An Enhanced Hybrid Cryptosystem based on DNA Computing

Brahim ouchao[1], Fatima Amounas[1], Hassain Sadki[1], Lahcen el Bermi[2]
[1]R.O.I Group, Computer Sciences Department, Faculty of Sciences and Technics, Moulay Ismaïl University, Errachidia Morocco
[2]GL-ISI, Computer Sciences Department, Moulay Ismaïl University, Faculty of Sciences and Technics, Errachidia, Morocco

Abstract— *Encryption is critical method to give secrecy while transmitting information over Internet. There are many methods used for encrypting and decrypting text message, image or other important data. This paper deals with a new hybrid cryptographic technique using combination of AES Algorithm and Elgamal cryptosystem based DNA computing. Further, this paper attempts to utilize the properties of DNA in encryption and decryption process with more efficient. The performance of the proposed scheme is compared with the existing cryptosystems. The steps of the implementation of our algorithm are also investigated.*

Keywords—*Cryptography, AES, Elgamal, Deoxyribo Nucleic Acid Encryption, ASCII.*

I. Introduction

The goal of Information security is to achieve confidentiality by cryptography. There are many techniques to achieve the security of information from unauthorized access. There are many techniques to achieve the security of information from unauthorized access. There are two cryptographic techniques used for data encryption which are Symmetric and Asymmetric techniques. Hybrid system is a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. It incorporates two or more encryption algorithms [1], [2]. In fact, asymmetric encryption can slow down the encryption process, but with the simultaneous use of symmetric encryption, both forms of encryption are enhanced.

DNA cryptography is a new optimistic field in cryptography which hides the data in terms of DNA sequence to make it secured. In this paper, we attempt to provide a hybrid encryption technique using a mixed encryption model based on AES and Elgamal cryptosystems. The Elgamal cryptosystem is based on discrete logarithm problem. Here, we improve the strength of Elgamal cryptosystem using DNA computing. This will provide a higher level of security. The rest of the paper is structured as follows: Section 2 briefly reviews some important background. Section 3 is devoted to proposed method. Section 4 gives a brief illustration with an example. Section 5 shows the results and comparisons of the proposed scheme with existing systems. The paper is concluded in section 6.

II. Background Information

A. Cryptography

Cryptography is the science or art of changing text to a coded form that makes the text unreadable for those people you don’t want to read it. The process of converting plain text to cipher text using some mechanism is called encryption. Decryption is converting the cipher text back to simple text form. There are two cryptographic techniques [3]: Symmetric and Asymmetric techniques. Private key cryptography is also known as symmetric key cryptography. In private key cryptography, the encryption and decryption both happen to be done using the same key. Examples are DES and AES cryptosystems. Public key cryptography is also known as asymmetric key cryptography. A key is basically a value that is used in an algorithm for cryptography to convert plain text to cipher text. That has a huge worth and is also measured in parts.

B. AES Cryptosystem

The Advanced Encryption Standard (AES) was proposed as a suitable replacement of the existing Data Encryption Standard (DES). It is a block cipher which takes as input a 128 bit plaintext, which is subject to an encryption with 128, 192 and 256 bit key depending upon the number of rounds i.e 10,12 or 14 respectively [4].

The various internal rounds that take place for encryption and decryption processes are explained in [5]. It broadly consists of substitution, shifting of rows, mixing of columns based on modular arithmetic multiplication followed by adding of round key till n-1 rounds. Mix column round is omitted in the final nth round. After the nth round a 128 bit cipher text is obtained. Today, AES system is one of the most practical symmetric cryptosystem and is widely used for secure data transmission.

C. Elgamal Cryptosystem

In 1984, Taher Elgamal announced a public key scheme based on discrete logarithms [6]. The Elgamal scheme is used for both digital signatures and encryption, and its security results from the difficulty of calculating discrete logarithms in a finite field [7]. This algorithm usually works in a multiplicative group of GF(p). In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret [8]. In Elgamal, this asymmetry is based on the practical difficulty of solving the logarithm discrete problem (PLD).

The Elgamal encryption algorithm works as follows:

When the user A wants to communicate secretly with the user B, they proceed thus:

Key generation:
- B Generates a cyclic group G of order p with generator g.
- B chooses randomly an integer k from {1, …, p-1}.
- B computes $x = g^k$.

B publishes x as her public key (while k remains secret).

Encryption: To encrypt a message m to B, the user A does the following steps:
- A chooses a random h from {1,…, q-1}, then computes $C_1 = g^h$.
- A computes the shared secret $y= x^h$.
- A imbeds his secret message m onto an element m’ of G. Then computes C_2=m’y.
- A sends the cipher text (C_1, C_2) to B.

Decryption: To decrypt a cipher text (C_1, C_2), B does the following steps:
- Computes the shared secret $y= C_1^k$. Then computes $m'=C_2y^{-1}$ where y^{-1} is the inverse of y in the group G.
- Reverses the embedding to get back the plaintext message m.

D. *Deoxyribonucleic Acid (DNA)*

DNA is a molecule called nucleotide, that caries most of the genetic instructions used in the development functioning and reproduction of all known living organisms and many viruses. Most DNA molecules consist of two biopolymer strands coiled around each other to form a double helix. The two DNA strands are known as polynucleotides since they are composed of simpler units called nucleotides. Each nucleotide is made up of one of four nitrogen-containing nucleobases: cytosine (C), guanine (G), adenine (A), or thymine (T) a sugar called deoxyribose, and a phosphate group. Recently, DNA computing had been used in cryptography to enhance the public key encryption methods and speed up its decryption [9-11].

DNA coding method is a procedure for conversion of plain text to ASCII code and subsequent conversion of ASCII code to DNA sequence [12]. For DNA, there are four basic units which are encoded into binary in the following manner:

TABLE I. DNA encoding.

DNA Sequence	A	C	G	T
Binary form	00	01	10	11

III. PROPOSED SYSTEM

Hybrid encryption algorithms may be developed from combining the operating modules of two or more different encryption algorithms. In this context, we attempt to put up an encryption algorithm that combines AES cryptosystem and Elgamal public-key cryptosystem based DNA computing. The flowchart of Fig. 1 explains the architecture of the proposed encryption and decryption method. In hybrid algorithm, the message is encrypted by the system as defined in algorithmic rule:

- Encryption process by using AES cryptosystem.
- Repeat encryption by using Elgamal Algorithm.
- Improving the structure of the system using DNA computing.

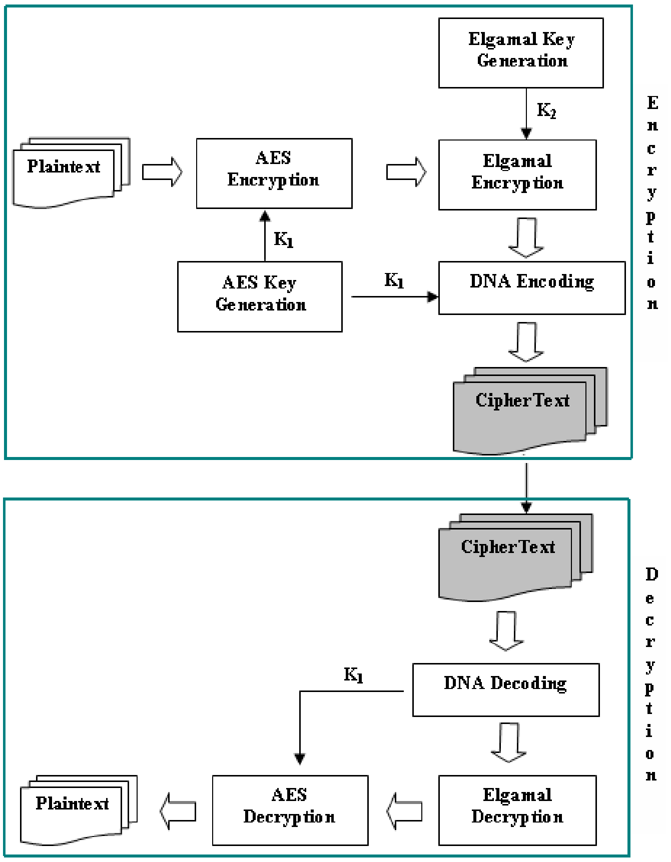

Fig. 1. Flowchart of the proposed system.

The above mentioned system is structurally divided into three phases as follows:

A. *Initial Phase*

- Generate the symmetric AES key.
- Generate of Elgamal private and public keys

B. *Encryption Process*

1. The input is considered as text file.
2. The plain text is being given as input to AES algorithm, which encrypts to give encrypted message.
3. The result ciphertext denoted plaintext which being applied to Elgamal algorithm for further encryption.
4. Convert the obtained values into binary form and then encode it by DNA coding and transform it into data nucleotides sequence.
5. Now, Send encrypted message along with encrypted AES key to the receiver.

C. *Decryption Process*

The receiver extracted the original data by using the following steps:

1. Apply DNA decoding process
2. Apply Elgamal decryption process.
3. Apply AES key to recover plaintext.

IV. Illustration with an Example

Now the encryption-decryption process is illustrated by using the plaintext “Thank you IRJAES” as below:

Step 1. Generate a random key of size= 8×n (128 bits). Let it is
41 45 43 20 63 72 79 70 74 6F 73 79 73 74 66 6D

Step 2. Get the ASCII values of each character of input string as follows:
45 68 61 6E 6B 20 79 6F 75 20 49 52 4A 41 45 53

Step 3. Apply AES encryption algorithm to generate ciphertext C_1 as:
34 5E B3 F2 46 A4 54 E3 38 C2 74 E1 3D 6F 5D 2B

Step 4. Now every ASCII value is encrypted by Elgamal cryptosystem. Then the result ciphertext C_2 becomes:
435 2256 904 624 1485 2045 370 2454 921 1636 878 73 710 861 848 1059 1072

Step 5. Convert the result cipher into binary form and perform the right circular shifts of binary values m times.

Step 6. Convert the data sequence into DNA cipher as follows:
CTGCGGCTAGTTATACAGTAAGCCTAGGCTAAACAG
CACGAACTTAGAGTGCATTTATAGCATGAGATGAAT
GGCAGTAGATTACATCTATCGATATATCTAATTTCAT
CGATCAATGACATCAGGTGCATTAGATACATACATC
GATATATCGTGAATCTATGAATCTATATATCTATACA
TAAATGAATCGATACATGAATCAATGAAATCAAGGA
TACATAAATCCATGCAATCAAGGATACATATTTCTAG
AGTTACGAGC

Step 7. Sends the result cipher text along with DNA key sequence to the receiver.

The recovery of cipher text is done as follows:

Step 1. Take cipher text and find out the DNA key sequence.

Step 2. Decode DNA cipher into binary form and perform the left circular shifts of binary values.

Step 3. Convert the data sequence to get the ASCII values.

Step 4. Perform Elgamal decryption algorithm to decrypt the cipher text C_2.

Step 5. Now, perform AES decryption process to decrypt the cipher text C_1.

V. Experimental Result

The hybrid system is implemented on the text data of various sizes using a netbeans 7.1 as tools [13]. The comparison is done in terms of encryption and decryption time measured in seconds.

The table II shows the results of the comparative analysis between the proposed hybrid system and the existing algorithms. Fig. 2 and Fig. 3 show a graphical representation.

TABLE II. Comparison between the proposed algorithm and existing systems in term of execution time.

	Encryption time			Decryption time		
Size (KB)	DES	RSA	Hybrid Alg.	DES	RSA	Hybrid Alg.
50	2.64	7.26	1.29	3.26	7.93	1.64
100	2.78	7.74	1.33	3.62	8.34	2.08
200	2.83	8.48	1.56	3.97	9.48	2.55
300	3.46	9.75	1.92	4.92	9.87	3.12
500	4.45	11.16	2.45	6.31	12.06	3.65

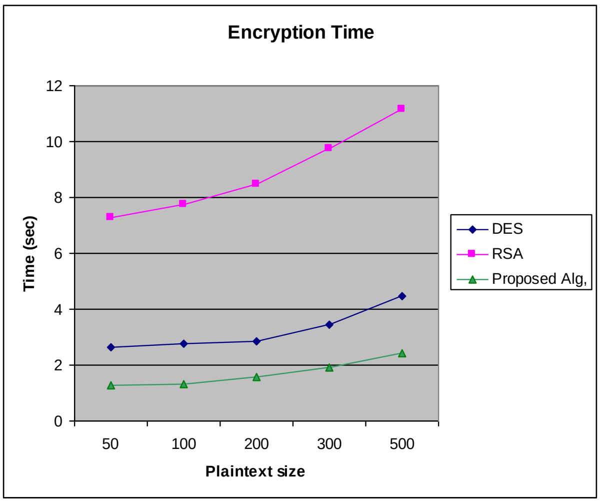

Fig. 2. Encryption time comparison.

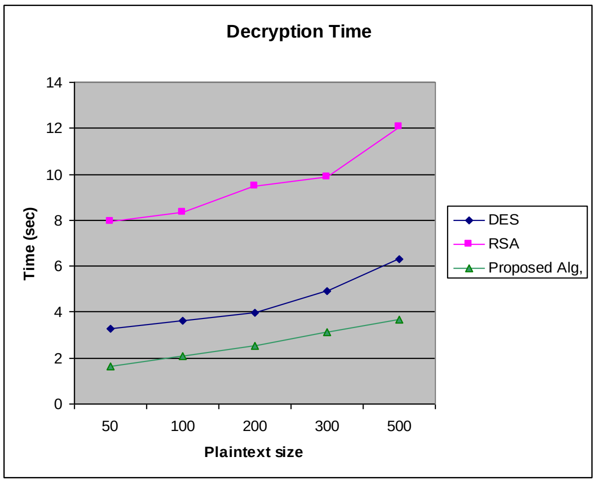

Fig. 3. Decryption time comparison.

According to the graph, it can be clearly seen that the proposed algorithm producing good results and hence can be incorporated in the process of encryption of any plain text.

VI. Conclusion

This paper presents an effective method that combines techniques that can be used to successfully communicate secretively in a network. The proposed algorithm reduces the effectiveness of brute-force attacks. The proposed system can obtain higher level of security using the properties of DNA computing. From the results comparison it is analyzed that efficiency of the proposed hybrid cryptosystem is very high as compared to existing cryptosystems. So, the proposed system will be suitable for practical use in the secure transmission over the Internet.

References

[1] R. K. Gupta and S. Parvinder, “A new way to design and implementation of hybrid crypto system for security of the information in public network,” *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 8, pp. 108-115, 2013.

[2] D. Chandravathi and Dr. P. V. Lakshmi, “A new hybrid homomorphic encryption scheme for cloud data security,” *Advances in Computational Sciences and Technology*, vol. 10, no. 5, pp. 825-837, 2017.

[3] A. Al-Vahed and H. Sahhavi, “An overview of modern cryptography,” *World Applied Programming*, vol. 1, issue 1, pp. 3-8, 2011.

[4] N. Khatri, R. Dhanda, and J. Singh, “Comparison of power consumption and strict avalanche criteria at encryption/decryption side of different AES standards,” *International Journal of Computational Engineering Research*, vol. 2, Issue 4, 2012.

[5] “Advanced Encryption Standard (AES),” Federal Information Processing Standards Publication 197, November 26, 2001.

[6] T. Elgamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” *IEEE, Transactions on Information Theory*, vol. 31, pp. 473- 481, 1985.

[7] S. William, *Cryptography and Network Security Principles and Practice*, Fifth Edition, Pearson Education, Prentice Hall, 2011.

[8] A. Shetty, Shravya Shetty K, and Krithika K, “A review on asymmetric cryptography -RSA and ElGamal algorithm,” *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, special issue 5, pp. 98-105, 2014.

[9] T. Mandge and V. Choudhary, “A DNA encryption technique based on matrix manipulation and secure key generation scheme,” *International Conference on Information Communication and Embedded Systems*, 21-22 Feb., 2013.

[10] T. Anwer, A. Kumar, and S. Paul, “DNA cryptography based on symmetric key exchange,” *International Journal of Engineering and Technology*, vol. 7, no. 3, pp. 938-950, 2015.

[11] P. Barman and B. Saha, “An efficient hybrid elliptic curve cryptography system with DNA encoding,” *International Research Journal of Computer Science*, vol. 2, issue 5, pp. 33-39, 2015.

[12] A. Agrawal, A. Bhopale, J. Sharma, M. Shizan Ali, and D. Gautam. “Implementation of DNA algorithm for secure voice communication,” *International Journal of Scientific & Engineering Research*, vol. 3, issue 6, pp. 1-5, 2012.

[13] Herbert Shildt, *Java Complete Reference*, Tata McGraw-Hill, 2011.