CBBC : A New Mode Of Chaining Blocks Before Cipher

N. Taboudjemat, O. Nouali, A. Berbar, R. Saadi
CERIST
E-mail:(nnouali, onouali)@mail.cerist.dz

Introduction

Nowadays, the world is like a little village thanks to the Internet that transports a big amount of information per second in the form of data exchange, banking transactions or many other types of messages. Electronic message exchange is a privileged target for attackers. The threats are numerous and can be intentional or accidental [14]. Accidental threats are errors caused by users manipulating the system. For example, sending by error a confidential message to a wrong addressee. On the other hand, intentional threats come from a harmful source. They can be passive (such as eavesdropping) or active (such as modifying the message content or falsifying its source information). The different attacks result in confidentiality, integrity and authentication breaches [12].

Cryptography is a basic mechanism in the security domain and its use occurs in several aspects of Internet security. Cryptography is a set of techniques offering means of transforming a plain text into an unintelligible one. Only the authorized receiver is able to decrypt the original text.

This paper describes a cryptographic solution offering a high level security thanks to two new ciphering modes. These modes are derived from the well-known chaining mode CBC (Chaining Bloc Cipher). CBC and other chaining bloc modes indicate the way of applying the ciphering technique to a text cut into blocks. The new chaining modes are named CBBC (Chaining Bloc Before Cipher) and CMBBC (Chaining and Mixing Bloc Before Cipher). They allow the combination of two ciphering algorithms at the same time instead of using only one as it is the case in the traditional solutions [2].

1- Ciphering techniques

Cryptography is the science of securing data with cryptographic algorithms. It allows to save or transmit on a network sensitive data in a secured and protected manner. Cryptographic algorithms are mathematical functions used in the ciphering and deciphering processes along with a key. Ciphering is the process of transforming a plaintext into an incomprehensive one and deciphering is the opposite process [19].

There are two principle classes of algorithms: symmetric or secret key algorithms and asymmetric or public key algorithms. The first class utilizes a single and same key for ciphering and deciphering. DES (Data Encryption Standard), TWOFISH and BLOWFISH are examples of the most known symmetric algorithms [4][10][8]. These algorithms work on a bloc basis; that is the plaintext is divided into blocks that are ciphered one by one according to a chaining mode. ECB (Electronic Code Book) and CBC (Chaining Bloc Cipher) are the most popular chaining modes [10][14]. Secret key algorithms are based on simple operations (arithmetic and permutations) and are known to be very rapid and strong, but their inconvenient is that they produce a big set of keys to manage. For n users there are $(n^2-n)/2$ keys to exchange in a reliable and secret manner. This has motivated the introduction of the second class of algorithms which utilize two different keys; a public key for encryption and a private one for decryption. The private key is kept secret, only its owner knows it [10]. There is no relation between the two key so no one can deduce one from the other. RSA (Rivest Shamir Adleman), Diffie-Helman are the most popular asymmetric algorithms [17]. This type of algorithm are based on complex mathematical theories such as factorization of integers, discontinuous logarithm, elliptic curves, etc. They use big keys to ensure security but they are 100 times slower than symmetric algorithms. In practice, the two types of algorithms, that is, symmetric and asymmetric algorithms are combined to capture the advantages of the both.

2- The ciphering modes of operation

A block cipher (that is the cipher algorithm) encrypts plaintext in fixed-size n-bit blocks (often n=64). For messages exceeding n bits, the simplest approach is to partition the message into n-bit blocks and encrypt each separately. This electronic code book (ECB) mode has disadvantages in most applications, motivating other modes of operation on larger messages. One of the most common modes is CBC (Cipher Block Chaining). CBC involves use of an n-bit initialization vector (denoted IV) [10][8].

In the following, E denotes the encryption function parameterized by key K, E^{-1}denotes decryption. A plaintext message $x=x_1....x_t$ is assumed to consist of n-bit blocks. The CBC mode follows the algorithm [13]:

Input : K-bit key K; n-bit IV; n-bit plaintext blocks $x_1,\dots,x_t$.

Output : produce cipher text blocks $c_1,....c_t$; decrypt to recover plaintext.

Encryption : $C_0 \leftarrow IV.\ For\ 1 \leq j \leq t,\ c_j \leftarrow E_k\,(c_{j-1} \oplus x_j)$

Decryption : $C_0 \leftarrow IV.\ For\ 1 \leq j \leq t,\ ,x_j \leftarrow c_{j-1} \oplus E_k^{-1}(c_j).$

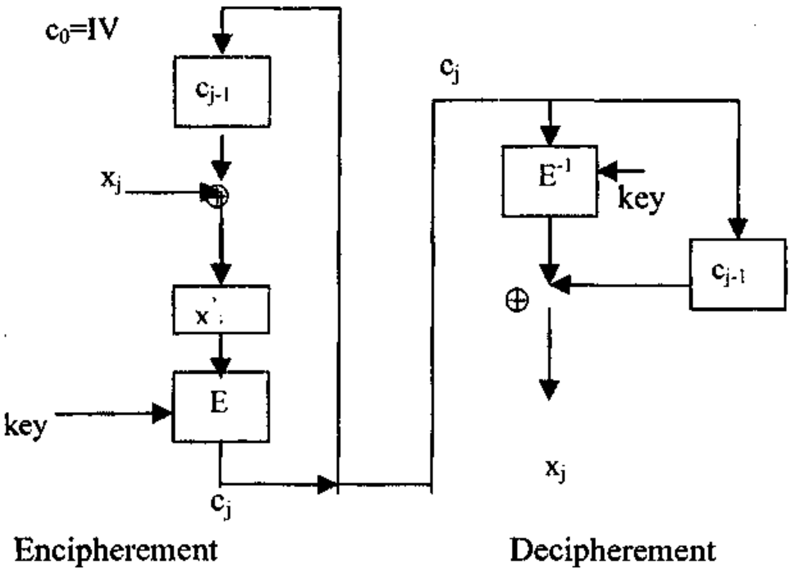

Figure 1 : The CBBC mode

In order to produce a more secure mode of ciphering we have made some modifications on the CBC (see figure 1). The results are two new modes we named :

- CBBC that is Chaining Bloc Before Cipher (see figure 2),
- CMBBC that is Chaining and Mixing Bloc Before Cipher.

3- The CBBC mode

The first modification we applied to CBC concerns the chaining dependencies. In the CBC mode the chaining mechanism causes cipher text c_j to depend on x_j and all preceding blocks. Consequently, rearranging the order of cipher text blocks affects decryption. Proper decryption of a correct cipher text block requires a correct preceding cipher text block. In the CBBC mode cipher text c_j depends on x_j XORed with x'_{j-1}, which

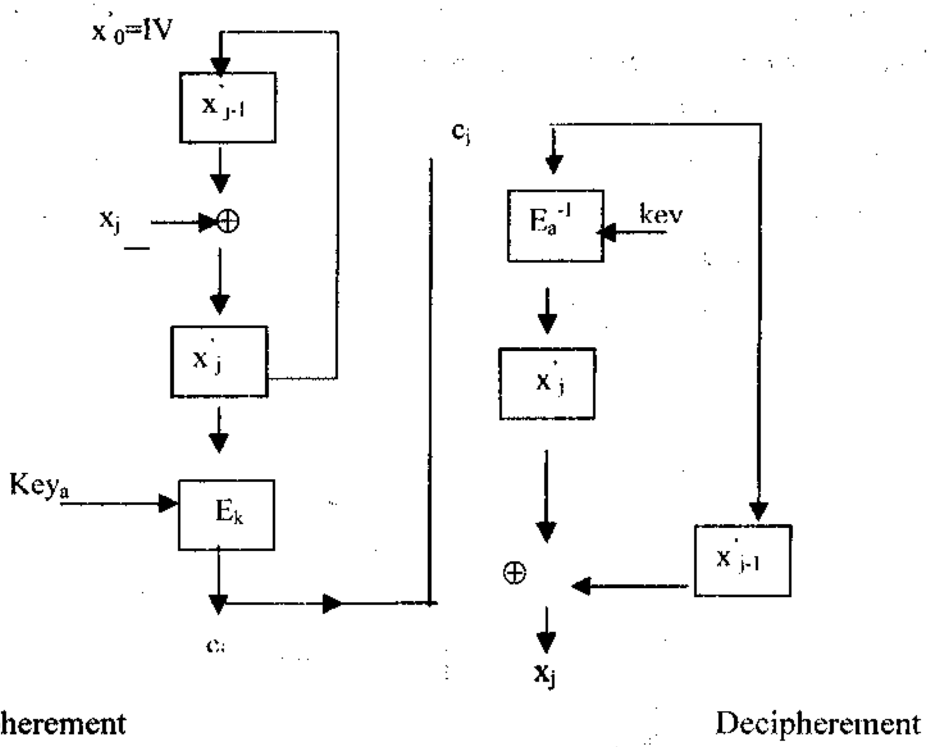

Figure 2 : The CBBC mode

in turn is the result of an XOR operation between x_{j-1} and x'_{j-2}, and so on .... x'_0 equals the initial vector *IV*. There are no dependencies between the cipher text blocks. This means that a XOR is operated between two plaintext blocks instead of a plaintext block and the last ciphered bloc as it is done by the CBC mode. The **second modification** is to encipher the message by alternating two algorithms, that is c_j is obtained from E_1 and c_{j+1} from E_2 (E_1 et E_2 are two different n-bits block cipher functions or algorithms). **In addition,** the first algorithm to start with is chosen at random. Consequently :

- rearranging the order of cipher text blocks does not affects decryption,
- a bit error in cipher text block c_j does not affect decipherment of other blocks as it is the case in the CBC mode.
- if an attacker discovers one of the two keys, he can not read either the message nor the block he has just decrypted for two reasons: The first reason is that the previous block of the message is enciphered with a different key, so one must discover this second key before deciphering the block. The second reason is that a XOR operation has been applied between the hijacked block and the previous plain block. So, to read the hijacked block one needs to know the previous plain block which in turn is XORed with a block that was ciphered by a different algorithm.

4- The CMBBC mode

The CMBBC mode is nearly the same as the previous mode. However there is a difference between the two modes. With the CBBC mode the enciphering is done in an alternate manner that is block by block. In the CMBBC mode, blocks will not be enciphered one by one, but a number of *m* blocks will be ciphered by algorithm1 and then *m* other blocks by algorithm2, etc. The number *m*, is a randomly generated number. In addition, as in the precedent method, the ciphering order of the blocks is clouded by the following chaining method : block1, block n+1, block 2, block n+2, ...block n, block 2N, ..., as it is shown in figure 3. In this manner, the attacker will never know neither the position of the blocks nor the algorithm used to cipher each block. This makes cryptanalysis more difficult.

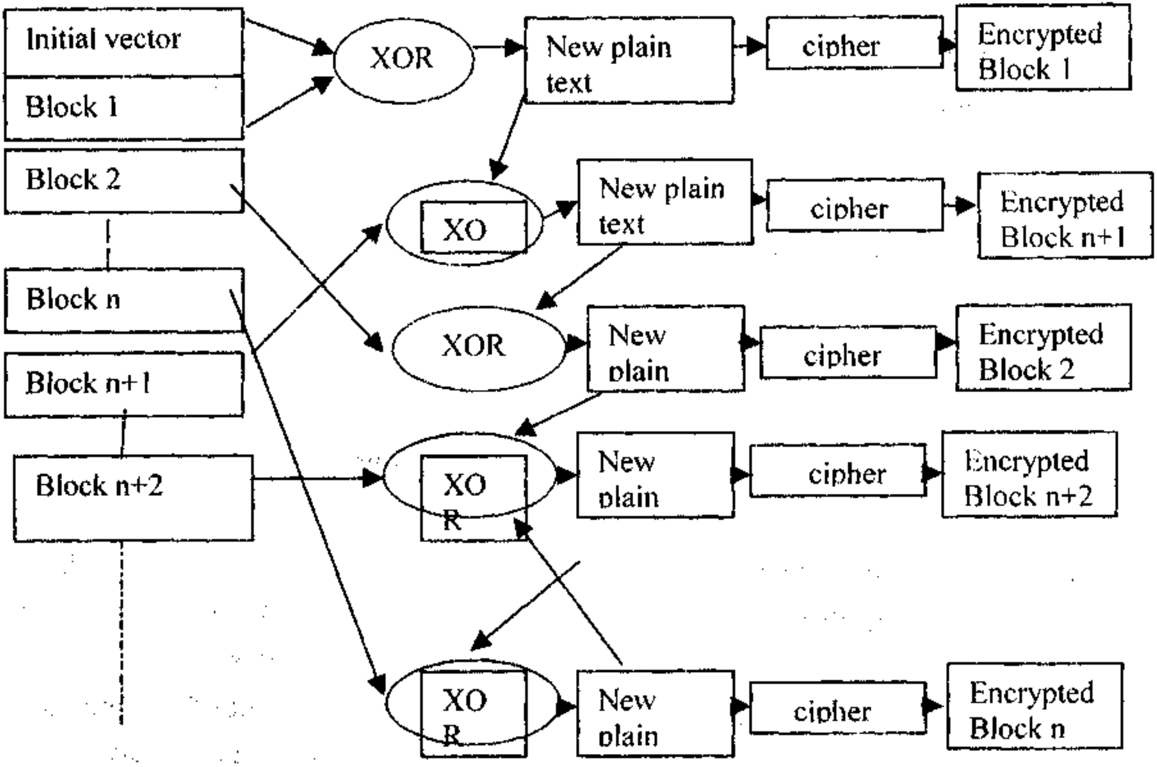

Figure 3 : The CMBBC mode

Example : Let us have a message composed of 5 blocks, and *m*=3. Ciphering is done as it follows: algorithm 1 ciphers blocks 1,2,3 and algorithm 2 ciphers blocks 4 and 5 (see figure 4).

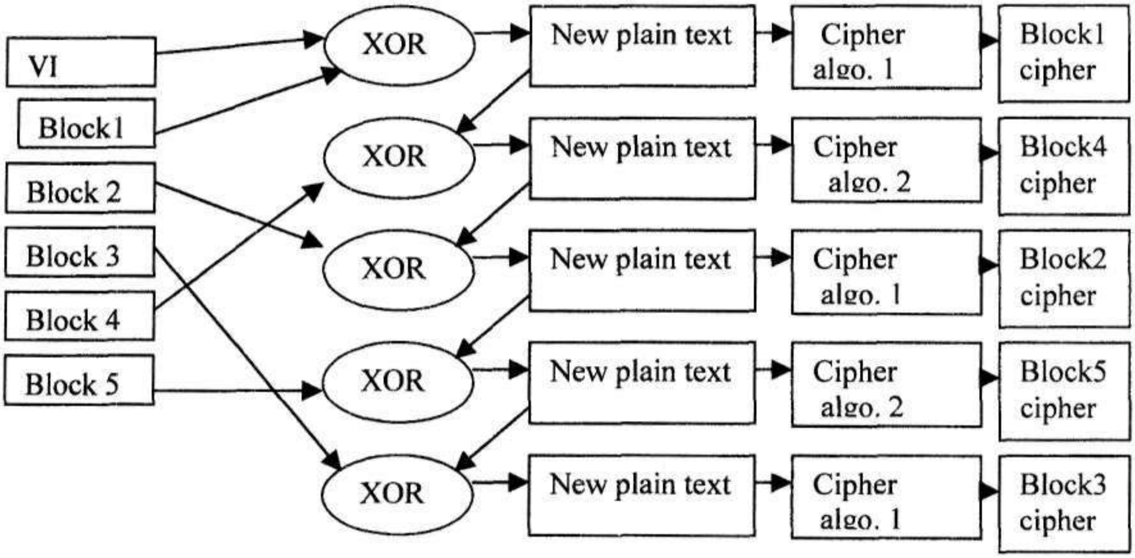

***Figure 4** : The CMBBC mode applied for a message of 5 blocks*

The number m is generated according to the formula : $m=1+nb$ *modulo* P, with $P=size(message)/2$, and nb a randomly generated number from time in milliseconds and position of the mouse pointer on the screen. Thus, n will be always greater than 1 and smaller than P; this means that their will be at least two computing rounds [2].

The drawback of this method is that it is slower than the previous one, so the ciphering takes more time. For this reason we chose to use it as an optional choice for the medium and high security levels.

5- Application to message security

We experienced the new chaining modes in a system designed for electronic message security. In this section we outline de system functionalities related to the confidentiality issue.

Our system offers tree levels of security :

- low security level,
- medium security level,
- and, high security level.

Each level uses a set of algorithms.

The low level that offers security for personal messages, uses one out of four algorithms with the CBC mode :

- BLOWFISH with a key size of 256 bits and blocks of 128 bits.
- TWOFISH with a key size of 256 bits and blocks of 128 bits.
- 3-DES with a key size of 192 bits and blocks of 64 bits.
- IDEA with a key size of 128 bits and blocks of 64 bits.

The medium level uses two algorithms at the same time with the CBBC or CMBBC mode as the user decides :

- 3-DES with a key size of 192 bits and blocks of 64 bits.
- IDEA with a key size of 128 bits and blocks of 64 bits.

The high level also uses two algorithms and lets the user choose between the CBBC and the CMBBC modes :

- BLOWFISH with the key size of 256 bits and blocks of 128 bits.
- TWOFISH with the key size of 256 bits and blocks of 128 bits.

Conclusion

This paper deals with security problems that messages can encounter during their transmission on the NET. We emphasis on the fact that our contribution is to design and implement new chaining modes derived from the famous CBC (Chaining Bloc Cipher). We called these modes CBBC (Chaining Bloc Before Cipher) and CMBBC (Chaining and Mixing Bloc Before Cipher) and demonstrated their efficiency in sections 3 and 4. These two modes allowed us to strengthen enciphering methods by combining two algorithms at the same time in a manner that complicates the cryptanalysis task.

Bibliographies

[1] R.Balter & S.Krakowiak & J.P.Banâtre. Construction des systèmes
d'exploitation répartis,
INA France 1991.

[2] B. Berbar, R. Saadi, N. Nouali, O. Nouali. Protection de la messagerie électronique par des méthodes cryptographiques, mémoire de fin d'études d'ingénieurs, USTHB, CERIST, octobre 2000.

[3] Dr. Dobb's Journal. http://www.contentepane.com/blowfish/analysis.html . Septembre 1995.

[4] Miller freeman. The politics of cryptography. http://www.performancecomputing.com/features/9910f1.shtml, October 1999

[5] Barbara Guttman & Robert Bagwill. Internet Security Policy : A Technical Guide. NIST. Special publication 800-xx, Jully 31 1997.

[6] Reto E.Haeni. Information warfare, an introduction, research report, George Washington. Univerity, Janvier 1997.

[7] Bertrand Ibrahim. Rapport Internet et sécurité, Université de Genève. 05/06/1998

[8] Iren Kam. Network security. Department of Computer Science Rensselaer Polytechnic. Institute USA . www.cs.rpi.edu/~iren/project.html 1997.

[9] Lorraine Kauffman. Certicom ECC challenge inroduction, Certicom Corp. http://www.certicom.com/ellypyticcurves/f001.htm, Janvier 2000.

[10] Matthieu Klein. PGP et applications cryptographiques. Rapport de licence EEA sur les techniques de chiffrement. http://www.hmet.fr/~matthieu/crypto/crypto.html, 03/04/2000.

[11] Marshall D. Abrams and Harold J.Podell. Cryptography, 1999.

[12] Carolyn Meinel, Ronald Rivest. La sécurité sur Internet N°260 http://www.pourlascience.com/numerous/pls-260/internet.html. Juin 99.

[13] Alfred J.Menzus, Paul C.Van Oorschot, Scott A.Vanstone. Handbook of applied cryptography, By CRC Press, Inc. 1997.

[14] Nabil Sahli. A synthesis of state of the art in Internet security and guidelines for developing countries, Proc of 5th conf of Computer Communication, Africom CCDC'98, Tunisia, 20-22 October 1998.

[15] Bruce Schneier. Cryptographie appliquée : algorithmes protocoles et codes sources, Traduction de Laurent Vienol. 2eme édition Paris 1997, ISBN : 2-84180-036-9.

[16] Introduction à la sécurité. http://xtream.online.fr/project/securite.html . 1999.

[17] SSH communication security. http://www.ssh.fi/tech/crypto/algorithms.html, Janvier 2000.

[18] Bruce Schneier, JhonKelsey, Neils Ferguson, Doug Whiting, David Wagner. Twofish : a 128 bits cypher . http://www.counterpane.com/twofish.ps.zip, Juin 1998.

[19] Phill Zimmerman . Introduction à la cryptographie , 1998.