Journal of Al-Azhar University Engineering Sector

Vol.15, No. 57, October, 2020, 981-991

# NETWORK SECURITY BY BLOCK CIPHERS

**Mohamed Hussein Mohamed Hassan**
Systems and Computer Engineering Dep., Faculty of Engineering(Girls), Al-Azhar University, Cairo, Egypt.
E-mail: m.hussein@azhar.edu.eg

**ABSTRACT**:
This paper reviews some of the encryption models through the block cipher technique used for the data encryption process. As an introduction, we explained Classical Substitution Ciphers by two example models (Caesar Cipher and Vigenere Cipher). They are followed by a block cipher which is presented by multiple encryption triple DES and block cipher modes of operation. Multiple encryption DES algorithms are using two or three keys to make the encryption process more complex. But still using a 64-bit fixed blocks message and also wasted a lot of time during the encryption and decryption process. So we need some ways to encrypt and decrypt arbitrary quantities of data. This paper presents five block cipher modes of operation to cover a wide variety of applications and can be used with any block cipher.

**KEYWORDS: Cryptography, Data Encryption Standard, Electronic Codebook, Cipher Block Chaining, Cipher Feedback, Output Feedback, and Counter.**

## نظرة عامة لأمن الشبكة من خلال تشفير كتلة بيانات

**محمد حسين محمد حسن**
قسم هندسة النظم والحاسبات ، كلية الهندسة بنات ، جامعة الازهر،القاهرة ، مصر.
البريد الاليكتروني:E-mail: m.hussein@azhar.edu.eg

**الملخص** :
يستعرض هذا البحث بعض نماذج التشفير من خلال تقنية تشفير الكتل المستخدمة لعملية تشفير البيانات. كمقدمة، أوضحنا شفرات الاستبدال الكلاسيكي من خلال نموذجين من الأمثلة ( سيزر، فيجنر). ينتقل البحث ليوضح تشفير كتلة من البيانات عن طريق التشفير المتعدد الثلاثي وأنماط تشغيل تشفير الكتلة. تستخدم الخوارزميات متعددة التشفير ذات مفتاحين أو ثلاثة لجعل عملية التشفير أكثر تعقيدًا. ولكن لا تزال هذه الخوارزمية تستخدم كتلة بيانات بحجم ثابت ٦٤ بت ، كما أنه أهدر الكثير من الوقت أثناء عملية التشفير وفك التشفير. لذلك نحن بحاجة إلى بعض الطرق لتشفير وفك تشفير كميات البيانات العشوائية والمتغيرة الإحجام. يقدم هذا البحث خمسة أنماط تشفير كتلة لتغطية مجموعة واسعة من التطبيقات ويمكن استخدامها مع أي تشفير لكتلة البيانات.

**الكلمات المفتاحية: أساليب وطرق التشفير، نظام تشفير البيانات المعياري ، خمسة أنماط جديدة لعملية التشفير (كتاب التشفير الاليكتروني، التشفير المتغير من خلال التغذية المرتجعة ، تشفير الخرج بالتغذية المرتجعة، التشفير باستخدام نظام العداد ) تم فحصها الرياضي بنجاح.**

## INTRODUCTION

In the Classical Substitution Ciphers, the letters of plaintext are replaced by other letters or by numbers or symbols, or if plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns [1]. In the second alternative, the idea of block cipher can be discussing by two techniques: Multiple Encryption triple DES, and block cipher modes of operation [2].

Multiple encryptions are a technique in which the encryption algorithm is used multiple times. In the first instance, plaintext is converted to ciphertext using an encrypted algorithm. This ciphertext is used again as an input. This process can be repeated in any number of stages. Triple DES uses three stages of the DES algorithm, using a total of two or three separate keys [3].

As the last technique in this paper, the block cipher modes of operation is a technique used to enhance the effect of a cryptographic algorithm or to adjust the algorithm for an application, there are five modes of operation for use in these techniques (ECB, CBC, CFB, OFB, and CTR) [4].

| Mode | Description | Typical Application |
|---|---|---|
| Electronic Codebook (ECB) | Each block of 64 plaintext bits is encoded independently by using the same key. | • Secure transmission of single values (e.g., encryption key) |
| Cipher Block Chaining (CBC) | The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the previous 64 bits of ciphertext. | • General-purpose block-oriented transmission<br>• Authentication |
| Cipher Feedback (CFB) | Input is being processed bits at a time. The preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce the next unit of ciphertext. | • General-purpose stream-oriented transmission<br>• Authentication |
| Output Feedback (OFB) | Similar to CFB, except that the encryption algorithm input is the previous encryption output, and full blocks are used. | • Stream-oriented transmission over a loud channel (e.g., satellite communication) |
| Counter (CTR) | Each plaintext block is XORed with an encrypted counter. The counter will be increased for each subsequent block. | • General-purpose block-oriented transmission<br>• Useful for high-speed requirements |

### Encryption Model techniques

The presented encryption model techniques are Classical Substitution Ciphers, multiple encryptions triple DES using two or three keys, and block cipher modes of operation.

### 1. Classical Substitution Ciphers

The idea of Classical Substitution Ciphers, is to replace a text character by another one. The examples of these are (Caesar Cipher and Vigenere Cipher) [5].

### 1.1 Caesar Cipher

This substitution cipher is used as one key for all letters. This key is explained by the following equations:

**C = (p + 3) mod 26**
**p = (C - 3) mod 26**
**1.2 Example:**
plain: meet me after the toga party
cipher: PHHW PH DIWHU WKH WRJD SDUWB
plain: a b c d e f g h i j k l m n o p q r s t u v w x y z
cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

| A | B | C | D | E | f | G | H | I | j | k | L | M | N | O |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |

| P | q | R | S | T | U | V | W | x | y | Z |
|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

**1.3 Vigenere CIPHER**
In this scheme, the set of related mono-alphabetic substitution rules consists of the 26 Caesar ciphers with shifts from 0 to 25. Each cipher is denoted by a key letter, which is the cipher-text letter that replaces a plain-text letter. As a result, character "**a**" Caesar cipher with a shift of 3 will be encrypted to a character **"d"** [6].

**1.4 Example:**
**Ci= (Pi+ Ki mod m) mod 26**
**Pi= (Ci- ki mod m) mod 26**
**key**: d e c e p t I v e d e c e p t I v e d e c e p t I v e
**plaintext:** w e a r e d i s c o v e r e d s a v e y o u r s e l f
**ciphertext:** Z I C V T W Q N G R Z G V T W A V Z H C Q Y G L M G J

| Key | 3 | 4 | 2 | 4 | 15 | 19 | 8 | 21 | 4 | 3 | 4 | 2 | 4 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Plaintext | 22 | 4 | 0 | 17 | 4 | 3 | 8 | 18 | 2 | 14 | 21 | 4 | 17 | |
| Ciphertext | 25 | 8 | 2 | 21 | 19 | 22 | 16 | 13 | 6 | 17 | 25 | 6 | 21 | |
| Key | 15 | 19 | 8 | 21 | 4 | 3 | 4 | 2 | 4 | 15 | 19 | 8 | 21 | 4 |
| Plaintext | 4 | 3 | 18 | 0 | 21 | 4 | 24 | 14 | 20 | 17 | 18 | 4 | 11 | 5 |
| Ciphertext | 19 | 22 | 0 | 21 | 25 | 7 | 2 | 16 | 24 | 6 | 11 | 12 | 6 | 9 |

Classical Substitution Ciphers are defined by an easy-to-use algorithm in the encryption process and maligned ease decoded by intruders and also does not provide high performance, and cannot be used for large data. This technique can be defined as a low degree of confidentiality.

## 2. BLOCK CIPHER

Block cipher can be classified to Multiple Encryption triple DES and block cipher modes of operation. In this technique, we're going to start encrypting the message process sent by cutting blocks to a group of blocks instead of encrypting a stream of bits in classical substitution cipher.

### 2.1 Multiple encryption and triple DES.

Considering the potential vulnerability of DES to a brute-force attack, there has been considerable interest in finding an alternative. Another alternative that would preserve the existing investment in software and equipment is the use of multiple DES encryption and multiple keys. Let us begin by looking at the simplest example of this second alternative [7].

### 2.1.1. Double DES

The simplest form of multiple encryptions has two stages of encryption and two keys are shown in Fig. 1. Given the plain text and two encryption keys, the cipher text is generated as [8]:

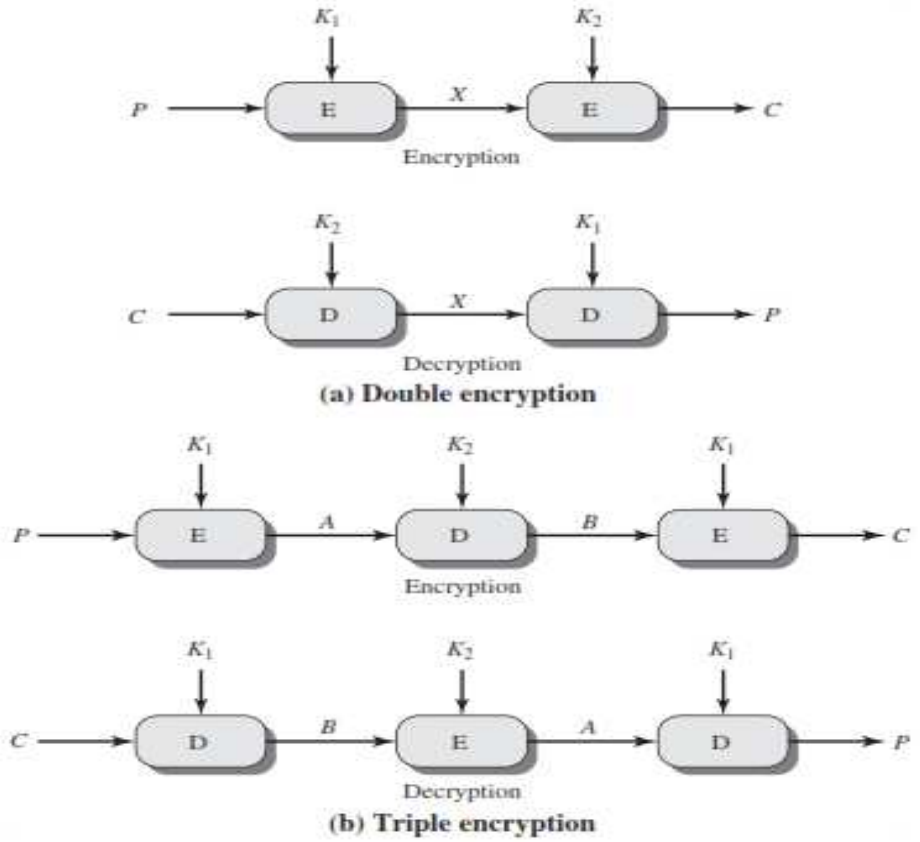



**Fig. 1. Multiple Encryptions**

**Encryption equation**: **are shown in fig.1. a.**

| |
|---|
| C = E (K2 , X) |
| C = E (K2 , X) |
| X = E (K1 , P) |
| **C = E (K2 , E (K1 , P))** |

**Decryption equation: are shown in fig.1. a.**

| |
|---|
| P = D (K1 , X) |
| X = D (K2 , C) |
| **P = D (K1 , D (K2 , C))** |

### 2.1.2. Triple DES with Two Keys equations:

Triple DES with two keys is a popular alternative to single-DES, but has a 3-fold slower start to run [9].

**Encryption equation: are shown in fig.1. b.**

| |
|---|
| C = E (K1 , B) |
| B = D ( K2 , A) |
| A = E (K1 , P) Then B = D (K2 , E (K1 , P)) |
| **C = E (K1 , D(K2 , E(K1 , P)))** |

**Decryption equation: are shown in fig.1. b.**

| |
|---|
| P = D (K1 , A) |
| A = E ( K2 , B) |
| B = D (K1 , C) Then A = E (K2 , D (K1 , C)) |
| **P = D (K1 , E(K2 , D(K1 , C)))** |

### 2.1.3. Triple DES with three Keys equations:

Although the attacks currently known seem impractical, anyone using two 3-DES keys may have some concern. As a result, many researchers now feel that 3-key 3DES is the preferred alternative. Three 3DES keys have an effective key length of 168 bits as shown in fig. 2 [10].

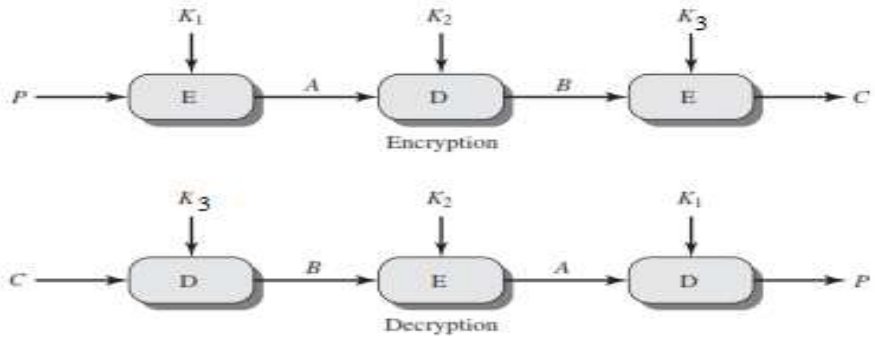



**Fig 2. Triple DES with three Keys**

**Encryption equation: are shown in fig.2.**

| |
|---|
| C = E (K3 , B) |
| B = D ( K2 , A) |
| A = E (K1 , P) Then B = D (K2 , E (K1 , P)) |
| **C = E (K3 , D(K2 , E(K1 , P)))** |

**Decryption equation: are shown in fig.2.**

| |
|---|
| P = D (K1 , A) |
| A = E ( K2 , B) |
| B = D (K3 , C) Then A = E (K2 , D (K3 , C)) |
| **P = D (K1 , E(K2 , D(K3 , C)))** |

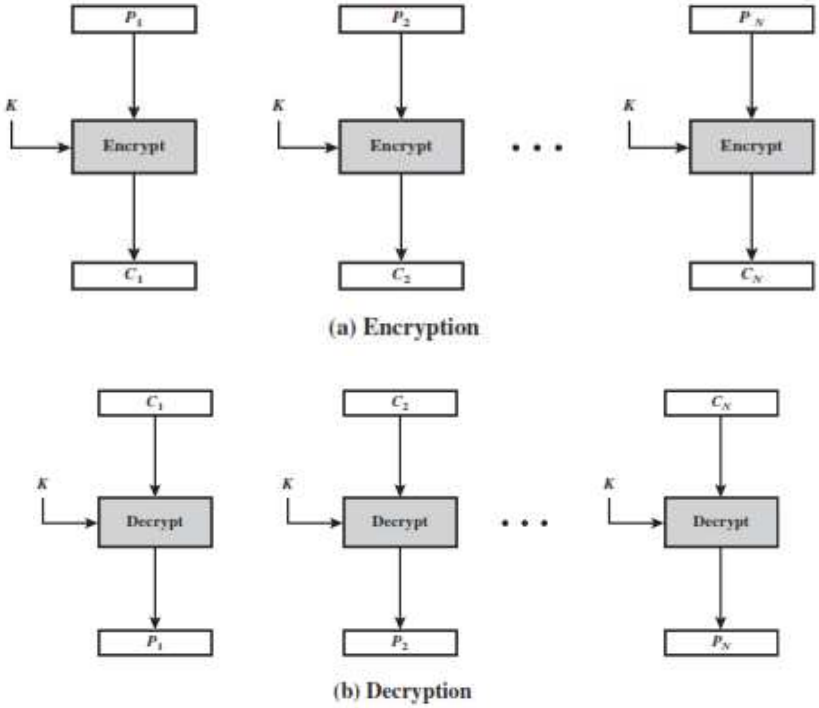
## 2.2 A block cipher modes of operation

DES (or any block cipher) is a simple building block that encrypts/decrypts a fixed block of data, e.g., DES encrypts 64-bit blocks [11]. So we need some ways to encrypt and decrypt arbitrary quantities of data. This section presents five block and stream modes to cover a wide variety of applications and can be used with any block cipher. Finally, the research presents another idea in

five different ways for each algorithm. Algorithms differ in the method of working with blocks, some of which deal with each block of text on the message unit to generate an encrypted block. And it deals with all the blocks together to produce a fully encrypted message once. This method is characterized by high reliability and efficiency, especially with large data volumes depending on the use of the Firmware encryption process which results in high efficiency and transmission speed. And, in this way, only the difficulty of producing an algorithm based on the Firmware maligned. This higher level of confidentiality is classified.

### 2.2.1. ELECTRONIC CODEBOOK (ECB)

The key feature of the ECB is that the message is divided into encrypted independent blocks. Each block is a value that is replaced by a codebook, hence a name. each block is coded independently of the other blocks. And we can use the ECB to safely transfer single vales as shown in fig. 3. The ECB Advantages, the repetition of the message may be shown in ciphertext of such graphics. The ECB Limitations are weakness is due to the encrypted message blocks being independent, vulnerable to cut-and-paste attacks, and the main use is to send a few blocks of data [12].




**. Fig. 3. Electronic Codebook (ECB) Mode**

**We can define ECB mode as Follows:**

| | | | | |
|---|---|---|---|---|
| **ECB** | Cj = E(K,Pj) | j = 1 ….N | Pj = D(K,Cj) | j = 1 .....N |

### 2.2.2. CIPHER BLOCK CHAINING MODE (CBC)

To fix the ECB's security deficiencies, we would like a technique in which the same plaintext block, if repeated, produces different ciphertext blocks [13]. The cipher block chaining (CBC) mode is shown in fig. 4. an easy way to fulfil this requirement. The key advantage of CBC is that the message is split into blocks and connected together in encryption process. Growing previous cipher block is chained to the current plaintext block. The IV is used to avoid the same P from producing the same C. As with the ECB mode, the CBC mode allows the last block to be packed to maximum bits if it is a partial block (usually 0's). For decryption, every cipher block is passed through the decryption algorithm. The result is XORed with the presiding ciphertext block

to construct a plaintext block. To construct the first block of ciphertext, the initialization vector (IV) is XORed with the first block of plaintext. Upon decryption, the IV is XORed with the output of the decryption algorithm to recover the first block of plaintext. The IV is a data block of the same size as the cipher block and is very well known (often all 0's). The IV must be known both to the sender and to the receiver but must be unpredictable by a third party. The advantages for CBC mode are applicable whenever a large amount of data need to be sent securely and authenticated, and provided that all data is available in advance (eg email, FTP, web etc) [14]. The drawback for CBC, the ciphertext block relies on all blocks before it, and any block change affects all following ciphertext blocks, and if sent in clear, an attacker may later the first block bits by modifying the corresponding IV block bits.

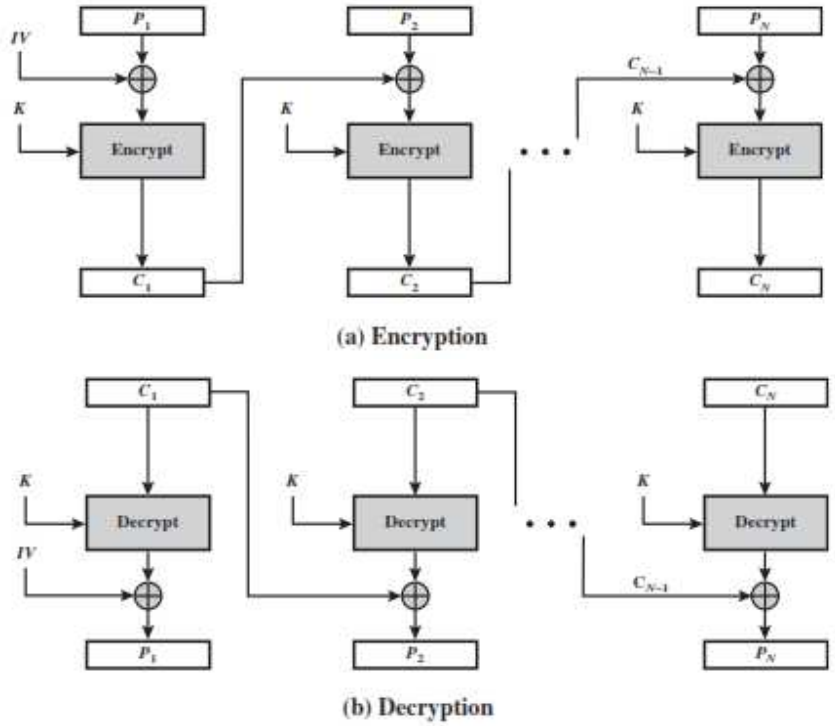



**Fig. 4. Cipher Block Chaining (CBC)**

**We can define CBC mode as Follows:**

| | | |
|---|---|---|
| **CBC** | $C_1=E(K,[P_1 \oplus IV])$<br>$C_j= E(K,[P_j \oplus C_{j-1}])$ $j = 2,..,N$ | $P_1 = D(K,C_1) \oplus IV$<br>$P_j = D(K,C_j) \oplus C_{j-1}$ $j=2,..,N$ |

## 2.2.3 CIPHER FEEDBACK MODE (CFB)

Entry to the encryption method is a b-bit shift register that is initially set to a certain initialization vector (IV). The leftmost (most significant) s-bits of the output of the encryption function are XORed with the first segment of plaintext P1 to generate the first unit of cipher text C1 to be transmitted. In addition, the contents of the shift register are shifted to the left by s-bits and C1 is placed in the rightmost (least significant) s-bits of the shift register. This process will continue until all plaintext units have been encrypted. The same scheme is used for decryption, except that the obtained ciphertext unit is XORed with the output of the encryption method to generate the plaintext unit. Remember that, it is the encryption function that is used, not the decryption function, and that CFB is the normal stream mode. But CFB slow down the encryption process as more encryption is required. The structure of the session is shown in Fig. 5. The advantages of CFB, the most common stream mode, are sufficient when data arrives in bits/bytes, and the restriction is required to stall while block encryption ever s-bits [15]. Note that the block cipher is used in both ends (XOR) encryption mode.

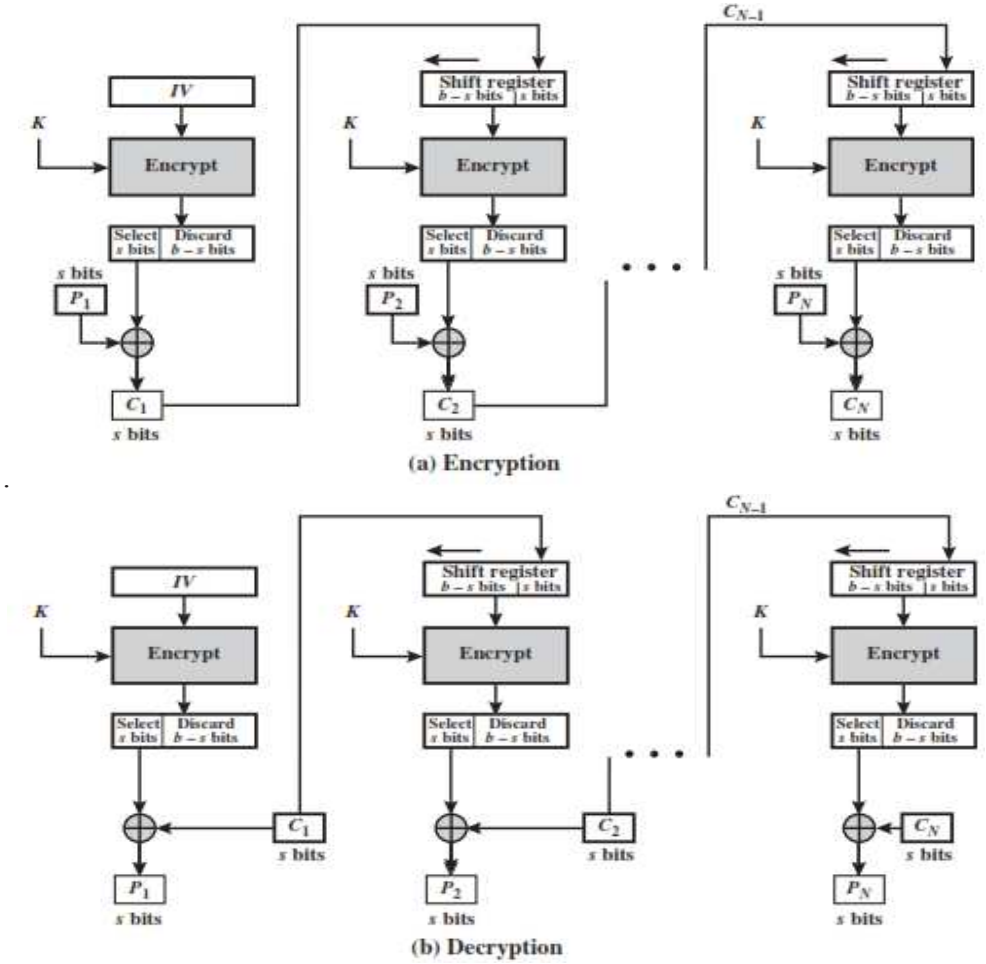



**Fig. 5. s-bit Cipher FeedBack (CFB) Mode**

**We can define CFB mode as Follows:**

| | | |
|---|---|---|
| **CFB** | $I_1 = IV$<br>$I_j = LSB_{b-s}(I_{j-1}) \| C_{j-1}$ j = 2,….,N<br>$O_j = E(K, I_j)$ j = 1,….,N<br>$Cj = P_j \oplus MSBs(Oj)$ j = 1,….,N | $I_1 = IV$<br>$I_j = LSB_{b-s}(I_{j-1}) \| C_{j-1}$ j = 2,….,N<br>$O_j = E(K, I_j)$ j = 1,….,N<br>$P_j = C_j \oplus MSBs(Oj)$ j = 1,….,N |

## 2.2.4. OUTPUT FEEDBACK MODE (OFB)

The main characteristic of OFB is that the message is treated as a bit stream, the output of the cipher is added to the message, the feedback is independent of the message and can be computed in advance. Fig. 6. As with CBC and CFB, the OFB mode requires an IV mode. The IV must be a nonce; that is, the IV must be unique to each execution of the encryption operation. OFB Advantages and Limitations needs an IV that is unique for each use, may pre-compute, not propagate bit errors, and maybe more vulnerable to message stream modification. Then, change arbitrary bits by changing ciphertext, sender & receiver must remain in sync, and only use full block input [16].

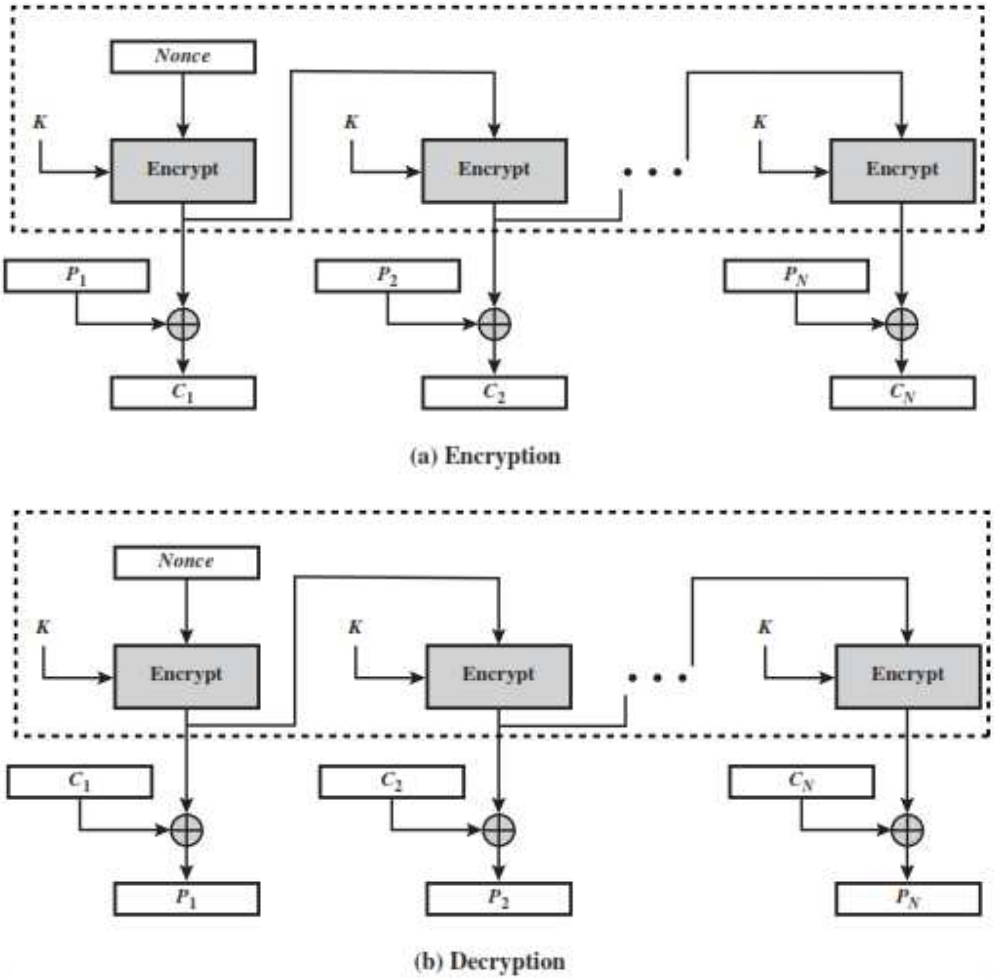



**Fig. 6. Output FeedBack (OFB) Mode**

**We can define OFB mode as Follows:**

| | | |
|---|---|---|
| **OFB** | $I_1$ = Nonce<br>$I_j = O_{j-1}$ j=2,…, N<br>$O_j = E(K,I_j)$ j=1,…,N<br>$C_j = P_j \oplus O_j$ j=1,….,N - 1<br>$C^*N = P^*_N \oplus MSBu(O_N)$ | $I_1$ = Nonce<br>$I_j = LSB_{b-s}(I_{j-1})\|\|C_{j-1}$ j =2,.,N<br>$O_j = E(K,I_j)$ j=1,...,N<br>$P_j = C_j \oplus O_j$ j=1,…,N - 1<br>$P^*N = C^*_N \oplus MSBu(O_N)$ |

## 2.2.5 CONTER MODE (CTR)

CTR is a "new" mode, similar to OFB, except it encrypts counter value rather than any feedback value. The main characteristics of the CTR, it must have a separate key & counter value for each plaintext block (never reused). For the chaining modes, the algorithm must complete one block of computation before starting on the next block [17]. This limits the overall throughput of the algorithm to the corresponding duration of one block encryption or decryption execution. Throughout CTR mode, the throughput is constrained only by the amount of parallelism achieved. And must ensure that key/counter values are never repeated, otherwise, they could break (OFB). The CTR facilities are shown in Fig. 7. The big advantages for CTR is efficiency,

which can do parallel encryptions in h/w or s/w, can preprocess in advance of need, good for burst high-speed links where it uses high-speed network encryptions. Too CTR has other advantages including random access to encrypted data blocks, provable security (good as other modes). The Limitations of CTR is but must ensure never reuse key/counter values.

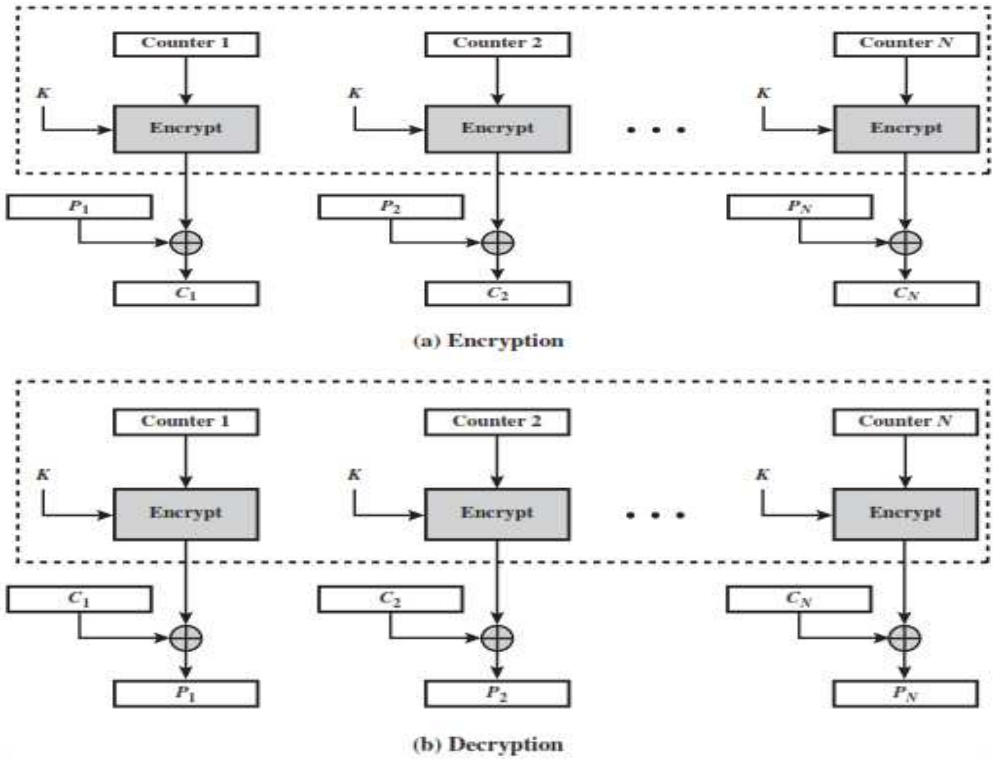



**Figure 7. Counter (CTR) Mode**

**We can define CTR mode as Follows:**

| | | |
|---|---|---|
| **CTR** | $C_j = P_j \underline{E}(K,T_j)$ j = 1,..,N – 1<br>$C^{\star}_N = P^{\star}_N$ MSBu[E(K,$T_N$)] | $C_j = P_j \underline{E}(K,T_j)$ j = 1,….,N – 1<br>$P^{\star}_N = C^{\star}_N$ MSBu[E(K,$T_N$)] |

## CONCLUSION

In this paper we have presented series of network security models with increasing levels of sophistication and demands for trusted network components. The used analysis here is vital to understanding when network components must be trusted and the type of security policy. This research has many ideas, including some examples of traditional methods in the encryption/decryption process. The triple-DES and then go searching to view some of the new models, and more advanced by five modes of operations are also investigated.

## REFERANCES


1. Osman, Ali BabikherBakheet, April 2019, "Performance Analysis of Signature - Based Network Intrusion Detection System" PhD. In Nayaf university, Network Security Department.
2. Varadharajan, 2018, "Design of a Network Security Policy Model", Hewlett-packard, U.K.
3. Jayshree, Ullal, Sep 2018, "BIG-IP logout page", senior VP of Cisco.
4. Jayshree, Ullal, Dec 1, 2015, "Automating Breach Detection For The Way Security Professionals Think", senior VP of Cisco.
5. Jayshree, Ullal, October 16, 2014 "A Role-Based Trusted Network Provides Pervasive Security and Compliance", senior VP of Cisco.
6. Wright, Jim Harmening, (2009), "Computer and Information Security", Publications Elsevier Inc Handbook Morgan Kaufmann.
7. Angus Wong and Alan Yeung, 2009, "Network Infrastructure Security", Springer.
8. Cisco Security MARS, 2008, "Security Monitoring", 1st ED., Book ISBN-10: 1-58705-270-9 ISBN-13: 978-1-58705-270-5,
9. Dale Tesch and Greg Abelar, Sep. 26 2006, "Security Threat Mitigation and Response", Cisco Press.
10. Duane De Capite, Sep. 8, 2006, "The Next Generation of Network Security", Self-Defending Networks Cisco Press. ISBN-10: 1-58705-253-9.
11. Gary Halleen, Greg Kellogg By Gary Halleen, Greg Kellogg, Jul 6, 2007, "Threat mitigation system deployment", Cisco Press.
12. Dave, Dittrich, Aug 27 2006, "Network monitoring/Intrusion Detection Systems (IDS)", the Wayback Machine, University of Washington.
13. Greg, Abelar, Sep 28 2006, "Security Threat Mitigation and Response", Understanding Cisco Security MARS By Dale Tesch, Cisco Press.
14. V. Gligoref al., Feb. 1987, “On the design and implementation of Secure Xenix workstations,” IEEE Trans. Software Eng., vol. SE-13.
15. Wilhelm, Burger, February 1987, "Networking of secure Systems", IEEE Journal on selected Arabs areas in communications, vol. 7. No. 2.
16. Eiji, Okamoto, member, IEEE, and Kazue Tanaka, February 1987, "Identity -Based Information Security Management System for Personal Computer Networks", IEEE journal on selected areas in communications, vol. 7. No. 2.
17. Stephen, T. Walker, Dec 1987, "Network security overview", Proc. Of IEEE Symposium on Security and Privacy, pp 62-76.