2011 UKSim 13th International Conference on Modelling and Simulation

A Competitive Study of Cryptography Techniques over Block Cipher

Ashwak M. AL-Abiachi, Faudziah Ahmad, Ku Ruhana
Information Technology Department, University Utara Malaysia, 06010, Sintok, Malaysia
ashwakalabaichi2007@yahoo.com, fudz@uum.edu.my, ruhana@uum.edu.my

Abstract—**The complexity of cryptography does not allow many people to actually understand the motivations and therefore available for practicing security cryptography. Cryptography process seeks to distribute an estimation of basic cryptographic primitives across a number of confluences in order to reduce security assumptions on individual nodes, which establish a level of fault-tolerance opposing to the node alteration. In a progressively networked and distributed communications environment, there are more and more useful situations where the ability to distribute a computation between a number of unlike network intersections is needed. The reason back to the efficiency (separate nodes perform distinct tasks), fault-tolerance (if some nodes are unavailable then others can perform the task) and security (the trust required to perform the task is shared between nodes) that order differently. Hence, this paper aims to describe and review the different research that has done toward text encryption and description in the block cipher. Moreover, this paper suggests a cryptography model in the block cipher.**

Keywords: **Cryptography, text encryption, block cipher, AES**

I. INTRODUCTION

Unclassified nature of the algorithm cannot be stressed enough. However, by publishing the algorithm, it gives the cryptographer choices to be seen by a wide range of academic cryptography, keen to break into the system to publish articles demonstrating how smart they are. The real secret is that the key and its length are very important, considering a simple combination is safer. The general principle is that figures are inserted in sequence and the key is secret. A key length of two digit means that there are 100 possibilities. A three-digit key length is 1000 possibilities and a key length of six figures means a million. As longer the key is, with greater workload (work factor) that the cryptanalyst has to do. Work factor to break the system by the exhaustive search in the digit space is exponential in relation to the key length [1]. The secret comes from having a strong algorithm (but public) and a long key. To prevent the younger brother to read other mail, there are enough 64-bit keys. To keep at distance powerful enemies the needed are at least 256 bits keys [2].

Encryption methods have historically been divided into two categories: substitution ciphers and transposition ciphers. Stallings had explained each of these ciphers as essential information for understanding modern cryptography [3].

An example of encryption algorithms is AES (Rijndael) which identifies as a symmetric algorithm. This means that the encryption key can be calculated from the corresponding decryption and vice versa [4]. Security an algorithm based on symmetric key, which must be remains secret [5]. The AES block cipher as acting in plaintext in groups of each bit time which are called blocks [6]. Typical size of a block is 64 bits. Each round transformation consists of three separate transformations called layers:

- Linear mixing layer;
- Non-linear layer;
- Key addition layer.

Before the first round of AES processing algorithms, a key addition layer takes place. The linear mixing layer of the final round is different than the other rounds. Each round of treatment consists of four different transformations that compose 3 layers [7].

Round (State, RoundKey) {ByteSub (State); ShiftRow (State); MixColumn (State); AddRoundKey (State, RoundKey);}The final round is defined as follows:
FinalRound (State, RoundKey) {{ByteSub (State); ShiftRow (State); AddRoundKey (State, RoundKey);}

However, AES is an iterative algorithm with variable size block processing and key which can be 128, 192 or 256 bits. The interim results of the algorithm after each transformation called State [8]. Each State is expressed as a rectangular table of data bytes [9]. The table blow has 4 rows, while the number of batteries (NB) is the size of the block processing divided by 32. Similarly, the encryption key (cipher key) expressed as rectangular table with data bytes. The table has 4 rows and number of columns [10] is the key length divided by 32. Each table element is one byte.

$a_{0.0}$	$a_{0.1}$	$a_{0.2}$	$a_{0.3}$	$a_{0.4}$	$a_{0,5}$
$a_{1.0}$	$a_{1.1}$	$a_{1.2}$	$a_{1.3}$	$a_{1.4}$	$a_{1,5}$
$a_{2.0}$	$a_{2.1}$	$a_{2.2}$	$a_{2.3}$	$a_{2.4}$	$a_{2.5}$
$a_{3.0}$	$a_{3.1}$	$a_{3.2}$	$a_{3.3}$	$a_{3.4}$	$a_{3.5}$

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$

Table1: State (with Nb = 6) and encryption key (with Nk = 4)

978-0-7695-4376-5/11 $26.00 © 2011 IEEE
DOI 10.1109/UKSIM.2011.85

IEEE computer society

Moreover, each column is referred as "word" or "4-byte vector". Each table can be considered as one-dimensional table of elements "4-byte vectors". The entrance and exit of AES can be regarded as dimensional data tables with 8-bit (byte) numbered from 4 * Nb-1. Similarly, the key numbered 0 to 4 * Nk-1. H entrance cipher (plaintext) is shown in bytes of the table with the State series:

The number of laps made by the algorithm denoted by Nr and depends on the values Nb and Nk as shown in table 1.

$a_{0,0}, a_{1,0}, a_{2,0}, a_{3,0}, a_{0,1}, a_{1,1}, a_{2,1}, a_{3,1}, a_{4,1}, \dots$ (1)

*While byte key shown in the table key in the order:

$k_{0,0}, k_{1,0}, k_{2,0}, k_{3,0}, k_{0,1}, k_{1,1}, k_{2,1}, k_{3,1}, k_{4,1}, \dots$(2)

Nr	Nb=4	Nb=6	Nb=8
Nk=4	10	12	14
Nk=6	12	12	14
Nk=8	14	14	14

Table 2: The values of Nr, Nb, Nk

A block cipher cryptosystem consists of two algorithms, the encryption algorithm and decryption algorithm that are illustrated in Figure 1. The encryption algorithm takes as input an n-bit plaintext M and a k-bit key K and outputs an n-bit ciphertext C; the decryption algorithm takes as input an n-bit ciphertext C and a k-bit key K and outputs an n-bit plaintext M [11]. For any fixed key, the decryption algorithm acts as the inverse process of the encryption algorithm as in following equation (1.1), (1.2).

C=Ek(M) ------------------ (1.3)

M=Dk (C) =E-1(Ek(M)) ----------- (1.4)

The block cipher breaks M into successive blocks M1, M2, and enciphers each M1 with the same key K; that is as in equation (1.5).

Ek(M)=Ek(M1) Ek(M2)----------- (1.5)

Typically, each block is several characters long. Two important block ciphers classes are substitution and transposition ciphers. Simple substitution and homophonic substitution ciphers are blocks ciphers even thought the unit of encryption is a single character. This is due to the same key being used for each character [12].

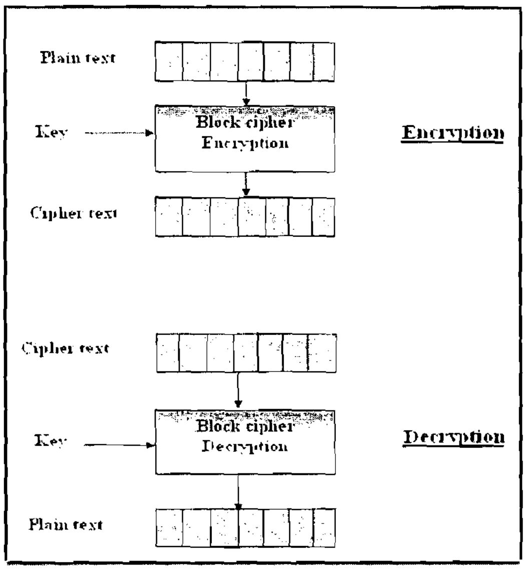

Figure 1: The encryption and decryption operations in block cipher algorithm (ref...)

Several groups of researchers that have analyzed some of the block algorithms already found a way to determine their strength or weakness. Apparently, there are some properties that determine the block algorithms strength or weakness.

- Complementation

The complexity of a brute-force attack is reduced factor of two by using this complementation property. The simple relation can be defined by the following rule IF Ek (P) = C THEN EK' (P') = C' P', C', and K' are the bit-wise complements of P, C and K [13].

There are no simple relations in a high-quality block cipher. Weaknesses in the block cipher are created by this property. An example that has this property is the DES algorithm.

- The Strict Avalanche Criteria (SAC)

The avalanche effect is a property that seems to be very important: it deals with the number of S-Box output bits change when the subsets of the inputs bits are changed.

Conditions can be easily imposed on the Boolean function to satisfy particular avalanche criteria but the difficult task is constructing them [14].

SAC guarantees that exactly half of the output bits change when one input bit is changed [15].

II. Existing Issues

Generally, the utilization of the encryption techniques has raises different security issues, which consisted mostly on how to effectively manage the encryption keys to ensure that they are safeguarded throughout their life cycle and are protected from unauthorized disclosure and modification.

Encryption keys are a sequence of symbols used with a cryptographic algorithm, which enables encryption and decryption. It is imperative that an efficient key management program be established and facilitated throughout public safety agencies. Key management ensures that critical and sensitive radio transmissions are protected with proper encryption methods and that encryption keys are controlled and securely stored during their life cycle. For purposes of this report, encryption is defined as the process of transforming plain text into unintelligible form by using a cryptographic system. The cryptosystem is hardware and software providing the means to encrypt and decrypt transmissions. Figure 2 presents a basic encryption concept.

The basic meteorological of encryption comprise the algorithm (i.e., a mode of changing information), the key (i.e., a secret introducing point for the algorithm), and the key authority (i.e., key management). The key is characteristically recognized as a binary number used with a cryptographic algorithm to authorize the encryption and decryption of information over the block cipher. The key jurisdictions the algorithmic alteration executed to information transmission during encryption and description process that must be anticipated so that a corresponding decryption algorithm can backtrack the operation by employing a suitable key. Several reasons in the encryption of information over block cipher are observed in terms of key management, which known as an important issue to the public safety community, most of these issues addressed the following:

- Difficulties in addressing the security issues regarding encryption key management;
- Lacks in providing a suitable details about the different threats in terms of decision makers on the importance of key management;
- Difficulties in generating the suitable recommendations for establishing proper key management.

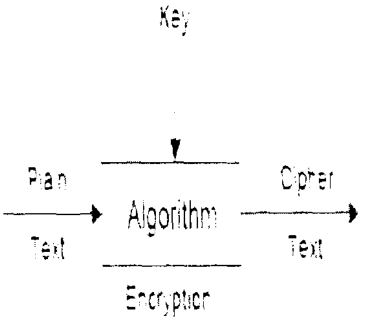

Figure 2: Basic Encryption Concept

III. RELATED WORKS

Chan & Fekri develooped a new private key cryptosystem based on the finite-field wavelet. The encryption and decryption are performed by the synthesis and analysis banks of the nonlinear finite-field wavelet transform whose filter coefficients are determined by the keys of the users. Authors illustrate the polyphone representation of the wavelets to introduce a shared key mechanism for the wavelet cryptosystem. As well as adopt the wavelets that operate over GF (256) and a nonlinear device that performs a mapping on the field elements to their inverse in the field. The block cipher system has a key length of 16 symbols (128 bits) and an input block size of 30 symbols (240 bits). To evaluate the efficiency of the developed two-round wavelet cryptographic scheme, the study also has compared with DES and AES. The results indicated that the wavelet cryptosystem has comparable computational complexity to AES and approximately half the complexity of DES. The security is tied to the length of the wavelet basis function and to the nonlinearity within the wavelet transform. Finally, Chan & Fekri conclude that the lowest complexity of any of these attacks is greater than an exhaustive key search [11].

Another study by Mousa & Hamad invistigates the analysis process of the effect of different parameters of the RC4 encryption algorithm that was performed to illustrate the performance of RC4 algorithm based on changing some of these parameters. Mousa & Hamad examined the execution time as a function of the encryption key length and the file size, which recognized as a complexity and security. Meanwhile, the study demonstrated a different data types and the role of the data type. The results have been analyzed and interpreted as mathematical equations showing the relationship between the examined data and hence can be used to predict any future performance of the algorithm under different conditions. The order of the polynomial to approximate the execution time was justified [16].

Additionally, Ray & Das, descirbed the Cellular Automata [5] as a computing model of complex System using simple rule. Ray & Das highlights the main issues in the space, which divided into number of cell and each cell can be one or several final state. Cells are affected by neighbors with the application of simple rule. Furthermore, the study deals with the Cellular Automata in cryptography for a class of Block Ciphers through a new block encryption algorithm based on programmable cellular automata. The proposed algorithm belongs to the class of symmetric key systems [17].

IV. PROPOSED MODEL

Sequentially, providing a secure and flexible cryptography mechanism raises the needs for analyzing and comparing different encryption algorithms for the aim of enhancing the security during the encryption process. Hence, this paper suggested a cryptography mechanism in the block cipher by managing the keys sequentially, which classified into encryption-secret-key, description-secret-key, and shared-secret-key. These keys will works dependently for extracting and generating the content relation to be managed later by the key management that helps to communicate and share sensitive information. In particular, the importance of thorough, consistent key management processes among public safety agencies with interoperable functions cannot be overstated. This model aims to secure dissemination, loading, saving, and eliminating faults of keys to make encryption implementations effective. There are inherent possibilities if suitable key management processes are not accompanied because of the intricacy of dispensing keys to all block in a certain fashion. This risk can be meaningfully appeased through sufficient key controls and proper education on encryption key management.

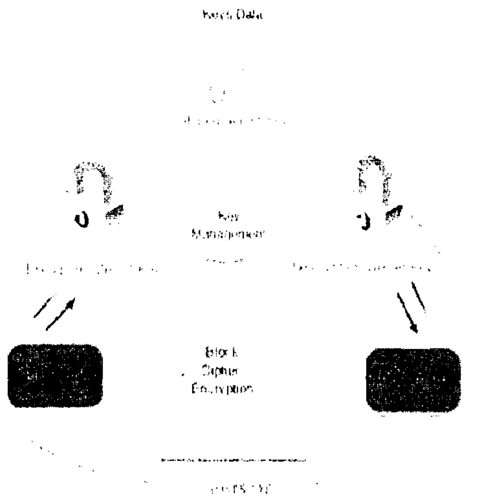

Figure 3: Cryptography Model over Block Cipher

V. Expected Benefits

The suggested cryptography model for block cipher will be expected to:

- Obtain a high security during the encryption and decryption process of the text contents;
- Simplify the management process of keys;
- Justify and eliminate faults and other relevant errors during the encryption process.

VI. Conclusion

Cryptography can be a technology that develops, but as long as security is made by man, cryptography is as good as the practice of people who uses it. This paper focused on the different security issues for providing a secure and effective cryptography technique over the block cipher. Most of these issues occurred when users leave keys unattended, keys that were chosen were easy to remember or maintain the same keys for years. This can be resolved by the suggested model, using the encrypting key that existed independently as an external tool by managing keys sequentially.

References

[1] W. Ehrsam, *et al.*, "A cryptographic key management scheme for implementing the Data Encryption Standard," *IBM Systems Journal,* vol. 17, pp. 106-125, 2010.

[2] J. Katz and Y. Lindell, *Introduction to modern cryptography*: Chapman & Hall/CRC, 2008.

[3] W. Stallings, *Cryptography and network security: principles and practice*: Prentice Hall, 2010.

[4] T. Fukunaga and J. Takahashi, "Practical fault attack on a cryptographic LSI with ISO/IEC 18033-3 block ciphers," 2010, pp. 84-92.

[5] J. Amigo, *et al.*, "Theory and practice of chaotic cryptography," *Physics Letters A,* vol. 366, pp. 211-216, 2007.

[6] X. Zhang and K. Parhi, "Implementation approaches for the advanced encryption standard algorithm," *Circuits and Systems Magazine, IEEE,* vol. 2, pp. 24-46, 2003.

[7] S. Heron, "Advanced Encryption Standard (AES)," *Network Security,* vol. 2009, pp. 8-12, 2009.

[8] A. Barenghi, *et al.*, "Low voltage fault attacks to AES and RSA on general purpose processors," *IACR eprint archive,* vol. 130, 2010.

[9] B. Jyrwa and R. Paily, "An area-throughput efficient FPGA implementation of the block cipher AES algorithm," 2010, pp. 328-332.

[10] N. Potlapally, *et al.*, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," *IEEE Transactions on Mobile Computing,* pp. 128-143, 2006.

[11] K. Chan and F. Fekri, "A block cipher cryptosystem using wavelet transforms over finite fields," *Signal Processing, IEEE Transactions on,* vol. 52, pp. 2975-2991, 2004.

[12] S. Lian, *et al.*, "A block cipher based on a suitable use of the chaotic standard map," *Chaos, Solitons & Fractals,* vol. 26, pp. 117-129, 2005.

[13] A. Biryukov and A. Shamir, "Cryptanalytic time/memory/data tradeoffs for stream ciphers," *Advances in Cryptology—ASIACRYPT 2000,* pp. 1-13, 2000.

[14] T. Xiang, *et al.*, "A novel block cryptosystem based on iterating a chaotic map," *Physics Letters A,* vol. 349, pp. 109-115, 2006.

[15] K. Gupta and P. Sarkar, "Construction of perfect nonlinear and maximally nonlinear multi-output Boolean functions satisfying higher order strict avalanche criteria," *Progress in Cryptology-INDOCRYPT 2003,* pp. 85-87, 2003.

[16] A. Mousa and A. Hamad, "Evaluation of the RC4 Algorithm for Data Encryption," *Proc. Of*

International Journal Computer Science & Applications, vol. 3, 2006.

[17] A. Ray and D. Das, "Encryption Algorithm for Block Ciphers Based on Programmable Cellular Automata," *Information Processing and Management*, pp. 269-275, 2010.