Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol.3, No.8, 2013

Design of a New Block Cipher Algorithm

Obaida Mohammad Awad Al-Hazaimeh
Department of Information Technology
AL-BALQA Applied University/ AL-Huson College, PO box 50, Al-Huson, Irbid – Jordan
dr_obaidam@yahoo.com

Abstract
The new attack methods show some lacuna in the encryption algorithms and key schedule. As the strength of an encryption algorithm depends on the difficulty of cracking the original message, a number of symmetric key encryption algorithms like DES, TRIPLE DES, AES, BLOWFISH, and RC6 have been developed to provide greater security affects. Most of them are most popular in achieving data security at a great extent like AES. But, as security level is increased, the time and complexity of algorithm is also increased. This is the major cause of decreasing speed and efficiency of the encryption system. This paper presents a new algorithm for block data encryption that enhances the security level. The proposed algorithm is executed with block wise parallel encryption model to decrease the delay time.
Keywords: Plain-text, encryption, block cipher, decryption, parallel encryption model

1. Introduction

Cryptography has had an interesting history and has undergone many changes through the centuries because it plays a major role in keeping a message safe when data is in transit across the network channels [1]. It provides a way to store sensitive information or transmit it across insecure networks i.e. the Internet. Cryptography converts the original message in to a non-readable format using the encryption process and sends the message over an insecure channel. The authorized person has the capability to convert the non-readable message to a readable one using decryption process [2]. The original message the person wishes to share with the other is defined as Plain-Text. The message that cannot be understood by anyone or a meaningless message is defined as Cipher-Text.
Encryption is the process of converting plain-text into cipher text with a key. A key is a numeric or alpha numeric text or may be a special symbol [1] [2]. A decryption is a reverse process of encryption in which an original message is retrieved from the cipher text. Encryption takes place at the sender end and decryption at the receiver end [2]. The input to the encryption process is plain text and the cipher text is the input to the decryption process. First the plaintext is passed through the encryption algorithm which encrypts the plaintext using a key and then the produced cipher text is transmitted. Figure 1 shows the process.

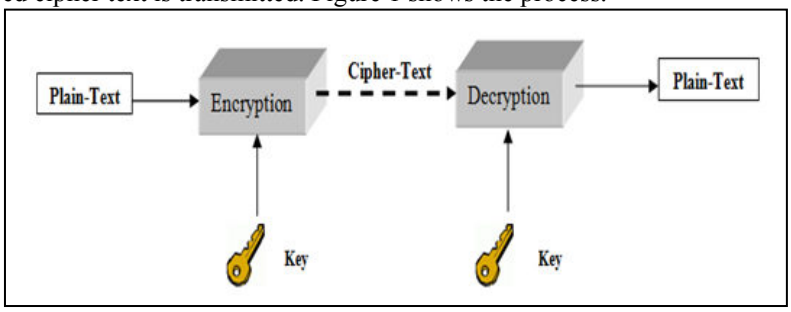

Figure1. Encryption/Decryption process

At the receiver side, a decryption process takes a place. The input cipher text is passed through the decryption algorithm which decrypts the cipher text using the same key as that of the encryption. Finally we get the original plain-text message.

2. Related work

During the past four decades, a large number of cryptographic algorithms have been proposed and implemented to provide security over the communication channels (i.e. internet). But nowadays more and more attention has been paid to attacking these algorithms by cryptanalysts techniques [3] [4].
Data Encryption Standard (DES) was the first encryption standard to be recommended by NIST. It was developed by an IBM team around 1974 and adopted as a national standard in 1997. The DES features are described in [3].
AES was developed by two scientists, Joan and Vincent Rijmen, in 2000. AES uses the Rijndael block cipher, as presented in [4]. In 1993, Bruce Schneier designed blowfish algorithm. It is considered a fast, and free alternative to existing encryption algorithms security. Its properties are described in [3].
Although a lot of work has been done on cryptographic field, many realistic problems still need to be solved, and

as far as we know, there is no algorithm that is completely secure against all attacks [5].

3. Types of Cryptography

Cryptography algorithms can be classified into two categories. Symmetric key cryptography and Asymmetric key cryptography. Both of these categories are summarized as follows:

3.1 Symmetric Key Cryptography

In symmetric cryptography, the key used for encryption is similar to the key used in decryption. Thus the key distribution has to be made prior to the transmission of information. The key plays a very important role in symmetric cryptography since the security directly depends on the nature of the key i.e. the key length etc. There are various symmetric key algorithms such as DES, TRIPLE DES, AES, RC4, RC6, and BLOWFISH [6].

3.2 Asymmetric Key Cryptography

In asymmetric cryptography, two different keys are used for encryption and decryption—public and private. The public key is announced for all on the network. Anyone who wants to encrypt the plaintext should know the public key of receiver. Only an authorized person can decrypt the cipher text through his own private key. Symmetric encryption algorithm runs faster than asymmetric key algorithms. Also the memory requirement of the symmetric algorithm is lesser than the asymmetric one [7] [9]. Therefore, the proposed algorithm is a symmetric key block cipher.

4. Methodology

Available data within a network environment is generally regarded a valuable asset. In such case, it is believed that such data should be handled in a secured manner in terms of storage and transmission to avoid undue access by unauthorized persons, as mentioned in the introduction. The proposed algorithm consists of some specifications. These specifications are summarized as follows:

- It is a Symmetric Key Cipher Algorithm;
- Each block size is 16 bytes;
- Key matrix values are randomly selected and ranged from 33 to 126;
- Each new block data has it is own unique key to strengthen the security level;
- ASCII code substitution concept is followed;
- Non-linear mixing is used to generate matrix of data block and key; and
- Linear mixing is used for confusion and diffusion concepts.

4.1 Encryption Algorithm

The cryptographic process usually involves encryption algorithms. These algorithms execute many iterations of substitutions and transformations on the original data (known as plaintext) in order to complicate the process of identifying the data by a hacker or intruder [1] [10]. The proposed encryption algorithm consists of the following processes:

- The letters of alphabet are assigned numerical values from 33 to 126 in sequence i.e. A, B, C, ..., X, Y, Z are assigned numerical values from 65, 66, 67, ..., 88, 89, 90, respectively, based on the ASCII code substation concepts.
- The plaintext is partitioned into fixed-length blocks of size 16 bytes (4*4) rows and columns. These blocks are represented by a matrix M_O.
- The values of key matrix (K_O) are randomly generated from the range 33 to 126. The size of key matrix is equivalent to the block size of plaintext 16 bytes (i.e. 4*4 matrix size).
- Calculate the transpose matrix of plain-text block matrix (M_O), which is denoted by M_{OT}.
- Convert the key matrix generated randomly to a binary key donated by K_B using the following formula: $K_B = K_O \bmod 2$.
- Add both of M_O with K_B and the result matrix is denoted by M_C.

$$M_C = M_O + K_B$$

- Capsulation process: Non-linear mixing between the M_C and K_O. In other words, insert the key inside the block cipher to generate 8*4 rows and columns matrix of data block and key.
- Linear mixing: using bits shuffling to create a diffusion effect, while substitution is used for confusion.
- Replace the numeric values after performing linear mixing by their corresponding characters based on ASCII code system to generate an encrypted block.

Diagrammatically, the steps are represented in Figure 2.

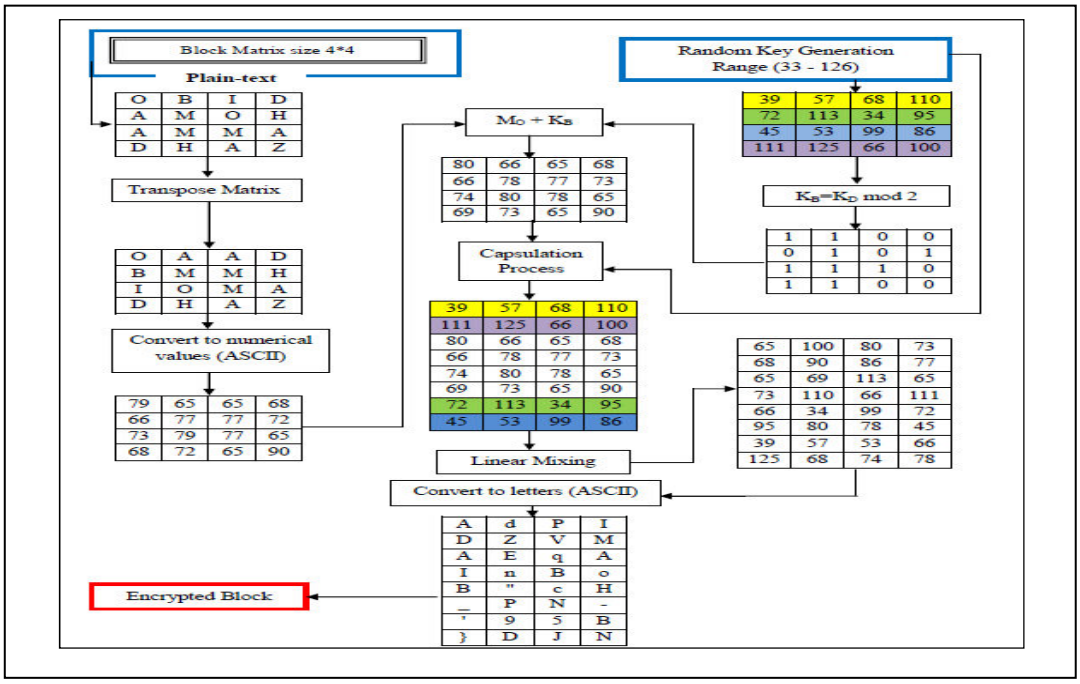

Figure 2. Proposed encryption architecture

4.2 Decryption Algorithm

Decryption is a process of reversing all that has happened in the encryption process. It involves converting the encrypted data back to its original form for the receiver to understand [8], as shown in Figure 3.

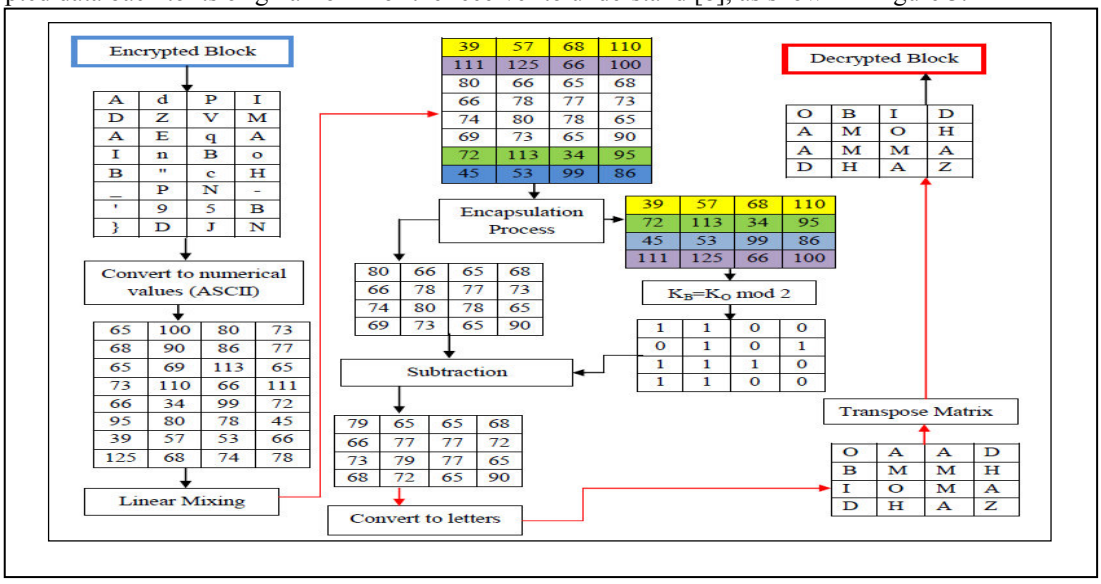

Figure 3. Proposed decryption architecture

The proposed decryption algorithm consists of the following processes:

- Capsulation process: involves extracting the key from the cipher-block data.
- Decryption process: involves calculating the binary key (K_B) then subtracting the operation between the encrypted data and the binary key. The end result of such operation is the plain text data (original text).

The accuracy of the decryption key cannot be negotiated. In short, the accuracy of the proposed algorithm is a function of the encapsulation process as to whether the key is correct or not where a correct key produces a correct result and vice versa.

5. Parallel Encryption and Decryption Model

There are two reasonable strategies for parallel encryption and decryption model. When a message shows up all at once, you might divide it roughly into equal parts and handle each part separately. Alternatively, you can take an interleaved approach, where alternating blocks are handled by different threads. That is, the actual message is

separated into two different plain-texts [1] [13].
The proposed algorithm is executed with block wise parallel encryption model as shown in Figure 4.

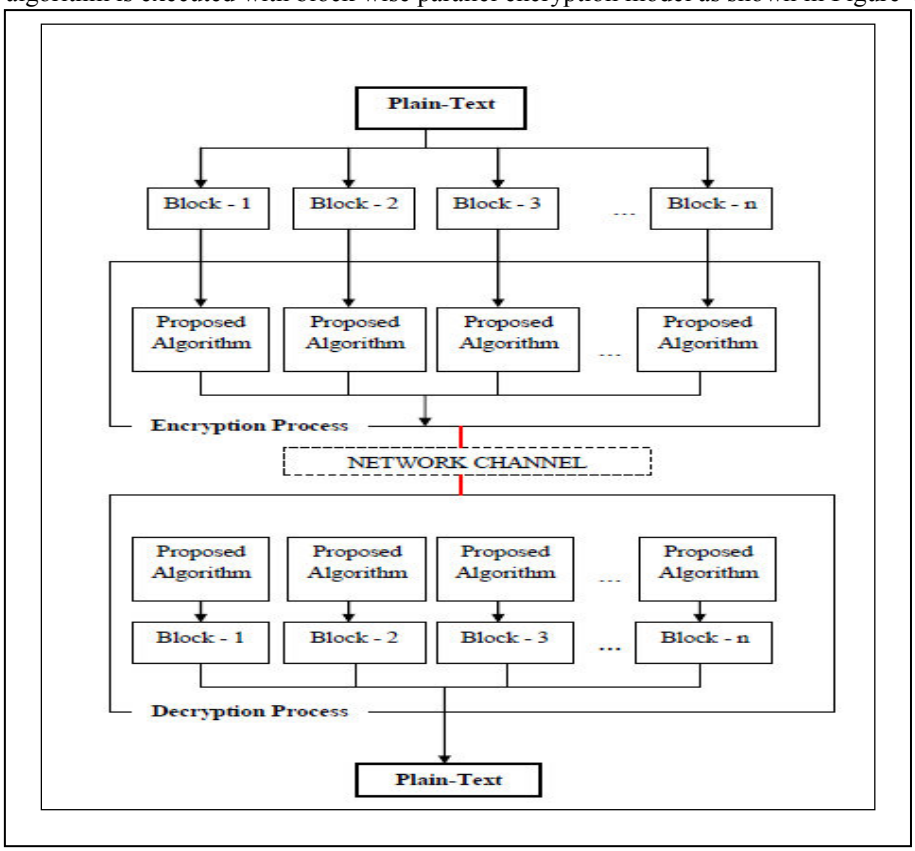

Figure 4. Parallel encryption and decryption Model

Plain-text data is divided into blocks i.e. 4 blocks passing into four threads of the proposed algorithm at a time. These threads are executed simultaneously by using multithreading technique. After encryption, these blocks are sent to a receiver where the blocks are passed into the reverse proposed algorithm in a parallel manner, and then the cipher text is decrypted into a plaintext and all the blocks of the plain-text collected together to get the original message. Since the algorithm is executed parallelly using multithreading technique, the execution speed and performance of the model increases.

6. Security Analysis

This paper aims to propose a new algorithm to improve block cipher performance by maintaining security on a plain-text. Security analysis of the proposed algorithm was conducted using correlation analysis [10].

5.1 Correlation analysis

The correlation between any kinds of data is known as intrinsic features. The existence of this feature can help attackers to trace the encrypted data. Therefore, correlation analysis is usually used to test the security and the correlation between the data. The formula for computing the correlation coefficient is given by the following equation [10]:

$$\Gamma = \frac{\sum (X - \bar{X}) \bullet (Y - \bar{Y})}{\sqrt{\sum (X - \bar{X})^2 \bullet \sum (Y - \bar{Y})^2}}$$

The strength of the relationship between the data after performing the capsulation process and the data after performing the linear mixing is determined by a correlation coefficient, which ranges from -1 to 1. The closer the coefficient is to +1or -1, the stronger is the relationship. This means that the data is related and has perfect correlation [10] [12]. In other words, if the correlation coefficient is equal to zero, then the data after performing the capsulation process and the data after performing the linear mixing are totally different (no association between the variables).

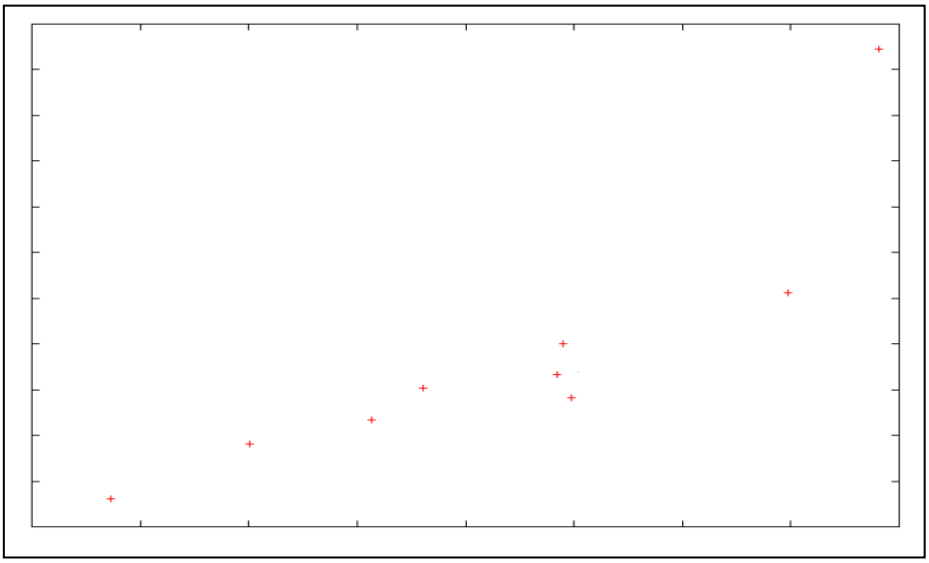

Figure 5. Correlation analysis after performed capsulation process

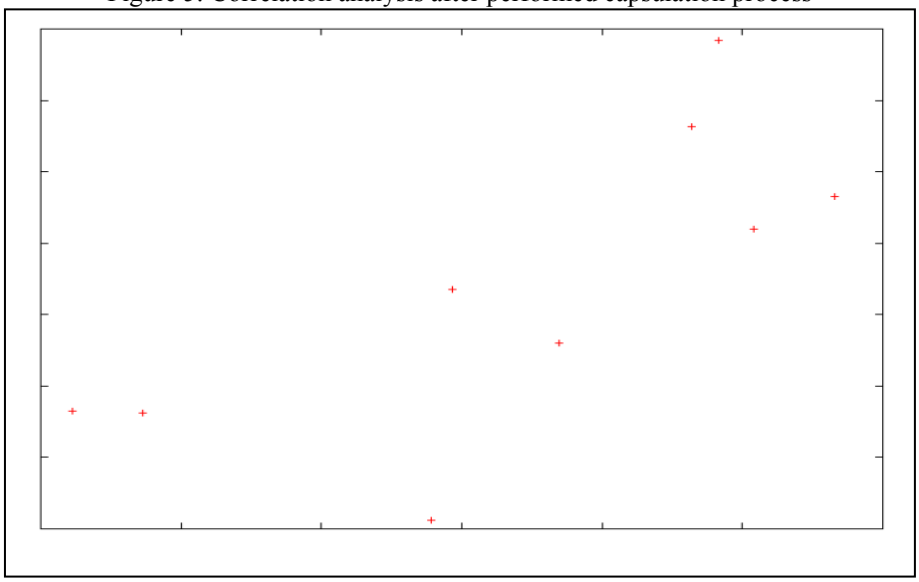

Figure 6. Correlation analysis after performed linear Mixing

It is clear from figures 5 and 6 that the proposed algorithm covered all the data characters and showed good performance because there is no feature that can help attackers to trace the encrypted data.

7. Conclusion

Design of a new block cipher algorithm is proposed in this paper, where multiple algorithms are used in a parallel manner to enhance the speed of the proposed algorithm. Based on security analysis, it can be concluded that the proposed algorithm is secure because it has satisfied correlation coefficient test. Thus, the proposed algorithm will be efficiently used or considered as a good alternative as compared to other existing algorithms.

8. Acknowledgement

Building the system for the proposed algorithm work lasted for one month, during which time I received a lot of help from my colleagues. The author would like to thank all the people who have supported this work.

References

[1] William Stallings, *Cryptography and Network Security: Principles and Practice*, (5th ed). Prentice Hall, Upper Saddle River, NJ, USA. January, (2010)
[2] P. Zimmerman, *An Introduction to Cryptography, Doubleday & Company*, Inc., United State of America, USA, (1999)
[3] A.Monika, P. Mishra, A Modified Approach for Symmetric Key Cryptography Based on Blowfish

Algorithm, *International Journal of Engineering and Advanced Technology*, vol.1,(2012)
[4] S. Karthikeyan, N. Sairam, G. Manikandan, A New Approach for Enhancing Data Security Using Parallel Processing, *Advances in Natural and Applied Sciences*, vol.6, (2012)
[5] W. David, Principles for Building Secure Systems, *Paxson Spring*, (2013)
[6] J. Kelsey, B. Schneier and D. Wagner, Key-schedule cryptanalysis of IDEA, GDES, GOST, SAFER, and Triple-DES, Advances in Cryptology, Proceedings Crypto '96,LNCS 1109, N. Koblitz, Ed., Springer-Verlag, 237-252, (1996)
[7] J. Daemen, L.R. Knudsen and V. Rijmen, The Block Cipher Square, Fast Software Encryption - FSE'97,Springer Verlag, Haifa, Israel, 149-165, January (1997)
[8] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag New York Inc., (1987)
[9] J. Hoffstein, J. Pipher, J. H. Silverman , NTRU: A new high speed public key cryptography system in Algorithmic number theory (ANTS III), Portland , June 1998, Lecture Notes in Computer Science 1423 (J. P. Buhler, ed.) *Springer-Verlag*, Berlin, 267-288, (1998)
[10]C. Shannon, Communication Theory of Secrecy Systems, *Bell Systems Technical Journal, MD Computing*, vol. 15, 57-64, (1998)
[11]S. Chang, the Design of A Secure and Pervasive Multimodal Web System, in the Proceedings of the 17th *International Conference on Advanced Information Networking and Applications (AINA'05)*, vol. 2, 683 – 688, Taiwan, (2005)
[12]J. Cheng Yen , J. Guo, A new image encryption algorithm and its VLSI architecture, in Proc. *IEEE Work-shop Signal Processing Systems*, pp. 430–437, (1999)
[13]B. Sunita, B. Anita, S. Sharma, A new Approach towards Encryption Schemes: Byte-Rotation Encryption Algorithm, *Proceeding of the world Congress on Engineering and Conputer Science*, vol. 2, USA, (2012)