ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Competitive Study of Cryptography Techniques over Block Cipher

Dr.S.Makbul Hussain
Associate Professor of Mathematics,
Osmania College (Autonomous), Kurnool.

M.Zahir Ahmed
Associate Professor of Physics,
Osmania College (Autonomous), Kurnool.

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.

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. 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 categories: substitution ciphers and transposition ciphers. Stallings had explained each of these ciphers as essential information for understanding modern cryptography. 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. Security an algorithm based on symmetric key, which must be remains secret. The AES block cipher as acting in plaintext in groups of each bit time which are called blocks. 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.

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. Each State is expressed as a rectangular table of data bytes. The table blow has 4 rows, while the number of batteries (NB) is the size of the block processing divided by 32.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Similarly, the encryption key (cipher key) expressed as rectangular table with data bytes. The table has 4 rows and number of columns is the key length divided by 32. Each table element is one byte.

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 asa 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.

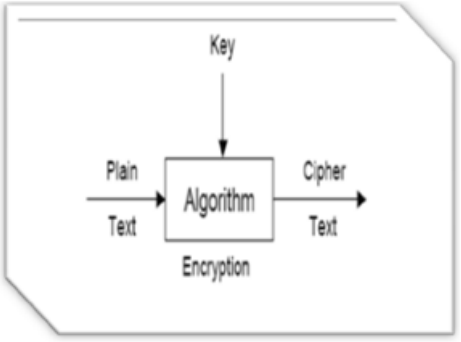

Figure: Basic Encryption Concept

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

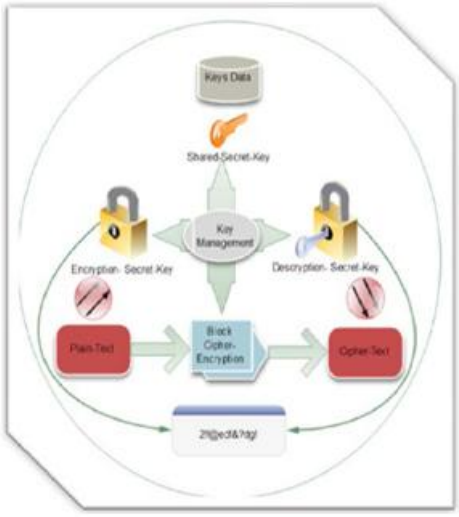

Figure: Cryptography Model over Block Cipher

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.