Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 4, Issue 1, pp: (12-18), Month: January - April 2017, Available at: www.noveltyjournals.com

Data Encryption Standard (DES)

[1]Omer Farooq Ahmed, [2]Mustfa Mhamed Ali

Department of Computer Applied Technology, HUST

Abstract: **It is not recommended, however it is possible while working with block ciphers, to use the same secret key bits for encrypting the same plaintext parts. Using one deterministic algorithm for some number of identical input data, results in some number of identical ciphertext blocks.**
It is a very dangerous situation for the cipher's users. An intruder would be able to get much information knowing a distribution of identical message parts, even if he would not be able to break the cipher and discover original messages.
There are ways to blur and mix plaintext blocks (which are known) with ciphertext blocks (which are created). They can prevent many identical output ciphertext blocks. These methods are called *the block cipher modes of operations*.

Keywords: **ciphertext, ECB, CBC, CFB, CTR.**

1. INTRODUCTION

Several types of symmetric algorithms are used today. They have different methods of providing encryption and decryption functionality

The one thing they all have in common is that they are symmetric algorithms, meaning the sender and receiver are using two instances of the same key.

In cryptography, modes of operation enable the repeated and secure use of a block cipher under a single key . A block cipher by itself allows encryption only of a single data block of the caper’s block length .

When targeting a variable – length message , the data must first be partitioned into separate cipher blocks. Typically , the last block must also be extended to match the cipher`s block length using a stable padding scheme.

A mode of operation describes the process of encrypting each of these blocks, and generally uses randomization based on an additional input value , often called an initialization vector , to allow doing so safely.

Modes of operation have primarily been defined for encryption and authentication.

Historically, encryption modes have been studied extensively in regard to their error propagation properties under various scenarios of data modification.

Later development regarded integrity protection as an entirely separate cryptographic goal form encryption. Some modern modes of operation combine encryption and authentication in an efficient way, and are known as authenticated encryption modes.

While modes of operation are commonly associated with symmetric encryption , they may also be applied to public-key encryption primitives such as RSA in principle (though in practice public – key encryption of longer messages is generally realized using hybrid encryption).

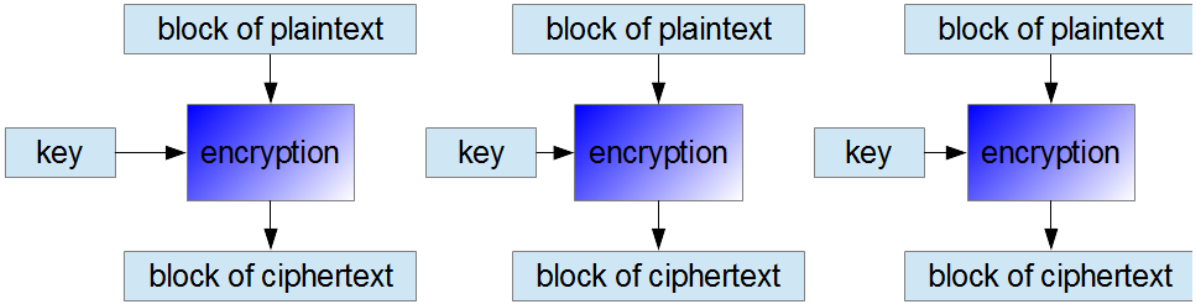
Novelty Journals

ISSN 2394-7314

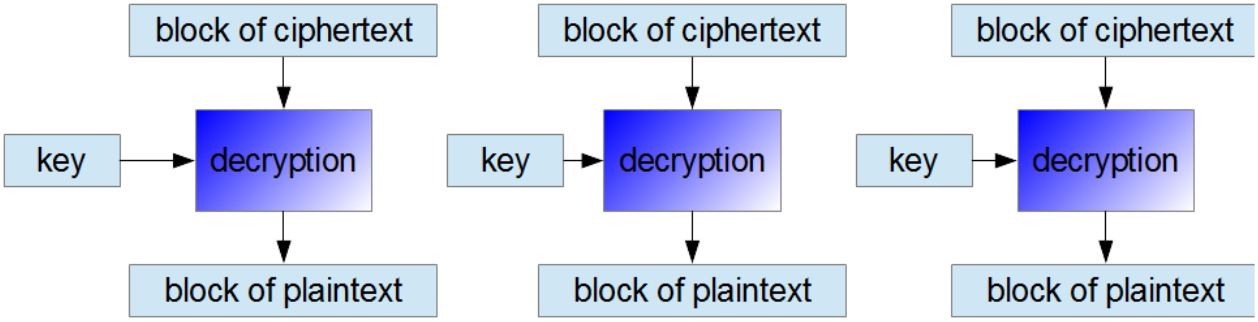
International Journal of Novel Research in Computer Science and Software Engineering
Vol. 4, Issue 1, pp: (12-18), Month: January - April 2017, Available at: www.noveltyjournals.com

2. ECB (ELECTRONIC CODEBOOK) MODE

It is the simplest mode of encryption. Each plaintext block is encrypted separately. Similarly, each ciphertext block is decrypted separately. Thus, it is possible to encrypt and decrypt using many threads simultaneously. In this mode, the created ciphertext is not blurred.



Encryption in ECB mode



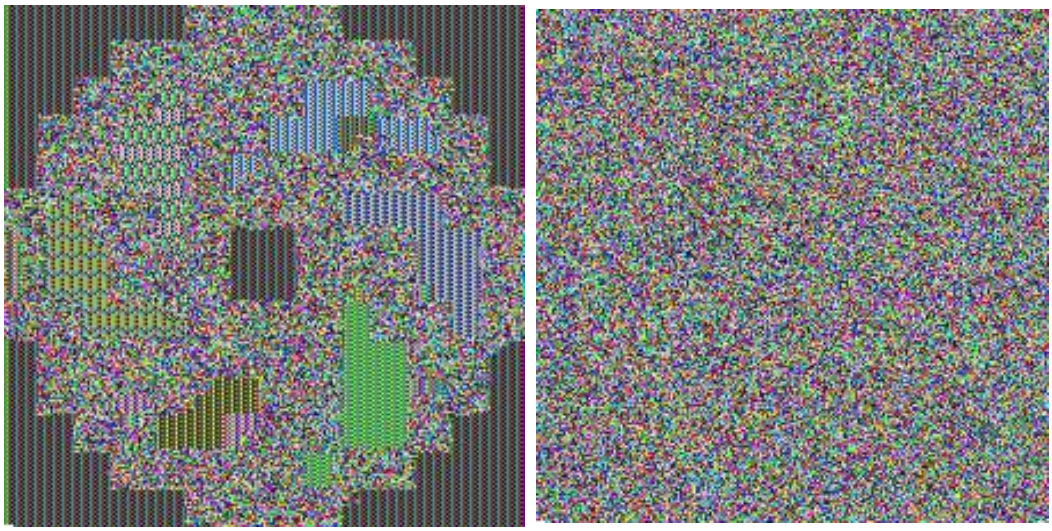
Decryption in ECB mode

A typical example of weakness of encryption using ECB mode is encoding a bitmap image (for example a .bmp file). Even a strong encryption algorithm that uses ECB mode, cannot blur efficiently its content.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 4, Issue 1, pp: (12-18), Month: January - April 2017, Available at: www.noveltyjournals.com



The bitmap image encrypted using DES and the same secret key. The ECB mode was used for the left image and the CBC mode was used for the right image.

Message that are encrypted using ECB mode should be extended until a size that is equal to an integer multiple of the single block length. The popular method of aligning the length of the last block is about appending an additional bit equals to 1 and then filling the rest of the block with bits equal to 0. It allows to determine precisely the end of the real message.

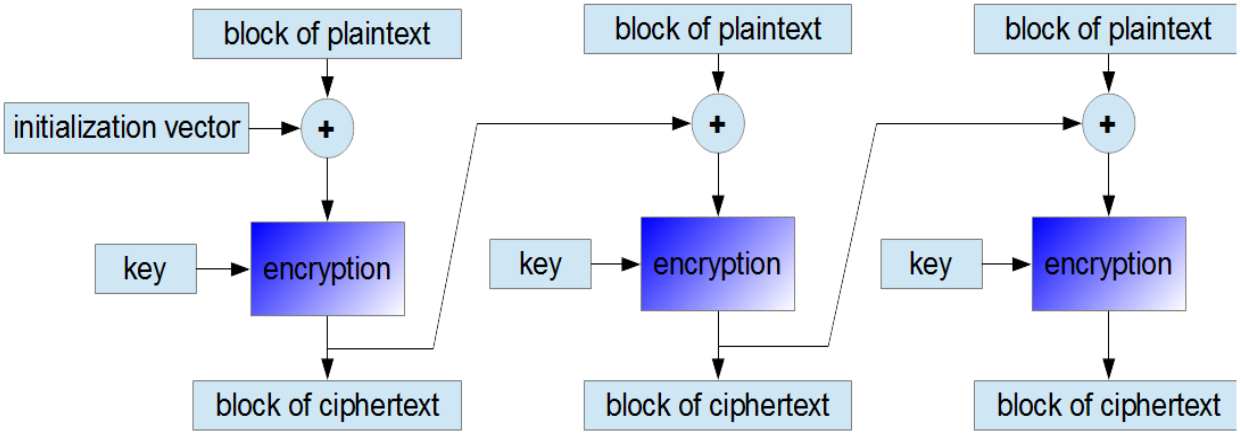
Ciphers that are used in ECB mode are more vulnerable to replay attacks.

3. CBC (CIPHER-BLOCK CHAINING) MODE

The CBC mode of encryption was invented by IBM in 1976. It is about to add XOR each subsequent plaintext block to a ciphertext block that was previously received. The result is encrypted using a cipher's algorithm in the usual way. Each subsequent ciphertext block depends on the previous one. The first plaintext block is added XOR to a random initialization vector (commonly referred to as IV). The vector has the same size as all plaintext blocks.

Encryption in CBC mode can be performed only using one thread. Despite this disadvantage, it is a very popular way of encrypting, which is used in various applications.

During decrypting ciphertext blocks, one should add XOR output data from decryption algorithm to previous ciphertext blocks. The receiver knows all ciphertext blocks just after obtaining encoded the message, thus he can decrypt the message using many threads simultaneously.

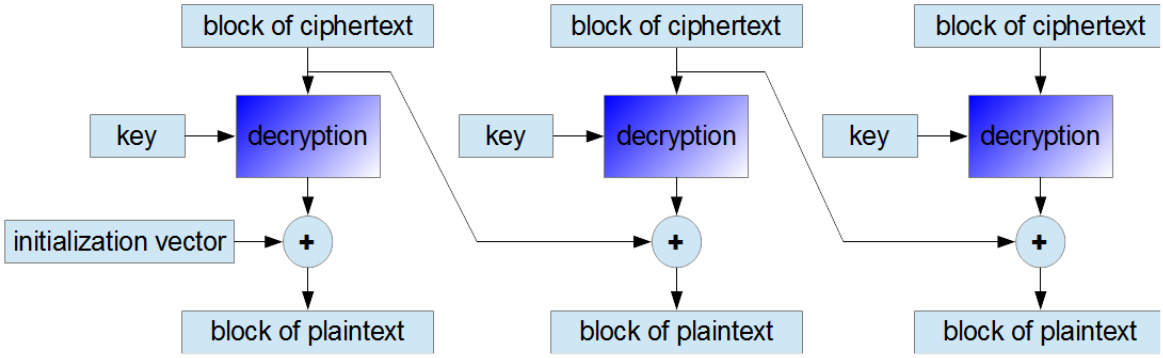


Encryption in CBC mode

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 4, Issue 1, pp: (12-18), Month: January - April 2017, Available at: www.noveltyjournals.com



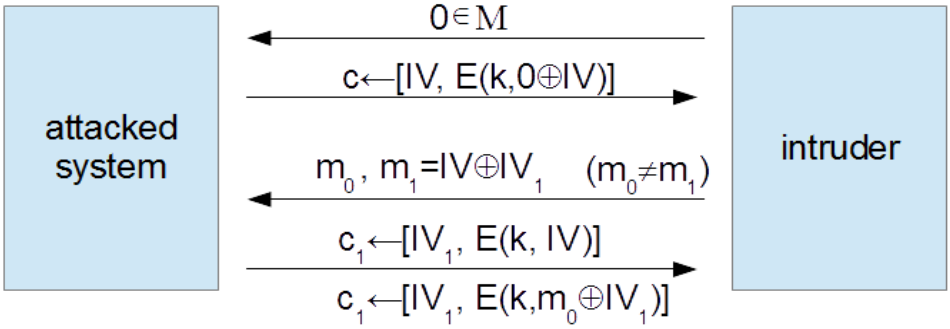
Decryption in CBC mode

If one bit of a plaintext message is damaged (for example because of transmission error), all subsequent ciphertext blocks will be damaged and it will not be possible to decode the ciphertext in the future. As opposed to that, if one ciphertext bit is damaged, only two received plaintext blocks will be damaged.

A message that is to be encrypted using CBC mode, should be extended until a size that is equal to an integer multiple of the single block length (as during using ECB mode).

Security of the CBC mode:

The initialization vector IV should be created randomly by the sender. During transmission it should be concatenated with ciphertext blocks, to allow decryption of the message by the receiver. If an intruder could predict what vector will be used, then encryption would not be resistant to chosen-plaintext attacks:



In the example presented above, if the intruder is able to predict that the vector IV_1 will be used during encryption the system's response c_1, he can guess which one of the two encrypted messages m_0 or m_1 is contained in the response. This situation breaks a rule that the intruder shouldn't be able to distinguish between two ciphertexts even if he has chosen both plaintexts. Therefore, the system is vulnerable to chosen-plaintext attacks.

If IV is generated based on non-random data, for example a user password, it should be encrypted before use. One should use a separate secret key for this activity.

The initialization vector IV should be changed after using the secret key a number of times. It can be shown that even properly created IV used too many times, makes the system vulnerable to chosen-plaintext attacks. For AES it may be estimated to be 2^{48} blocks, while for 3DES it is about 2^{16} plaintext blocks.

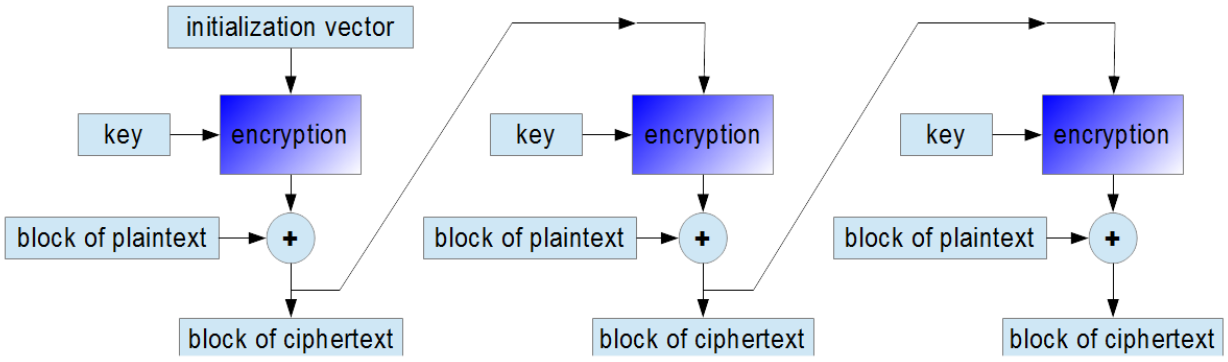
4. CFB (CIPHER FEEDBACK) MODE

The CFB mode is similar to the previously described CBC mode. The main difference is that one should encrypt mixed data from the previous round (so not plaintext blocks) and then add to plaintext bits. It does not affect the security strength but it results in using cipher's encryption algorithms (the same that were used for encrypting plaintext) during decryption process.

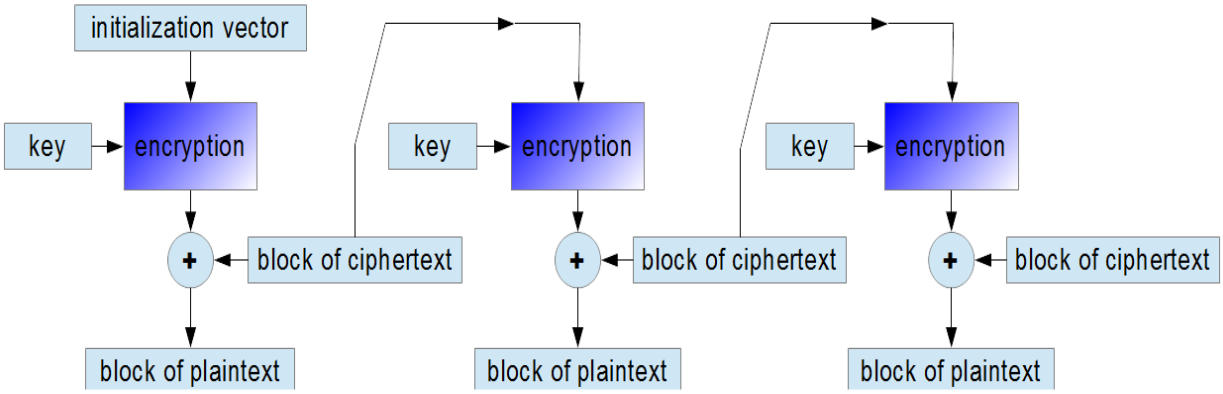
Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 4, Issue 1, pp: (12-18), Month: January - April 2017, Available at: www.noveltyjournals.com



Encryption in CFB mode



Decryption in CFB mode

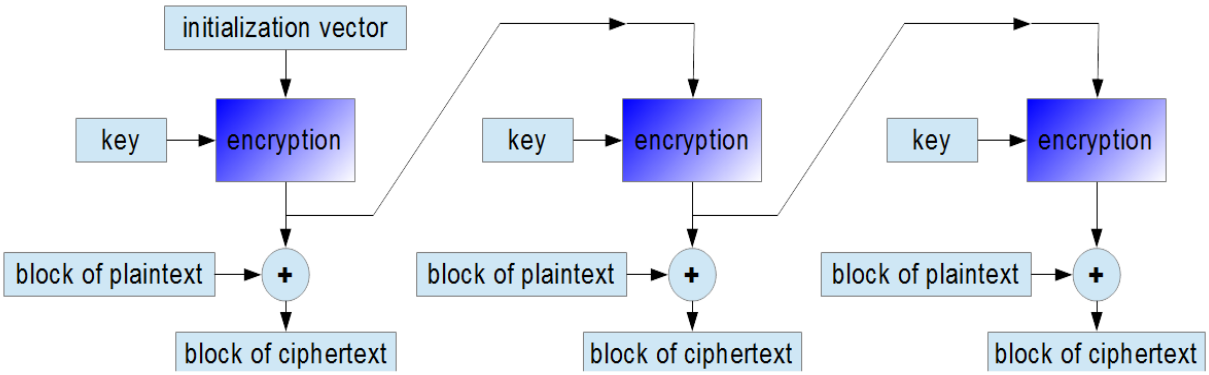
If one bit of a plaintext message is damaged, the corresponding ciphertext block and all subsequent ciphertext blocks will be damaged. Encryption in CFB mode can be performed only using one thread.

On the other hand, as in CBC mode, one can decrypt ciphertext blocks using many threads simultaneously. Similarly, if one ciphertext bit is damaged, only two received plaintext blocks will be damaged.

As opposed to the CBC mode, the encrypted message doesn't need to be extended until a size that is equal to an integer multiple of the single block length.

5. OFB (OUTPUT FEEDBACK) MODE

Algorithms that work in the OFB mode, create keystream bits that are used for encryption subsequent data blocks. In this regard, the way of working of the block cipher becomes similar to the way of working of a typical stream cipher.

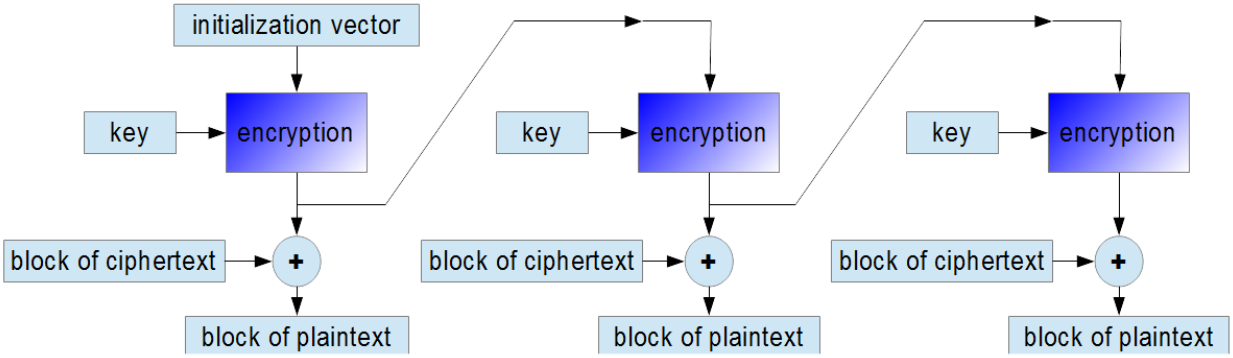


Encryption in OFB mode

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 4, Issue 1, pp: (12-18), Month: January - April 2017, Available at: www.noveltyjournals.com



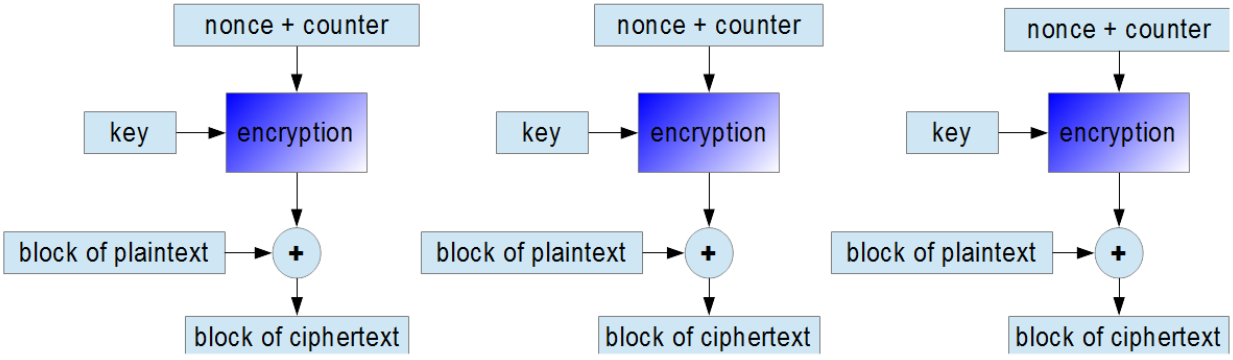
Decryption in OFB mode

Because of the continuous creation of keystream bits, both encryption and decryption can be performed using only one thread at a time.

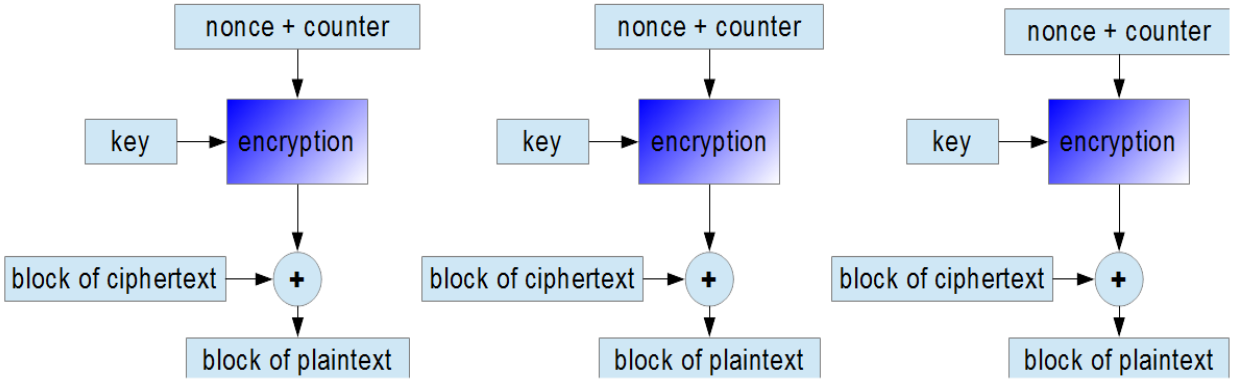
If one bit of a plaintext or ciphertext message is damaged (for example because of transmission error), only one corresponding ciphertext or respectively plaintext bit is damaged as well. It is possible to use various correction algorithms to restore the previous value of damaged parts of the received message.

6. CTR (COUNTER) MODE

Using the CTR mode makes block ciphers' way of working similar to stream ciphers' way of working. As in the OFB mode, key stream bits are created regardless of content of encrypted data blocks. In this mode, subsequent values of an increasing counter are added to a nonce value and the results are encrypted as usual. The nonce plays the same role as initialization vectors in the previous modes.



Encryption in CTR mode



Decryption in CTR mode

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 4, Issue 1, pp: (12-18), Month: January - April 2017, Available at: www.noveltyjournals.com

It is one of the most popular block ciphers modes of operation. Both encryption and decryption can be performed using many threads at the same time.

If one bit of a plaintext or ciphertext message is damaged, only one corresponding output bit is damaged as well. Thus, it is possible to use various correction algorithms to restore the previous value of damaged parts of received messages.

Security of the CTR mode:

As in the case of the CBC mode, one should change the secret key after using it for encrypting a number of sent messages. It can be proved that the CTR mode provides better security and the secret key should be changed less often.

For example, for the AES cipher the secret key should be changed after about 2^{64} plaintext blocks.

7. CONCLUSION

- Block ciphers may provide excellent cryptographic properties, but for practical application they need modes of operation
- Such modes of operation may be used both for confidentiality and integrity
- There are many different modes of operation for specific purposes, including network traffic protection, hard drive encryption, etc.
- Careful selection of mode is needed, otherwise even a strong block cipher (e.g., AES-256) protection might be broken in some circumstances

REFERENCES

[1] American National Standard for Financial Services X9.52-1998, “Triple Data Encryption Algorithm Modes of Operation.” American Bankers Association, Washington, D.C., July 29, 1998.

[2] FIPS Publication 197, “Advanced Encryption Standard (AES).” U.S. DoC/NIST, November 26, 2001.

[3] FIPS Publication 46-3, “Data Encryption Standard (DES).” U.S. DoC/NIST, October 25, 1999.

[4] FIPS Publication 81, “DES Modes of Operation.” U.S. DoC/NIST, December 1980.

[5] A. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography.” CRC Press, New York, 1997.