Volume 5, Issue 3
June 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Comparison Of Three Modes Of Cryptography Operation For Providing Security and Privacy Based on Important Factors

[1]Anita Dashti, [2] Hashem Alvandi Kheradmand,[3]Mohammad Davarpanah Jazi

[1]Department of Electrical Engineering, Graduate student of Software Engineering , Steel-of-Fooladshahr- Institute of Higher Education for postcode 8491663763

[2]Department of Electrical Engineering, Graduate student of IT Engineering , Steel-of-Fooladshahr- Institute of Higher Education for postcode 8491663763

[3]Department of Electrical Engineering, Assistant Professor, Department of Computer Engineering and Information Technology, Isfahan - Fooladshahr-Institute of Higher Education for steel - code 8491663763

E-mail: [1]Anita.Dashti2015@Gmail.com, [2]Hashem313@Gmail.com, [3]mdjazi@cc.ui.ac.ir

ABSTRACT

Cryptography is the study of secret writing that hides the content of message from unwanted persons except authenticated persons such as the sender and receiver of the message. It is also used to authenticate the correctness of message to the recipient. Today data security is the challenging issue that is used in many contexts including computers and communication. Recently cyber security attacks have certainly influenced the user sentiments. In other words, it would be prominent to say that cryptography is one way to make sure that confidentiality, authentication, integrity and availability of user data is maintained further that security and privacy of data are provided to the user. In the paper three classical modes of operation CBC, CFB and OFB have been proposed in the literature for comparison. Features of comparison that is used are block size, throughput, random access, error propagation, parallelizing, cipher type and identical plaintext. These three modes are totally studied and general comparison are provided.

Keywords: *Symmetric Encryption, Encryption, Comparative Study.*

1. INTRODUCTION

Cryptography is the art and science of protecting information from unwanted person and converting it into a form indistinguishable by its attackers when transmitted and stored. The main aim of cryptography is keeping data secure from unauthorized persons. Data cryptography is the content of the data, such as text data, image related data , audio and video related data to compose the data illegible, imperceptible or unintelligible during communication or storage called Encryption process. The reverse process of data encryption is called data Decryption.

Some security goals are provided by cryptography to avoid a security issue. Due to security advantages of cryptography, it is widely used today [2].

2. GOALS OF CRYPTOGRAPHY

Confidentiality: Just future receiver can read the message. Computer information is transmitted and only authorized parties can read it [3].

Authentication: This process proves the user's identity. The information is received by system then is checked the identity of the sender to make sure that the incoming information is from an authorized person [1].

Integrity: Only the authorized party is modifying the transmitted information or message. Nobody can change the given message [1].

Non-Repudiation: This is a mechanism to prove that the message is really sent by the right sender. If the sender denies that he doesn't send the message, this method does not allow doing any action to sender [1].

Access Control: Only the authorized parties are capable to read the given information[1].

2.1 SECURITY AGAINST ATTACK

Cryptanalysis is an art of breaking the encrypted codes that are created by applying some cryptographic algorithms. Cryptanalysis attacks can be classified as is described in following text.

Cipher-text-only attack: In cipher-text only attack, the attacker has a part of the cipher text using available information, the attacker tries to find out the corresponding key to decrypt the plain-text [4].

Known-plaintext attack: The known-plaintext attack (KPA)

Volume 5, Issue 3
June 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

is an attack model for cryptanalytic which the criminal has samples of each plain-text and its encrypted version cipher-text. These reveal any secret data like secret keys and codebooks [1].

Chosen-plaintext attack: A chosen-plain-text attack (CPA) is an associate attack model for cryptography that decides on arbitrary the plain text to be encrypted and procures the corresponding cipher-text [1].

Chosen-cipher text attack: A chosen cipher-text attack (CCA) is an attack model for scientific discipline within which the cryptologist gathers data by selecting a cipher-text and gets its decipherment beneath an unknown key [1].

Chosen-text attack: A chosen text attack is a combination of choosing plain text and chosen cipher-text attack [4].

Brute-force attack: This type of attack is a passive attack. The attacker can try all the possibilities of the key until the message is not broken. This is the very slow attack. Suppose that the message is encrypted using the 56-bit key ,then the attacker can try all the possibilities up to 255-bit [3].

Dictionary attack: The extension of the Brute-force attack is the Dictionary attack. In the Dictionary Attack, it will try also same possibilities, but take only those key bits whose chances of success will be more [3].

Timing attack: Timing Attack is a channel side attack that the attacker tries to reveal a cryptosystem by analyzing the time that is taken to execute cryptographic algorithms. Each consistent operation in a computer takes time to perform [3].

Man-in-the-middle attack: This is the type of active attacks. This differs from what is mentioned above in that it involves tricking individuals into compromise their keys. The attacker is placed in the two parties through communication channel who wish to exchange their keys for secure communication [3].

3. TYPES OF CRYPTOGRAPHY

There are several ways to classify the cryptography algorithms. The most common types are [2]:

- Secret Key Cryptography this is also called as Symmetric Key Cryptography
- Public Key Cryptography this is also called as Asymmetric Key Cryptography

3.1 Symmetric Cryptography

In this type of encryption, same key is used for both encryption and decryption process. Symmetric algorithms have the advantage of consuming few computing power and high speed working with encryption. The symmetric key encryption happens in three modes, either as a block cipher or as a stream cipher. In the block cipher mode data are divided into a couple of blocks. In stream cipher mode data are divided into small blocks such as single bits, then after the encryption takes place it would be randomized. Symmetric key cryptosystems perform faster than the asymmetric key cryptosystems. The comparative study took place for the following symmetric key encryption techniques such as the CBC, CFB and OFB classical modes of operation [5].

3.1.1 Cipher Block Chaining

If the first block has indexed, the mathematical formula for cipher block chaining will be:

$$C_i = E_K(P_i \oplus C_{i-1}), C_0 = IV$$

The mathematical formula for CBC decryption is:

$$P_i = D_K(C_i) \oplus C_{i-1}, C_0 = IV.$$

In comparison with cipher modes, the very common using mode of operation is CBC. Its main problem is that encryption is sequential, and that the message must be padded into a multiple blocks of cipher block size. One way to handle last issue is using cipher-text stealing.

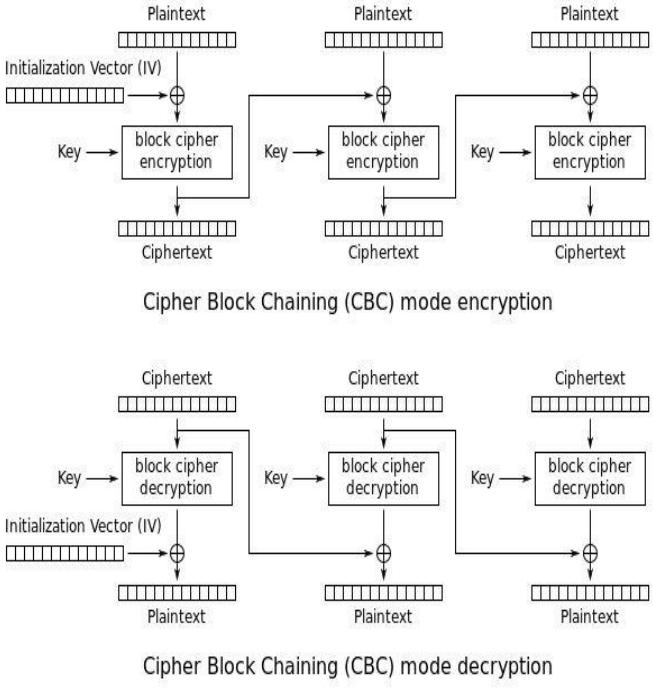


Figure 1: Cipher Block Chaining (CBC)

Decrypting with the incorrect IV causes corruption the first block of plaintext but subsequent plaintext blocks won't affect. This is because of XOR-ing each block with the cipher-text of the previous block, so previous block does not need to be decrypted before using it as the IV for the decryption of the current one. Can be figured out that a plaintext block can be

Volume 5, Issue 3
June 2016

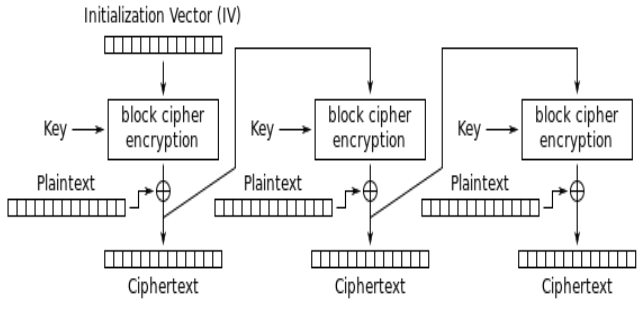
ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

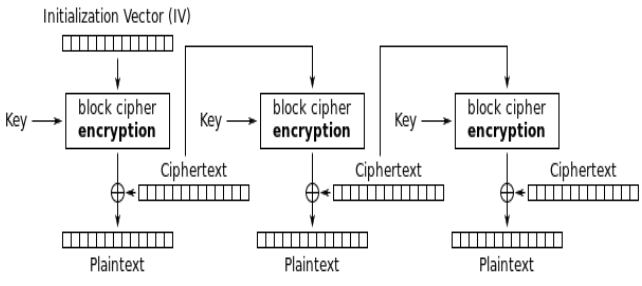
recovered from two adjacent blocks of cipher-text. So decryption can be parallelized. Note that a one-bit change to the cipher-text will cause complete corruption of the corresponding block of plaintext, and will invert the corresponding bit in the following block of plaintext, but the rest of the blocks will remain intact. This peculiarity is exploited in different padding oracle attacks, such as POODLE. Explicit IVs take advantage of that property by pending a single random block into the plaintext. Encryption is done as normal, except the IV that does not need to be communicated to the decryption routine. Whatever IV decryption uses, only the random block is "corrupted". It can be safely discarded and the rest of the decryption will be the original plaintext.

3.1.2 Cipher-text Feedback

The DES scheme is a block cipher mode technique that is used *b*-bit blocks. It would be possible to convert DES into a stream cipher by using either the CFB or OFB mode. A stream cipher does not need to pad a message block and also can be operated in real time. Therefore, if a character stream wants to be transmitted, each character can quickly be encrypted and transmitted. One important property of a stream cipher mode is that the cipher-text would be the same length size as the plaintext. So if 8-bit characters want to be transmitted, each character should be encrypted to develop an 8-bit cipher-text output. If more than 8 bits are produced, transmission capacity would be wasted. In figure 2 CFB scheme is demonstrated. In this scheme the unit of transmission assumed as bits and common value assumed as $s = 8$. As shown in the figure, the units of plaintext are chained to each other, so that the cipher-text of a plaintext is a function of all the preceding plaintext. In this case, the plaintext is divided into *segments* of *s*-bit [4].



Cipher Feedback (CFB) mode encryption

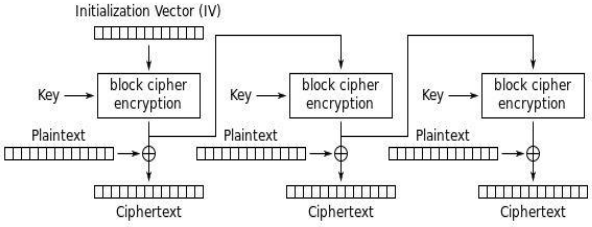


Cipher Feedback (CFB) mode decryption

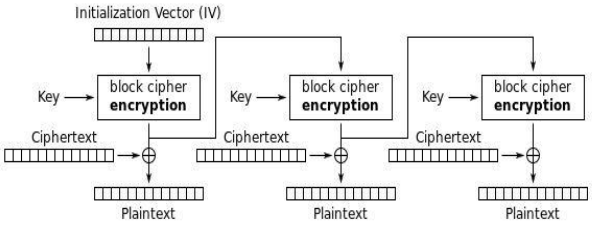
Figure 2: Cipher Feedback (CFB) Mode

First, consider encryption. The input to the encryption function is a *b*-bit shift register that is initially set to some initialization vectors that is called IV. The leftmost *s*-bits of the output of the encryption function will be XORed with the first segment of plaintext P_1 to produce the first unit of cipher-text C_1, which then will be transmitted over the network. After that, the contents of the shift register will be shifted left by *s*-bits and C_1 will be placed in the rightmost *s*-bits of the shift register. This process will continue till all plaintext units have been encrypted. For decryption, the same process will perform, except that the received cipher-text unit will be XORed with the output of the encryption function to produce the plaintext unit. Note that in this process the *encryption* function should be used. To explain that, assume $_S(X)$ to define as the most significant *s* bits of *X*. Then C1 is produced by $C_1 = P_1 \oplus [E(K, IV)]$ Therefore, to gain P1 it would be $P_1 = C_1 \oplus [E(K, IV)]$. And in this way other steps of process will be performed [4].

3.1.3 Output Feedback



Output Feedback (OFB) mode encryption



Output Feedback (OFB) mode decryption

Figure 3: Output Feedback (OFB) Mode

The Output Feedback mode makes a block cipher into a synchronous stream cipher. It generates key-stream blocks, which will then be XORed with the plaintext blocks for getting the cipher-text block. Just as other stream ciphers, flipping a bit in the cipher-text produces a flipped bit in the plaintext at the same location. This property will allow many errors, correcting codes to function normally even when applied before encryption. Because of the symmetric of the XOR operation, encryption and decryption will be the same:

Volume 5, Issue 3
June 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

$$C_j = P_j \oplus O_j$$
$$P_j = C_j \oplus O_j$$
$$O_j = E_K(I_j)$$
$$I_j = O_{j-1}$$
$$I_0 = \mathrm{IV}$$

Each OFB cipher operation depends on all previous ones, so cannot be performed in parallel. However, because the plaintext or cipher-text is only used for the final XOR, the block cipher operations should be performed in advance, allowing the final step to be performed in parallel once the plaintext or cipher-text is available. It is possible to obtain an OFB mode key-stream by using CBC mode with a constant string of zeroes as input. This can be useful, because it allows the usage of fast hardware implementations of CBC mode for OFB mode encryption. Using OFB mode with a partial block as feedback like CFB mode will reduce the average cycle length by a factor of 2^{32} or more.

3.2 Asymmetric Cryptography

Asymmetric key encryption is a technique in which different keys are for encryption and decryption process. One key is known as public and second is kept as private. If the encryption key is first published then the system enables private communication [6]. If the decryption key is the one published then the system will act like a signature verifier of documents that are locked by the owner of the private key [1].

4. Comparing Classical Modes Of Operation

Block ciphers are basic building blocks for providing data security. To enhance the security of cipher, block ciphers are used in different modes of operation. These modes are named as follows.

1. Electronic Code Book that's known as ECB.
2. Cipher Block Chaining that's known as CBC.
3. Cipher Feedback that's known as CFB.
4. Output Feedback that's known as OFB.
5. Counter that's known as CTR.
6. Galois/Counter Mode that's known as GCM.

As shown in Table 1 three modes of operation CBC, OFB and CFB are compared using 9 factors.

Table 1: Comparison Classical Modes Of Operation

Factors	Modes		
	CBC	**CFB**	**OFB**
Defined for	DES	DES	DES
Block size	64-bit	64-bit	64-bit
Throughput	When widely used, mode's privacy-only security properties result in frequent misuse.	The rate of enciphering and deciphering is reduced by a factor of n/r, that is, for every r bits of output the algorithm must carry out one n-bit enciphering operation.	Encryption and decryption inefficient from being inherently serial.
parallelizing	Yes, encryption is parallelizable	Yes, encryption is parallelizable	No
Difference	IV need not be secret, but its integrity should be protected.	IV need not be secret (XOR ed with x1)	IV need not be secret, but should be changed if a previously used key is to be used again
Identical plaintext	changing IV or the first plaintext block results in different cipher-texts.	Same as CBC	Same as BC
Error propagation	Single bit error on c_j may flip the corresponding bit on x_{j+1}, but changes x_j significantly.	Single bit error on c_j may flip the corresponding bit on x_j, but changes x_{j+1} significantly.	Single bit error on c_j may only affect the corresponding bit of x_j
Random Access	Yes, allows for Cipher-text	Yes, allows for Cipher-text	No
Cipher Type	Symmetric Block Cipher	Symmetric Block Cipher	Cipher Type

Volume 5, Issue 3
June 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

5. IMPELIMENTATION CODES

CBC
Monte Carlo Algorithm:
Key[0]= Key
IV[0]= IV
PT[0]= PT
For i = 0 to 99
Output Key[i]
Output IV[i]
Output PT[0]
For j = 0 to 999
If (j=0)
CT[j] = AES(Key[i], IV[i], PT[j])
PT[j+1] = IV[i]
Else
CT[j] = AES(Key[i], PT[j])
PT[j+1] = CT[j-1]
Output CT[j]
If (keylen = 128)
Key[i+1] = Key[i] xor CT[j]
If (keylen = 192)
Key[i+1] = Key[i] xor (last 64-bits of CT[j-1] || CT[j])
If (keylen = 256)
Key[i+1] = Key[i] xor (CT[j-1] || CT[j])
IV[i+1] = CT[j]
PT[0] = CT[j-1]

OFB
Monte Carlo Algorithm:
Key[0] = Key
IV[0] = IV
PT[0] = PT
For i = 0 to 99
Output Key[i]
Output IV[i]
Output PT[0]
For j = 0 to 999
If (j=0)
CT[j] = AES(Key[i], IV[i], PT[j])
PT[j+1] = IV[i]
Else
CT[j] = AES(Key[i], PT[j])
PT[j+1] = CT[j-1]
Output CT[j]
If (keylen = 128)
Key[i+1] = Key[i] xor CT[j]
If (keylen = 192)
Key[i+1] = Key[i] xor (last 64-bits of CT[j-1] || CT[j])
If (keylen = 256)
Key[i+1] = Key[i] xor (CT[j-1] || CT[j])
IV[i+1] = CT[j]
PT[0] = CT[j-1]

CFB
Monte Carlo Algorithm:
Key[0] = Key
IV[0] = IV
PT[0] = PT
For i = 0 to 99
Output Key[i]
Output IV[i]
Output PT[0]
For j = 0 to 999
If (j=0)
CT[j] = AES(Key[i], IV[i], PT[j])
PT[j+1] = BitJ(IV[i])
Else
CT[j] = AES(Key[i], PT[j])
If (j<128)
PT[j+1] = BitJ(IV[i])
Else
PT[j+1] = CT[j-128]
Output CT[j]
If (keylen = 128)
Key[i+1] = Key[i] xor (CT[j-127] || CT[j-126] || … || CT[j])
If (keylen = 192)
Key[i+1] = Key[i] xor (CT[j-191] || CT[j-190] || … || CT[j])
If (keylen = 256)
Key[i+1] = Key[i] xor (CT[j-255] || CT[j-254] || … || CT[j]) IV[i+1] = (CT[j-127] || CT[j-126] || … || CT[j])
PT[0] = CT[j-128]

6. CONCLUSION AND FUTURE WORK

In this paper, we generally studied three classical modes of operation CBC, OFB and CFB. Good to say that the CBC is the most commonly used modes and other modes perform in the same way as the CBC does as well. Choosing an encryption mode affects encryption/decryption speed, bit flips and error propagation, So for a better result first chooses an appropriate cryptography algorithm then use a good mode of operation. In future, it can be possible to compare more factors in these three modes of operation and also it would be possible to do research on analyzing the performance of the three modes of operation.

REFERENCES

[1]. "A Comparative Performance Analysis of DES and Blowfish Symmetric Algorithm", Srinivas B.L, Anish Shanbhag, International Journal of Innovative Research in Computer and Communication Engineering Volume 2, Special Issue 5, October 2014.

[2]. "Comparative Study of Symmetric and Asymmetric Cryptography Techniques", Ritu Tripathi, Sanjay Agrawal, International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 6, June 2014.

[3]. "Survey on Modular Attack on RSA Algorithm", Satish N .chalurkari ,Nileshkhochare ,B.B. mashram, IJCEM International Journal of Computational Engineering & Management, Vol. 14, October 2011.

[4]. "Cryptography and network security", ITL Education Solution ltd, 4th edition, November 2005.

[5]. "Performance Evaluation of Cryptographic Algorithms", International Journal of Computer Applications, Volume 41– No.7, March 2012.

[6]. "A Survey on Various Most Common Encryption Techniques", E .Thambiraja ,G. Ramesh ,Dr. R. Umarani, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012.