pp. 368–377.

[9] Teo, Sui-Guan and Al-Mashrafi, Mufeed and Simpson, Leonie R. and Dawson, "Analysis of authenticated encryption stream ciphers" ,Proceedings of the 20th National Conference of Australian Society for Operations Research, September 2009,pp.27-30.

[10] http://shodhganga.inflibnet.ac.in/bitstream/10603/9416/11/11_chapter3.