International Journal of Information Technology and Management

Vol. VI, Issue No. I, February-2014, ISSN 2249-4510

SECURE AND EFFECTIVE CRYPTOGRAPHY TECHNIQUE OVER THE BLOCK CIPHER

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. VI, Issue No. I, February-2014, ISSN 2249-4510

Secure and Effective Cryptography Technique over the Block Cipher

Mounika Adavelli[1], Afreen Sultana[2], Vinitha Bhodhe[3], Chandu Naik Azmera[4]

[1]Student, Department of Computer Science and Engineering, Varadha Reddy College of Engineering, Warangal, India

[2]Student, Department of Computer Science and Engineering, Varadha Reddy College of Engineering, Warangal, India

[3]Student, Department of Computer Science and Engineering, Varadha Reddy College of Engineering, Warangal, India

[4]Assistant Professor, Department of Computer Science and Engineering, Varadha Reddy College of Engineering, Warangal, India

Abstract – The convolution of cryptography does not allow many people to actually understand the determination and therefore available for practicing security cryptography. Cryptography process attempts to distribute an estimation of basic cryptographic primitives across a number of confluxes in order to reduce security assumptions on individual nodes, which establish a level of fault-tolerance opposing to the node alteration. In a successively networked and distributed communications environment, there are more and more useful scenarios where the ability to distribute a computation between a number of dissimilar network intersections is needed. The reason back to the efficiency is the separation of nodes that perform distinct tasks, fault-tolerance is achieved if some nodes are unavailable then others can perform the task and the trust required to perform the task is shared between nodes to obtain security, that order differently. Hence, this paper aims to describe and analyze the different research that has done toward text encryption and description in the block cipher. Moreover, this paper demonstrates a cryptography model in the block cipher.

----------♦----------

I. INTRODUCTION

Cryptographic algorithms are mathematical functions that are used in the encryption and decryption process. A cryptographic algorithms works in combination with a ***key*** (a number, word or phrase), to encrypt the plain text. Same plain text encrypts to different cipher texts for different keys. Strength of a cryptosystems depends on the strength of the key. The real secret is that the key and its length are very important. 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 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. 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. Encryption methods have historically been divided into two types. They are substitution ciphers and transposition ciphers. A substitution cipher is a method of encryption by which units of plaintext are replaced with cipher text according to a regular system; the "units" may be single letters, pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution. A transposition cipher, the units of the plaintext is rearranged in a different and usually quite complex order, but the units themselves are left unchanged. By contrast, in a substitution cipher, the units of the plaintext are retained in the same sequence in the cipher text, but the units themselves are altered. An example of encryption algorithms is AES which is a symmetric algorithm. This means AES uses two keys, one for encryption and other for decryption. Security of an algorithm based on symmetric key, which must be remains secret. The AES uses block length of 128 bits and key length can be 128,192 or 256 bits. Most commonly implemented key length is 128 bit. For a key length of 128 bits there are 3.4*10^38 possible combinations.

The input to encryption and decryption algorithms is a single 128 bit block. This block is represented as a

square matrix of bytes. This block is copied into state array, which is modified at each stage of encryption or decryption. After the final state, state is copied to an output matrix. Similarly, the 128 bit key is represented as a square matrix of bytes. This key is then expanded into an array of key schedule words: each word is four bytes and total key schedule is 44 words for the 128 bit key. The key that is provided as input is expanded into an array of forty-four thirty-two bit words. Four different words serve as a round key for each round.

Four different keys are used, one for permutation and remaining for substitution:

- Substitute bytes: Uses a table, referred to as S-box, to perform byte by byte substitution of the block.

- Shift rows: A simple permutation that is performed row by row.

- Mix columns: The substitution that alters each byte in column as a function of all of the bytes in column.

- Add round key: A simple bitwise XOR of the current block with a portion of expanded key.

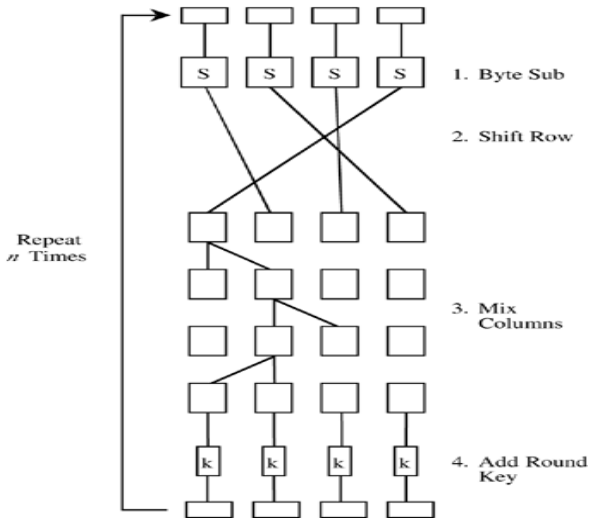

Figure.1

The structure is simple. For both encryption and decryption, the cipher begins with Add round key stage, followed by nine rounds that each includes all four stages, followed by tenth round of three stages. Only Add round key stage makes use of key. So, the cipher begins and ends with an Add round key stage.

Add round key stage by itself would not be formidable. The other three stages together scramble the bits, but by themselves, they would provide no security because they do not use the key. We can view the cipher as alternating operations of XOR encryption of a block, followed by scrambling of the block, followed by XOR encryption, and so on. This is both efficient and secure.

Each stage is easily reversible. For the substitute byte, shift row and mix columns stages, an inverse function are used in decryption algorithm. For Add round key stage, the inverse function is achieved by XORing the same round key to the block.

Decryption algorithm makes use of the expanded key in reverse order. However decryption algorithm is not identical to the encryption algorithm. This is the consequence of the particular structure of AES.

The final round of both encryption and decryption consists of only three stages.

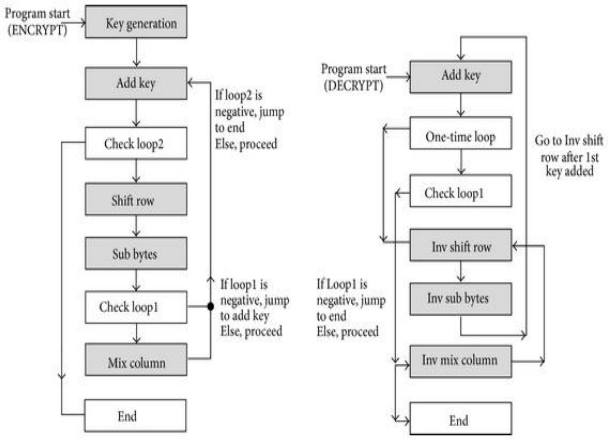

Figure 2. Encryption and decryption process

A cryptographic system has five components;

1. A plaintext message space, P

2. A cipher text message space, C

3. A key space, K

4. A family of enciphering transformations E[K]:P[C]

5. A family of deciphering transformations D[K]:C[P]

A block cipher cryptosystem consists of two algorithms, the encryption algorithm and decryption algorithm. The input for encryption algorithm is n-bit plaintext P and a k-bit key K and outputs an n-bit cipher text C; the input for decryption algorithm is n-bit cipher text C and a k-bit key K and outputs an n-bit plaintext. 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=E[K,P] (1.1)

P=D[K,C] (1.2)

Mounika Adavelli[1], Afreen Sultana[2], Vinitha Bhodhe[3], Chandu Naik Azmera[4]

The block cipher breaks P into successive blocks P1, P2, and enciphers each P1 with the same key K; that is as in equation (1.3).

E[K,P]=E[K,P1] E[K,P2] (1.3)

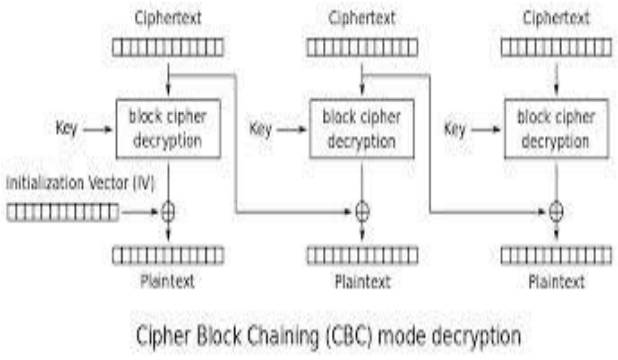

figure.3

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.

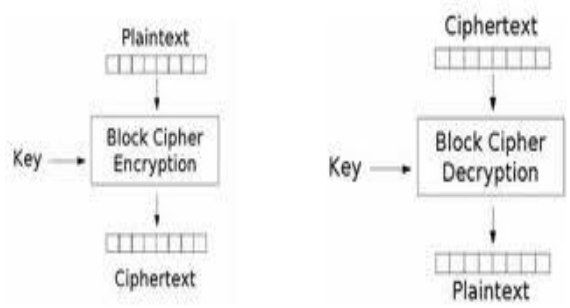

Figure 4: The encryption and decryption operations in block cipher algorithm

There are some properties which determine strength or weakness of the block algorithms.

- 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 E [K, P] = C THEN E [K' [P']] = C'

P', C', and K' are the bit-wise complements of P, C and K. 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 input bits are changed. Conditions can be easily imposed on the Boolean function to satisfy particular avalanche criteria but the difficult task is constructing them. SAC guarantees that exactly half of the output bits change when one input bit is changed.

II. EXISTING ISSUES

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

Encryption keys are a sequence of symbols used with a cryptographic algorithm, which enables encryption and decryption. It is crucial that an efficient key management program be established and benefited throughout public safety agencies. Key management ensures that censorious 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 converting plain text into unintelligible form (cipher text) by using a cryptographic system.

The cryptosystem is hardware and software providing the means to encrypt and decrypt conversions. Figure 2 presents a basic encryption and decryption concept.

The basic meteorological of encryption comprise the algorithm, the key, and the key management. The key is easily identified 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 decryption process that must be predicted so that a corresponding decryption algorithm can retract 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:

- Complications in addressing the security issues related to encryption key management;

- Dearth in providing a suitable details about the different threats in terms of decision makers on the importance of key management;

- Complications in generating the suitable recommendations for constructing proper key management.

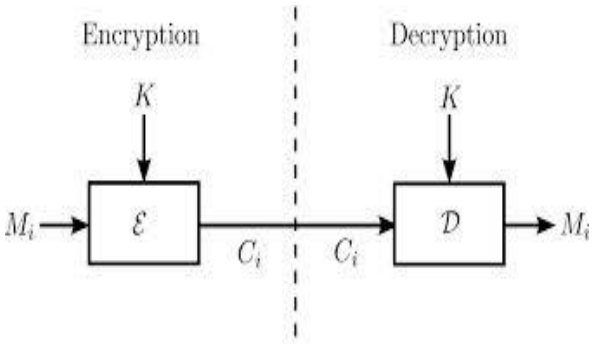

Figure 5: Basic Encryption Concept

III. RELATED WORK

Chan & Fekri developed a new private key cryptosystem based on the limited period wavelet. The encryption and decryption are performed by the combination of part and a detail examination of banks of the nonlinear limited period wavelet transform whose a device coefficients are determined by the keys of the users. Authors describe the combination of a number of keys in description 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 contrast with DES and AES. The results indicated that the wavelet cryptosystem has similar, calculate, complex to AES and approximately half the complexity of DES. The security is bind 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 a tire out key search.

Another study by Mousa & Hamad investigates the analysis process of the effect of distinct parameters of the RC4 encryption algorithm that was performed to describe the performance of RC4 algorithm based on changing some of these parameters. Mousa & Hamad inspected the execution time of 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 state that an event occurs in any future presentation of the algorithm under different conditions.

The order of the polynomial to approximate the execution time was justified. Additionally, Ray & Das, described the Cellular Automata as a calculating model of complex System using simple rule. Ray & Das highlights the main issues in the space, which categorized into number of cell and each cell can be one or several final state. Cells are altered by sides by cells 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.

IV. EXPECTED BENEFITS

The proposed cryptography model for block cipher will be anticipated to:

- Acquire a high security during the encryption and decryption process of the text contents;

- Simplify the management process of keys;

- Justify and remove faults and other relevant errors during the encryption process.

V. 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 concentrated on the several security issues for providing a secure and effective cryptography technique over the block cipher. Most of these issues occurred when users leave keys unsecured, keys that were chosen were easy to remember or maintain the same keys for years. This can be resolved by the proposed model, using the encrypting key that existed independently as an external tool by managing keys sequentially.

VI. 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* 418 *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.