Penerbit Akademia Baru

Journal of Advanced Research Design

Journal homepage: www.akademiabaru.com/ard.html
ISSN: 2289-7984

Blowfish Security Enhancement using DNA–Genetic Technique

Open Access

H. Elkamchouchi[1,*], F. Ahmed[2], A. Abd ElMaksoud[3]

[1] Faculty of Engineering, Alexandria University, Alexandria, Egypt
[2] Alexandria Higher Institute of Engineering and Technology, Alexandria, Egypt
[3] El Gazeera Higher Institute of Engineering and Technology, Cairo, Egypt

ARTICLE INFO

Article history:
Received 5 July 2017
Received in revised form 10 October 2017
Accepted 14 December 2017
Available online 22 March 2018

Keywords:
Confusion, diffusion, blowfish algorithm, DNA sequence, genetic algorithm, security analysis

ABSTRACT

A composite algorithm for improving Blowfish security is achieved by using a DNA and Genetic technique. In this paper, the data input is changed using rotation and XOR'ed which gives us high confusion and diffusion. Then this data encrypted with Blowfish algorithm produces a cipher text. To increase the security of this cipher text several stages are added. The cipher text is converted to DNA sequence and the stages of a genetic technique are used by dividing cipher text into chromosomes of fixed length, each chromosome consists of 32 elements of DNA. Then cross over the chromosomes to produce new offspring and each offspring is mutated. The proposed algorithm is compared with Blowfish algorithm that produces highly avalanche effect. The new algorithm is compared with Blowfish and gives excellent results from the viewpoint of the security characteristics and the statistics of the cipher text.

1. Introduction

Due to the rapid growth of networks, information security becomes more substantial for protecting commerce secrecy and privacy. There are many Encryption algorithms which are used for information security. They are labeled into two types depending on the type of security keys. The two labels are symmetric and asymmetric encryptions. In symmetric or private encryption only one key has been used to encrypt or decrypt the data, like 'BLOWFISH' algorithm [1]. While in a symmetric or public key encryption the sender and the receiver have two keys, one is a public key and the other is a secret key which is known by the sender and the receiver only. An example of Public Key algorithms: Diffie-Hellman, Rivest-Shamir-Adleman (RSA) [2].

Many researchers have been completed in the field of cryptography using different methods. In [3] the DNA cryptography is used for hiding data transmission and increase the security of data. The algorithm selected a DNA sequence. The DNA sequence is a combination of A, C, G and T base pairs.

* *Corresponding author.*
E-mail address: Helkamchouchi@ieee.org (H. Elkamchouchi)

As the next step, a single letter is replaced with a specific letter defined by the complementary rule that based on the properties of a nucleic acid. In [4] the encryption algorithm used the one-time pad (OTP) technique through which the data could secure within DNA sequences and its structure. In [5] Proposed system was symmetric algorithm depends on the random key generation of DNA pattern. The steps of this algorithm are Encryption, Random Key Generation, and Decryption.

In this paper, a new symmetric algorithm based on Blowfish algorithm and DNA-Genetic techniques are suggested. The data input is rotated and XOR'ed with the key. Then Blowfish algorithm is used to produce cipher text. This cipher text would be applied on DNA-genetic techniques, which are used for four stages of proposed algorithm. First, the encrypted data has been converted to DNA sequence. Second, the DNA sequence has been reshaped in the form of blocks; each block consists of 32 elements. Third, the crossover has been applied by rotating left in elements. Finally, the mutation has been performed by complementing the elements of DNA sequence.

When comparing the suggested algorithm in this paper and the referred researchers above we find that in [3] works with complementary rules only and in [4] uses one-time pad for encrypting data, while in this work, the data input is rotated and XOR'ed with key and encrypted with blowfish algorithm which gives a higher security then uses DNA- genetic technique to increase data secrecy.

The rest of this paper is introduced as follows, in section 2, the proposed algorithm is presented. In section 3, security analysis is introduced. Finally, the conclusion is illustrated in section 4.

2. The Proposed Data Encryption Algorithm

Data encryption algorithm is suggested with different algorithms like Blowfish algorithm, for improving the security of this algorithm, we constructed more stages, the main stages of the proposed algorithm is illustrated in Figure 1.

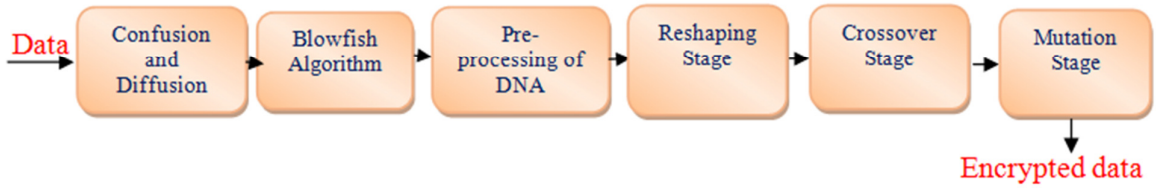

Fig. 1. Block diagram of the proposed algorithm

2. 1 Confusion and Diffusion

The term confusion and diffusion was announced by cloud Shannon to advance a product cipher that substitute's confusion and diffusion functions. The term confusion referred to that changing 1-bit of the key which will cause a total change in the corresponding cipher text. While the term diffusion is referred to that changing in 1-bit of the plaintext which will cause a total change in the corresponding ciphertext [6].

In this stage, we presented that by constructing an array of the same length of the message and divided the length of the key to 64-blocks, which can fill in 7 blocks of the array. The rest of this array is filled by rotating left to 12 bits of the whole bits of the key then still doing this until the array has been loaded. After that counting one in every block of the original key and rotating the message left by this number. Finally XOR'ed this message with key to produce a new plaintext to be ready for encryption with Blowfish algorithm. In the following stage, the blowfish algorithm has been used for encrypting data to produce ciphertext [7-10].

2.2 Pre-Processing of DNA Sequence

DNA is deoxyribonucleic acid, DNA has been used for storing and transferring data. The idea of utilizing DNA in the fields of cryptography has been recognized as a possible technology that may bring forward a new hope for unbreakable algorithms. Strands of DNA are long polymers of millions of linked nucleotides. These nucleotides consist of one of four nitrogen bases, the nucleotides that make up these polymers are named after the nitrogen base that it consists of; Adenine (A), Cytosine (C), Guanine (G) and Thymine (T).where A and T, C and G are complementary pairs [11].

After encrypting data with Blowfish algorithm, DNA sequence has been used by converting the encrypted data to ASCII code, then group them into 8-bits of binary data. Every two adjacent bits has been transferred to the corresponding DNA sequence according to the following Table1.

Table 1
DNA and Representation of bits

Bits	DNA
00	A
01	C
10	G
11	T

2.3 Reshape Stage

After Encryption and converting data to DNA sequence, the genetic technique that consists of three basic operations: reproduction, crossover, mutation [12] has been used to generate a genetic material that passes to the next operation in the form of chromosomes. The Reshaping stage has been used. In this stage, first number and length of a chromosome are defined. Reshape it by stratifying the DNA sequence into rows to construct parents' chromosomes (chromosome population). Each chromosome consists of 32 elements from DNA sequence.

2.4 Crossover Stage

After constructing parent's chromosomes, the next stage is how to produce a new child from these parents chromosomes, this step can be achieved by using crossover method. The crossover can be satisfied by rotating left/right for some element in the parent's chromosomes to get new off springs (child) that will achieve the mutation.

2.5 Mutation Stage

After crossover stage, the new offspring has been subjected to the mutation stage. Mutation is the permutation of string elements. In this stage, mutation is done by converting every four bits to two elements of DNA sequence (0001->AC), then complement the elements with it opposes one according to Table 2**.**

Table 2
Mutation of data

NA	its	NA	its	NA	its	NA	its
A	000	A	100	A	000	A	100
C	001	C	101	C	001	C	101
G	010	G	110	G	010	G	110
T	011	T	111	T	011	T	111

3. Security Analysis

In order to achieve the data protection for several genders of attacks. Inspection of performance analysis has been utilized to elucidate the proposed algorithm [13]. In this section, the security analysis of encryption algorithm using blowfish, DNA-Genetic technique has been explained in details. We discuss the avalanche effect of plaintext and ciphertext, statistical analysis of the ciphertext.

3.1 Avalanche Effect

Avalanche effect is obvious that if, change of one bit in the plaintext or key will cause a significant change in the ciphertext. A desirable feature of any encryption algorithm is that small change in the plaintext or key must make a significant change in the ciphertext [14]. Table 3 and 4 Shows the result obtained after changing one bit in the Plaintext or key with different size using avalanche effect. The avalanche effect is calculated as:

$$Avalanche\ \ effect = {no\ \ of\ \ flipped\ \ in\ \ the\ \ ciphertext} \Big/ {no\ \ of\ \ bits\ \ in\ \ the\ \ ciphertext} \times 100 \quad (1)$$

Table 3
Avalanche effect for one bit change in plaintext

P.T	Length of P.T in bits	Change first bit in plaintext		Change middle bit in plaintext		Change last bit in plaintext	
		B.F	Proposed	B.F	Proposed	B.F	Proposed
Case 1	158656	0.015%	49.99%	0.021%	49.99%	0.0176%	49.99%
Case 2	1024	2.44%	50.19%	2.92%	49.51%	2.53%	50.39%

Table 4
Avalanche effect for one bit change in key

P.T	Length of P.T in bits	Change first bits in key		Change middle bits in key		Change last bits in key	
		B.F	Proposed	B.F	Proposed	B.F	Proposed
Case 1	158656	49.93%	50.1%	49.90%	50.06%	50.03%	50.26%
Case 2	1024	50.58%	52.14%	47.85%	49.41%	49.70%	50.97%

The avalanche effect of the proposed algorithm provides higher value than Blowfish algorithm because in Blowfish algorithm it works in its data block. While in our case, we use DNA and genetic technique that make a different change when changing one bit.

3.2 Language Statistics

Shannon suggested a new method to appraisal entropy and redundancy of a language. A cryptosystem is deliberated unbreakable against statistical analysis if its ciphertext has flat distribution [15]. Figure 2 shows the plaintext statistics of text file used and the cipher text statistics of Blowfish and proposed algorithm are plotted in Figure 3 and Figure 4.

3.3 Analysis Method in Strict Avalanche Criterion

The Strict Avalanche Criterion (SAC) was presented by Webster and Tavares in a survey of scheme criteria for definite cryptographic functions. A Boolean function $f: z_2^n \to z_2$is said to content with the SAC if complementing a single input bit results in changing the output bit with probability accurately one-half. In this section, two analysis techniques for strict avalanche criterion (SAC) are tested [16].

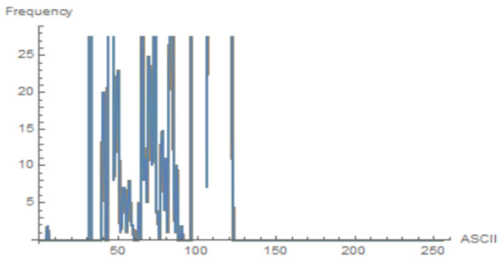

Fig. 2. Plaintext statistics of text file

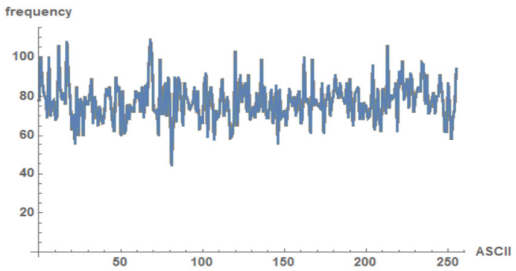

Fig. 3. Ciphertext statistics of Blowfish

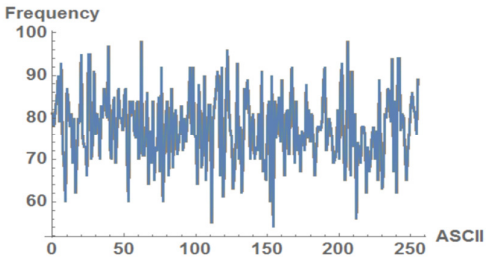

Fig. 4. Ciphertext statistics of proposed

3.3.1 Analysis of the frequency of various hamming weight

In this technique, if the frequency of testing result is as like as Gaussian diagram, this result shows the cipher has good properties of Strict Avalanche Criterion. Figure 5 and Figure 6 shows the Hamming weight of Blowfish and Proposed algorithm.

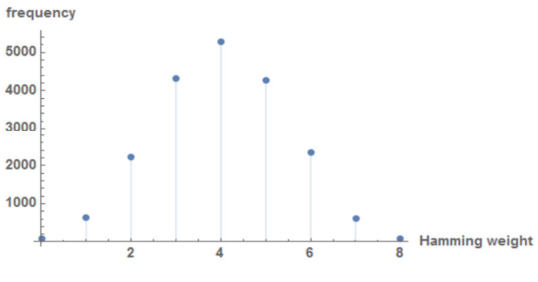

Fig.5. Blowfish analysis of the frequency of various Hamming weight

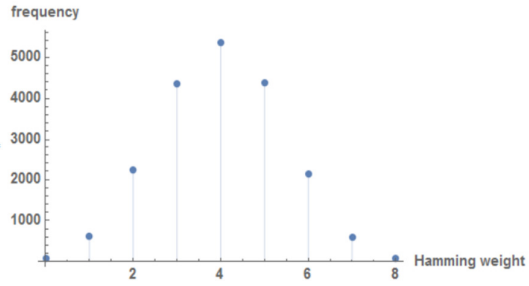

Fig. 6. Proposed analysis of the frequency of various Hamming weight

3.3.2 Analysis of the frequency of various differential value

In this technique, if the frequency of testing result has near values, this result shows the cipher has good properties of completeness properties. Figure 7 and Figure 8 shows the differential value of Blowfish and Proposed algorithm.

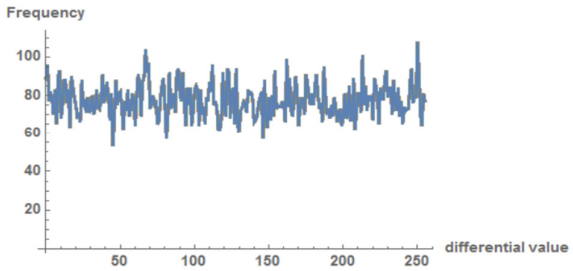

Fig. 7. Blowfish analysis of the frequency of various differential value

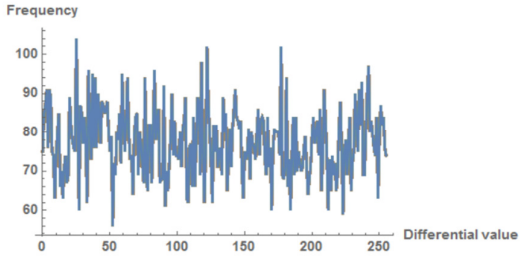

Fig. 8. Proposed analysis of the frequency of various differential value

4. Conclusion

In this paper, we introduce a new algorithm based on Blowfish algorithm and DNA Genetic technique. We have enhanced the security of Blowfish algorithm by rotating the bits of key and plaintext then XOR'ed them to produce new plaintext for blowfish algorithm. After encrypting this plaintext with blowfish several stages of the DNA-Genetic technique were added. We have converted data into DNA sequence and rotating this data to the left as the crossover stage in order to produce new encrypted data that delivered to mutation stage. In this work, if we changed several bits in the plaintext or the key, more than half of the bits were changed in the cipher text. When the Hamming weight of Blowfish and the proposed algorithm is tested, we got that both of them satisfied Gaussian curve but the proposed algorithm satisfied that with a higher value than the unaided Blowfish algorithm.

References

[1] P. Rohilla, "Blowfish algorithm: Security and Performance Enhancement," in World Academy of Informatics and Management Sciences(WAIMS), Vol1 Issue5, 2012.

[2] Scholar, P., and Jijo S. Nair. "A Review of Image based Cryptography." *International Journal of Computer Security & Source Code Analysis* 1, no. 3 (2015): 13-16.

[3] Menaka, K. "Message encryption using DNA sequences." In *Computing and Communication Technologies (WCCCT), 2014 World Congress on*, pp. 182-184. IEEE, 2014.
[4] Kumar, Deepak, and Shailendra Singh. "Secret data writing using DNA sequences." In *Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference on*, pp. 402-405. IEEE, 2011.
[5] Raj, Bonny B., J. Frank Vijay, and T. Mahalakshmi. "Secure Data Transfer through DNA Cryptography using Symmetric Algorithm." *International Journal of Computer Applications*133, no. 2 (2016): 19-23.
[6] Stallings, William. *Cryptography and network security: principles and practices*. Pearson Education India, 2006.
[7] Chaudhari, Maulik P., and Sanjay R. Patel. "A survey on cryptography algorithms." *International Journal of Advance Research in Computer Science and Management Studies* 2, no. 3 (2014).
[8] Haldankar, Chaitali, and Sonia Kuwelkar. "Implementation of AES and Blowfish Algorithm." *International Journal of Research in Engineering and Technology* 3, no. 03 (2014): 143-146.
[9] ALabaichi, Ashwak, Ramlan Mahmod, and Faudziah Ahmad. "Analysis of some security criteria for S-boxes in blowfish algorithm." *International Journal of Digital Content Technology and its Applications* 7, no. 12 (2013): 8.
[10] S Manku, Saikumar, and K. Vasanth. "Blowfish encryption algorithm for information security." *ARPN Journal of Engineering and Applied Sciences* 10, no. 10 (2015): 4717-4719.
[11] Song, Chunyan, and Yulong Qiao. "A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos." *entropy* 17, no. 10 (2015): 6954-6968.
[12] Mitchell, Melanie. *An introduction to genetic algorithms*. MIT press, 1998.
[13] Mousa, Ayman, Osama S. Faragallah, S. El-Rabaie, and E. M. Nigm. "Security analysis of reverse encryption algorithm for databases." *International Journal of Computer Applications*66, no. 14 (2013).
[14] Kulsoom, Ayesha, Di Xiao, and Syed Ali Abbas. "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules." *Multimedia Tools and Applications* 75, no. 1 (2016): 1-23.
[15] Schneider, Bruce. *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons, 1996.
[16] Mar, Phyu Phyu, and Khin Maung Latt. "New analysis methods on strict avalanche criterion of S-boxes." *World Academy of Science, Engineering and Technology* 48, no. 150-154 (2008): 25.