International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, March 2013

A NEW APPROACH FOR COMPLEX ENCRYPTING AND DECRYPTING DATA

Obaida Mohammad Awad Al-Hazaimeh

Department of Information Technology, Al-balqa Applied University,
AL-Huson University College, Irbid, Jordan.
dr_obaidam@yahoo.com

ABSTRACT

During the last decades, information security has become a major issue. Encrypting and decrypting data have recently been widely investigated and developed because there is a demand for a stronger encryption and decryption which is very hard to crack. Cryptography plays major roles to fulfilment these demands. Nowadays, many of researchers have proposed many of encryption and decryption algorithms such as AES, DES, RSA, and others. But most of the proposed algorithms encountered some problems such as lack of robustness and significant amount of time added to packet delay to maintain the security on the communication channel between the terminals. In this paper, the security goals were enhanced via "A New Approach for Complex Encrypting and Decrypting Data" which maintains the security on the communication channels by making it difficult for attacker to predicate a pattern as well as speed of the encryption / decryption scheme.

KEYWORDS

Encryption, Decryption, QoS, RC6, PKI,

1. INTRODUCTION

In network security, cryptography has a long history by provides a way to store sensitive information or transmit it across insecure networks (i.e. the Internet) so that it cannot be read by anyone except the intended recipient, where the cryptosystem is a set of algorithms combined with keys to convert the original message (Plain-text) to encrypted message (Cipher-text) and convert it back in the intended recipient side to the original message (Plain-text) [1]. The first model proposed by Shannon on the cryptosystem is shown in figure 1 [2].

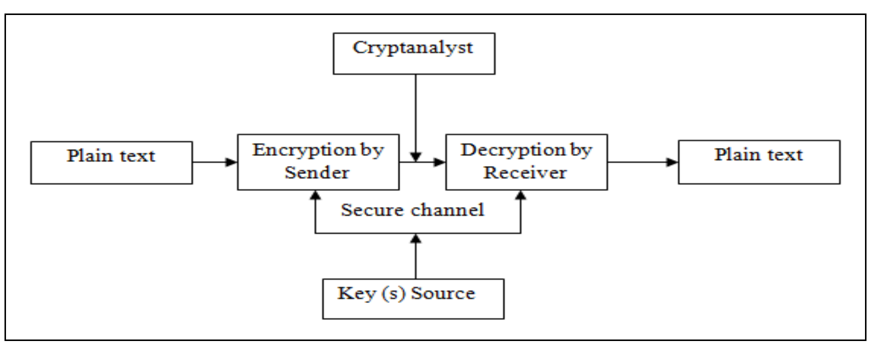

Figure 1. Shannon model of secret communication

In computer systems, the algorithm consist of complex mathematical formulas that dictate the rules of conversion process from plain text to cipher text and vice versa combined with the key. However, some of encryption and decryption algorithms use the same key (i.e. sender, and receiver). And in other encryption and decryption algorithms they use different keys but these keys must be related.

The major issue to design any encryption and decryption algorithm is to improve the security level. Therefore, this paper aims to propose a new algorithm to improve the security level and increase the performance by minimizing a significant amount of delay time to maintain the security and makes comparative study [4]. This paper is structured as follows: comparison between the most popular encryption algorithms, Advanced Encryption Standard (AES), Public Key Infrastructure (PKI), proposed technique, performance analysis, security analysis, and conclusion

1.1. Comparisons of Most Popular Encryption Algorithms

There is quite a number of encryption algorithms used for keeping information secured. Their complexity and ability to resist attack varies from one algorithm to another. The main component of encryption process is the algorithms that serve basic purpose in different ways. Popularly used algorithms include DES, TripleDES, RC2, RC4, Blowfish, Twofish and Rijndael (AES) as we mentioned in the abstract. The basic information of the most popular ciphers is shown in table 1 [5].

Table 1. Comparison of popular encryption algorithms

Algorithm	Key size	Block size	Rounds	Status
DES	56- Bits	64-Bits	16	Cracked
RC2	128- Bits	64- Bits	16 mix 2 mashing	Cracked
RC4	Variable	Variable	Unknown	Cracked
Blowfish	128- Bits	64-Bits	16	Not Cracked Yet
Towfish	(128, 192, 256)-Bits	128- Bits	16	Not Cracked Yet
3-DES	(112, 168)- Bits	64-Bits	48	Not Cracked Yet
AES(Rijndael)	(128, 192, 256)-Bits	128- Bits	10, 12, or 14	Not Cracked Yet

1.2. Advanced Encryption Standard (AES)

Based on the table 1, the National Institute of Standards and Technology (NIST) in 1997, announced officially that Rijndael algorithm would become the Advanced Encryption Standard (AES) to replace the aging Data Encryption Standard (DES). AES algorithm is a block cipher text the block size can be 128, 192 or 256 bits. 128(AES -128), 192(AES -192) and 256 (AES -256) bits key lengths [5- 7].

The Rijndael algorithm is based on round function, and different combinations of the algorithm are structured by repeating these round function different times. Each round function contains uniform and parallel four steps, byte substitution, row shifting, column mixing 147 and key addition, the data is passed through Nr rounds (10, 12, and 14), and each step has its own particular functionality as shown in figure 2 [7].

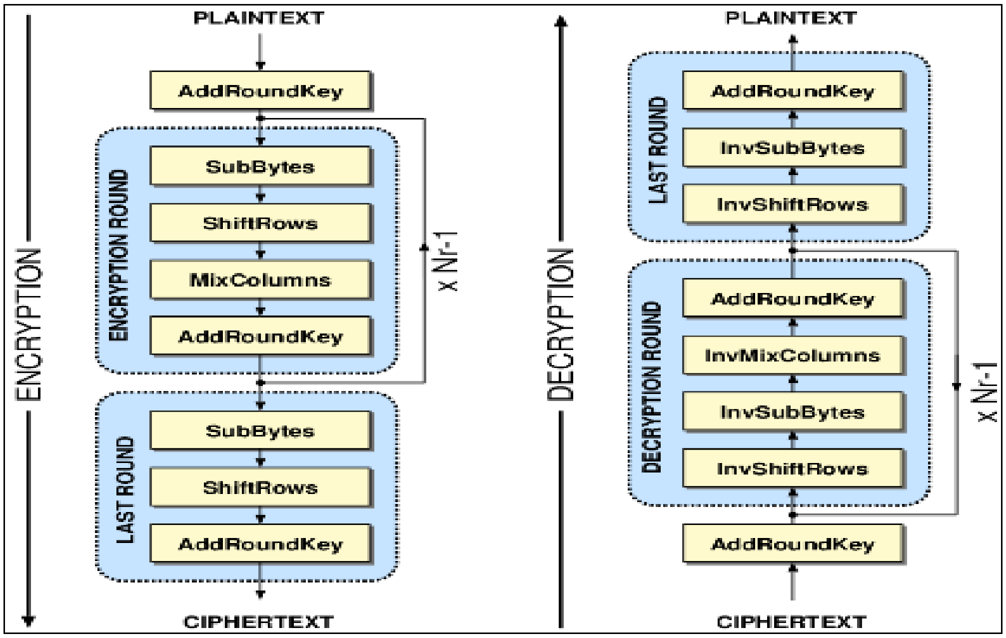

Figure 2: Advanced encryption standard structure

1.3. Public Key Infrastructure (PKI)

PKI provides series of security services such as, authentication, confidentiality, non-repudiation, and integrity to the messages being exchanged [8- 10]. In this paper, PKI use in connection establishment phase to exchange the security value between the network terminals i.e sender, and receiver.

2. PROPOSED TECHNIQUE

The proposed algorithm is an attempt to present a new approach for complex encrypting and decrypting data based on parallel programming in such a way that the new approach can make use of multiple-core processor to achieve higher speed with higher level of security.

2.1. Encryption

In term of encryption process, the algorithm consists of combination of public key infrastructure for hybrid system and RC6 algorithm for confusion and diffusion operations as shown. The proposed encryption algorithm consists of the following processes as shown in figure 3.

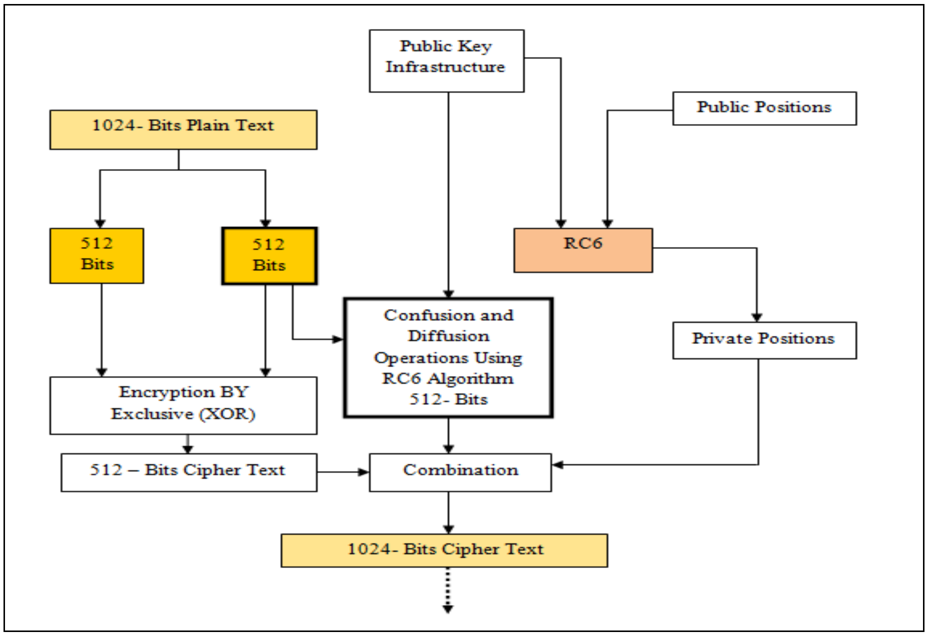

Figure 3. Proposed encryption structure

Public position is Hexadecimal numbers arranged in 8*8 matrix announced to all. In this step RC6 algorithm play major roles to generate a private position based to the secrete value from public key infrastructure. Plain-text 1024- bits size divided to 2 blocks. One of these blocks used as key after performed confusion and diffusion operations using RC6 algorithm. The last step is Insert the key inside the Cipher data based on the private position. RC6 is further described by a pseudo-code as shown in figure 4.

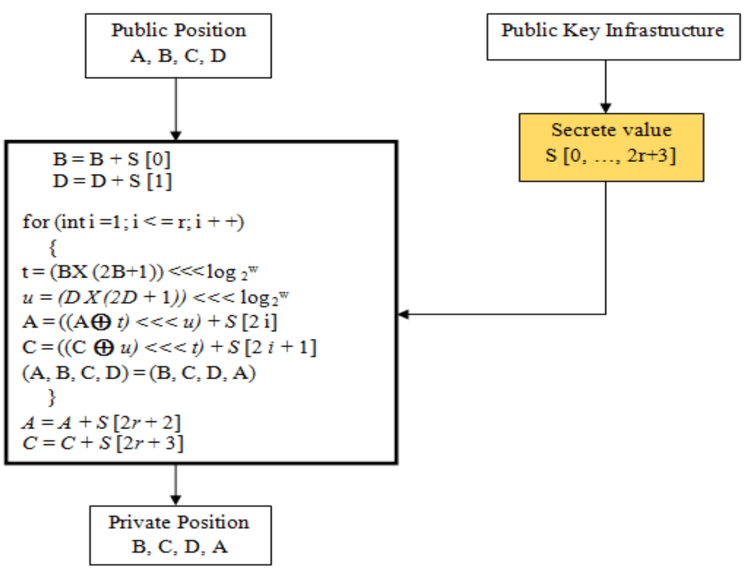

Figure 4. RC6 algorithm structure

2.2. Decryption

The decryption process involves converting the encrypted data back to its original form for the receiver's understanding. The same process is performed at the beginning of the encryption and decryption process (connection established) as described in the encryption part at the sender side to generate the same private position at the receiver side to eliminate the key from the cipher text. . The proposed decryption algorithm consists of the following processes as shown in figure 5.

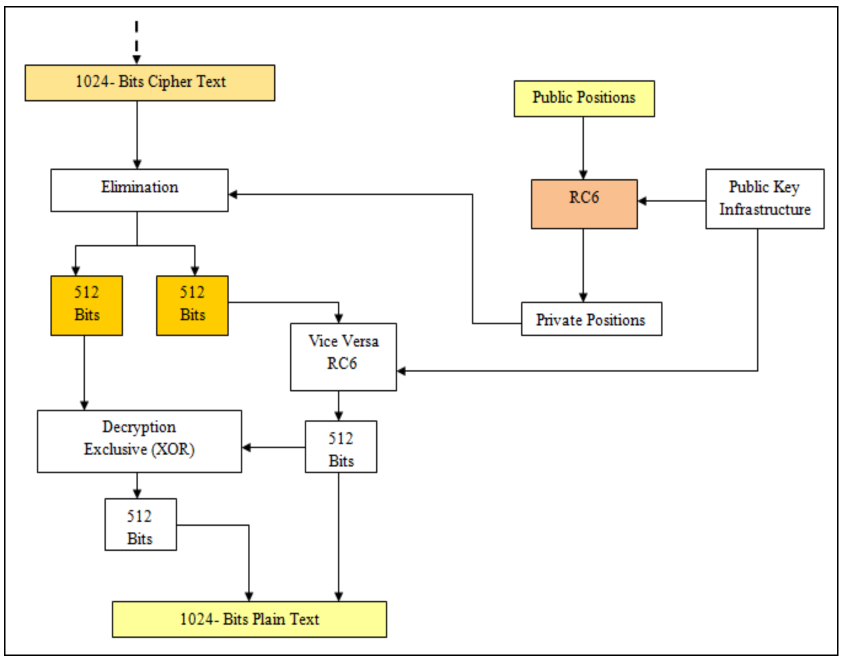

Figure 5. Proposed decryption structure

3. PERFORMANCE ANALYSIS

In order to test the performance analysis for any encryption and decryption algorithms, the speed play a major roles [4, 11-12]. In this paper, the proposed algorithm compared with Rijndael algorithm in term of the speed in both encryption and decryption process because the National Institute of Standards and Technology (NIST) announced officially that Rijndael algorithm become the Advanced Encryption Standard (AES) as we mentioned in the previous section. Both algorithms are implemented in the same environment and same conditions using *C* language.

3.1. Speed analysis for encryption and decryption

The speed of the algorithm can be characterized by measuring the time required for encryption and decryption. This parameter is measured for both the algorithms: Proposed algorithm and AES as shown in table 2, and 3.

Table 2. Speed for Encryption in different key lengths

Algorithm	**Key Length**			
	128 - Bits	192 - Bits	256 - Bits	512- Bits
Proposed Technique	0.1814575	0.2014440	0.2377533	0.2972729
AES	0.5500000	0.6043321	0.7132599	0.8918188

Table 3. Speed for Decryption in different key lengths

Algorithm	**Key Length**			
	128 - Bits	192 - Bits	256 - Bits	512- Bits
Proposed Technique	0.2701433	0.2968131	0.2978936	0.3187594
AES	0.5402866	0.5936262	0.5957872	0.6375188

The following column charts showing the relationship between the key lengths and the encryption and decryption time in both cases in figure 6 and 7.

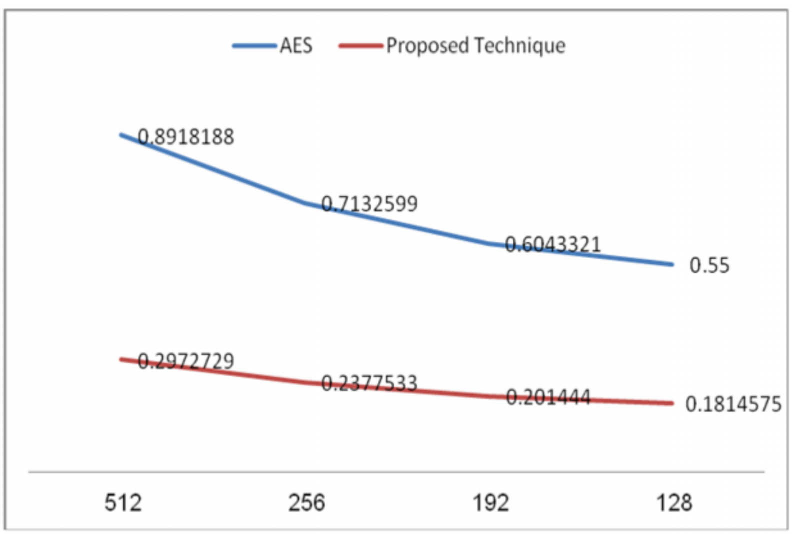

Figure 6. Column chart for Encryption process in both cases

The result in this paper shows that the average time required to encrypt the data is 0.2972729 ms in 512-bits key length using the proposed solution, and to encrypt the data using AES is 0.8918188 ms in 512-bits key length.

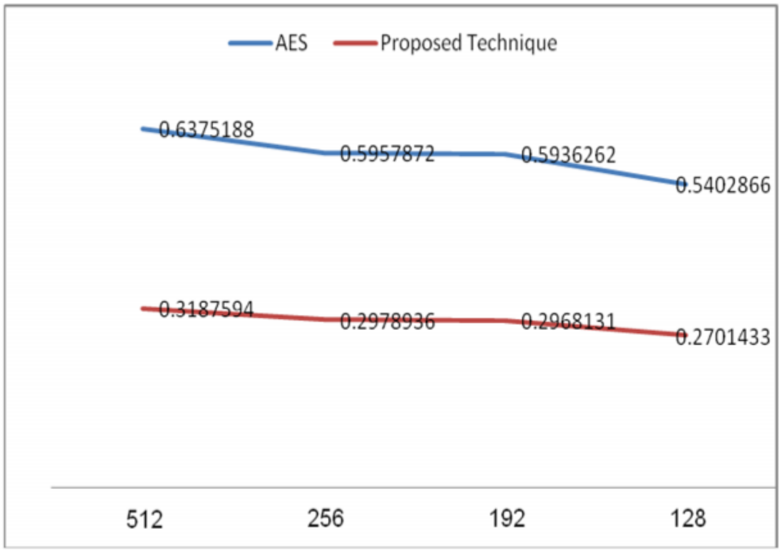

Figure 7. Column chart for decryption process in both cases

As well as, the result shows that the average time required to decrypt the data is 0.3187594 ms in 512-bits key length using the proposed solution, and to decrypt the data using AES is 0.6365188 ms in 512-bits key length. In other words, the result in this paper shows the average time needed to encrypt and decrypt a data using a proposed algorithm is much smaller than AES algorithm.

4. SECURITY ANAYSIS

In order to test the security level of the proposed algorithm, a set of tests and analysis are performed on the algorithm. Some of these tests are taken from different cryptanalysis papers, NIST statistical suite, and combination of several other statistical analyses. The following analysis methods are performed on the algorithm: Information Entropy [13], correlation analysis between the public and private positions [14-15].

4.1. Correlation Analysis

As we mentioned in section 2.1, RC6 algorithm play major roles to generate a private position based to the secrete value from public key infrastructure. To analyze the correlations between the public and the private positions, correlation coefficients test is used. The correlation coefficients rules are described by a pseudo-code shown in figure 8 [13, 15].

```
If (CC = = 0 )
Then
Private table NOT EQUAL Public table
else
Private table EQUAL public table
Where,
CC represents correlation coefficients
```

Figure 8. Rules of correlation coefficients

In correlation analysis, we randomly choose different values in the public and private positions (8*8 matrix). The correlation coefficients of the public and the private positions in vertical, horizontal, and diagonal directions were calculated. The correlation coefficients for the three dimensions in the private positions are close to zero, and for public positions are close to one. This indicates that the public and private positions are not correlated.

4.2. Information Entropy

To calculate the entropy H(X), we have:

$$H(X) = \sum_{i=1}^{n} p_i \log_2\left(\frac{1}{p_i}\right)$$

The entropy H(X) rules are described by a pseudo-code as shown in figure 9. The result shows the entropy value H (X) for the proposed algorithm is 7.98789 which is very close to the theoretical value 8. This indicates that the encryption algorithm is secure upon the entropy attack.

If (H(X) ideally close (smaller than) to 8)
Then
There is no predictability which threatens the security threatens exists
else
If (H(X) less than 8)
Then
There exists a predictability which threatens the security

Where,
H(X) represents Information Entropy

Figure 9. Rules of Information Entropy

4.3. The Strength of Encryption

The strength of encryption measure by the time required to decode or extract the key [10]. The calculation of encryption strength of an encryption algorithm the following equation is used [16].

$$\frac{(\text{Differential Characteristic})^{-1/2} * \text{CompSpeed}}{3600\ \text{second} * 24\ \text{houres} * 365\ \text{days}}$$

Differential Characteristic = (p1p2) −1 ×Filtering weight. The result shows, the proposed algorithm needed 1.00E+68 time (Years) to crack.

5. CONCLUSION

This paper introduced a new approach for complex encrypting and decrypting data. Although there have been many researchers on the cryptography, but most of the existing algorithms have several weaknesses either caused by low security level or increase the delay time due the design of the algorithm itself. The proposed algorithm have been tested against different known attacks and proved to be secure against them. Therefore, it can be consider as a good alternative to some applications because of the high level of security and average time needed to encrypt and decrypt a data using a proposed algorithm is much smaller than AES algorithm.

REFERNCES

[1] P. Zimmerman, "*An Introduction to Cryptography"*, Doubleday & Company, Inc., United State of America, USA, 1999.

[2] C. Shannon, “Communication Theory of Secrecy Systems”, *Bell Systems Technical Journal*, *MD Computing*, vol. 15, pp. 57-64, 1998.

[3] I. Nichols, K. Randall (1999), ICSA Guide to Cryptography, McGraw-Hill, Companies Inc, New York.

[4] H. Mohan, and R. Raji. "Performance Analysis of AES and MARS Encryption Algorithms". *International Journal of Computer Science Issues (IJCSI),* Vol. 8, issue 4. 2011.

[5] A. Lee, NIST Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government, National Institute of Standards and Technology, November 1999.

[6] J. Nechvatal, Report on the Development of the Advanced Encryption Standard (AES), National Institute of Standards and Technology, October 2, 2000.

[7] M. Wali and M. Rehan, “Effective Coding and Performance Evaluation of the Rijndael Algorithm (AES)”, *in the Proceedings of the Engineering Sciences and Technology Conference*, vol. 7, pp. 1-7, Karachi, 2005.

[8] C. Jie, “Design Alternatives and Implementation of PKI Functionality for VoIP”, Master of Science dissertation, Telecommunication Systems Laboratory, Royal Institute of Technology (KTH), Stockholm, 2006.

[9] R. Hunt, “PKI and Digital Certification Infrastructure”, *in the Proceedings Ninth IEEE International Conference on Networks*, vol. 4, pp. 234 – 239, Bangkok, Thailand, 2001.

[10] S. Xenitellis, *The Open–Source PKI Book: A Guide to PKIs and Open-Source Implementations,* Open CA Team, 2000.

[11] W. Emm, “Impact of Multiencryption in Data Security”, *International Journal of Computer Theory and Engineering*, vol. 1, pp. 571-567 , 2009.

[12] B.D.C.N.Prasad, P E S N Krishna Prasad, “A Performance Study on AES algorithms”, International Journal of Computer Science and Information Security, Vol. 8, No. 6,September 2010,pp 128-132.

[13] S. Tao, W. Ruli, and Y. Yixun, “Clock-Controlled Chaotic Key-Stream Generators”, *Institution of Engineering and Technology Electronics Letters*, vol. 34, pp. 1932-1934, 1998.

[14] A. Masoun, ”Cryptography Primitives Based on Piecewise Nonlinear Chaotic Maps”, Master of Science dissertation, Universiti Sains Malaysia (USM), Pineng, Malaysia, 2008.

[15] Obaida. Al-Hazaimeh, " Increase the Security Level for Real-Time Application Using New Key Management Solution", *International Journal of Computer Science Issues(IJCSI),* Vol. 9, Issue 3, 2012.

[16] L. Chang-Doo, C. Bong-Jun, P. Kyoo- Seok (2004), “Design and evaluation of a block encryption Algorithm using dynamic-key mechanism”, Future
Generation Computer Systems 20, 327–338.

Authors

Obaida Mohammad Awad Al-Hazaimeh received the B.S. degree in Computer Science from Applied Science University (ASU), Jordan in 2004, the MSc in Computer Science/ Distributed system from University Science Malaysia (USM), 2005, and PhD in Computer Science/ Network security (Cryptography) for Real-Time Application (VoIP), 2010.