A COMPETITIVE ANALYSIS OF CRYPTOGRAPHY TECHNIQUES OVER BLOCK CIPHER

Abid Hussain* Murtuza Ahmed Khan
LIET, Hyderabad, India,

ARTICLE INFO

Corresponding Author:
Abid Hussain,
LIET, Hyderabad, India,
abid.pg12@gmail.com

Keywords:
Cryptography, Text Encryption, Block Cipher, AES

ABSTRACT

The complication of cryptography does not allow many people to actually understand the motivations of working security cryptography. Cryptography process seeks to distribute an estimation of basic cryptographic primitives across a number of unions in order to reduce security assumptions on individual nodes, which establish a level of fault-tolerance contrasting to the node modification. In an increasingly networked and distributed communications setting, there are more and more useful situations where the ability to distribute a computation between a number of dissimilar network intersections is needed. The reason back to the efficiency, fault-tolerance and security that order differently. Hence, this work aims to describe and review the different research that has done toward text encryption and description in the block cipher. Moreover, the proposed method suggests a cryptography model in the block cipher.

2012, AJCSIT, All Right Reserved.

INTRODUCTION

Unspecified scenery of the algorithm cannot be stressed enough. However, by publishing the algorithm, it gives the cryptographer options to be seen by a wide range of studious 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 that the cryptanalyst has to do. The work factor has to break the system for the comprehensive search in the digit space is exponential in relation to the key length [1]. The secret comes from having a strong algorithm 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. Each of these ciphers as essential information for understanding modern cryptography [3]. An example of encryption algorithm is Advanced Encryption Standard (AES) 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 kept secret [5]. The AES block cipher as performing in plaintext in groups of each bit time which are called blocks [6]. Typical size of a block is 64 bits. Each round conversion consists of three separate conversions called layers:

- Linear mixed layer;
- Non-linear layer;
- Additional Key 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]. However, AES is an iterative algorithm with variable size block processing and key which can be 128, 192 or 256 bits. The temporary results of the algorithm after each conversion called State [8]. Each State is expressed as rectangular table of data bytes [9] as shown in Table 1. The table below has 4rows, while the number of batteries (NB) is the size of the block processing divided by 32. Similarly, the encryption 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.

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

![Table1: State (with Nb = 6) and encryption key (with Nk=4)](image)

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
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. For any fixed key, the decryption algorithm acts as the inverse process of the encryption algorithm as in following equation 3, 4.

\[ C = E_k(M) \]  
\[ M = D_k(C) = E_k^{-1}(E_k(M)) \]

The block cipher breaks M into successive blocks M1, M2, and enciphers each M1 with the same key K; that is as shown in equation (5).

\[ E_k(M) = E_k(M1) E_k(M2) \]

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

![Figure 1: The encryption and decryption operations in block cipher algorithm](image)

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. The difficulty 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 \( E_k'(P') = C' \), and \( K' \) are the bit-wise complements of P, C and K. There are no simple relations in a high-quality block cipher. The weaknesses in the block cipher are created by this property. An example that has this property is the DES algorithm. 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. The Strict Avalanche Criteria (SAC) guarantees that exactly half of the output bits change when one input bit is changed.

### 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](image)
A new private key of 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. 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. It 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. 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.

III. 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 is shown in Figure 3.

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 work focuses 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