AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

A New Bio-inspired Computing Algorithm for Symmetric Encryption

[1]Ms Bonny B Raj and [2]Dr J Frank Vijay

[1]*Department of Computer Science and Engineering Hindustan University, Chennai, India.*
[2]*HoD in Information Technology KCG College of Engineering and Technology Chennai, India.*

Address For Correspondence:
Ms Bonny B Raj, Department of Computer Science and Engineering Hindustan University, Chennai, India
E-mail: bonzbaburaj@gmail.com

ARTICLE INFO
Article history:
Received 12 January 2016
Accepted 22 February 2016
Available online 1 March 2016

Keywords:
Bio-inspired computing; Symmetric Encryption;

ABSTRACT
In this paper, a new Bio-inspired computing algorithm for symmetric encryption. Information flows throughout the network that can be of local or of global scope. It is mandatory to secure information from unauthorized access of it by any node in the path. So security is necessary before encryption. This paper proposes a symmetric key generation method which generates primary cipher and it is then converted into final cipher using random key generated DNA sequences, so that reading can be complicated.

INTRODUCTION

Cryptography and data security helps in secure transmission and storage of information via insecure internet. Most cryptographic systems applies encryption of valuable information and produces an encrypted output which may be meaningless to an eavesdropper who has no knowledge of the key. The fundamental tool for cryptography is a simple function which is easy to compute but hard to invert. In cryptography both encryption and decryption phase are determined by keys. Depending on keys, cryptographic systems are classified as Symmetric Key Cryptography (SKC) and Asymmetric Key Cryptography (AKC). Symmetric Key Cryptographic systems use same keys for both encryption and decryption process where as Asymmetric Key Cryptographic system uses different keys for both encryption and decryption process. Asymmetric Key Cryptographic systems are known as Public Key Cryptographic systems (Sireesha, K., V. Srujana, 2013).

Biologically-inspired computing is an area of study which includes areas of connectionism, social behavior and its emergence. Bio-inspired computing is the use of different computers to model living phenomena and simultaneously the nature study to improve the usage of computers (Priyadharshini, V., *et al*., 2015). Bio-inspired techniques often involve a set of simple organisms that adhere a set of specific mathematical rules and properties of iterations and its applications. Some forms of complex behavior arises after several generations of rules (Camelia, Mihaela Pintea, 2014). Complexity gets built upon more and more until the result is something most complicated and often completely different from the original rules that would expected to produce. DNA computing is a very good example for Bio-inspired computing.

Dna Based Cryptography:

De-oxyribo nucleic acid, (DNA) contains genetic instructions which can be used for the growth and functioning of all living being. DNA is a collection of complex organic molecules. The substance that is found in every cell of the organism which make them unique. DNA is often compared with a set of blueprints, like any other code. They also contains the instruction that are required to construct other components of cells such as proteins, RNA molecules etc. The DNA segments that hold this genetic information are known as genes,

To Cite This Article: Ms Bonny B Raj and Dr J Frank Vijay., A New Bio-inspired Computing Algorithm for Symmetric Encryption. ***Aust. J. Basic & Appl. Sci.,*** *10(5): 134-136, 2016*

Australian Journal of Basic and Applied Sciences, 10(5) Special 2016, Pages: 134-136

are involved in modifying the use of this genetic information. Related to any binary data DNA strands are encoded as zeroes and ones. DNA strands are encoded with four bases which can be represented by letters A (Adenine), T (Thymine), C (Cytosine) and G (Guanine)[6]. The information in DNA strands are stored as a code made up with these four different chemical bases. The double helical structure of DNA molecule is shown in the Fig.1.The bases (nucleotides) are spaced every 0.34 nanometers along the DNA molecule, can give a remarkable data density approaches 18Mbits per inch. These nucleotides always come together in pairs such a way that A pair with T and C always pair with G.

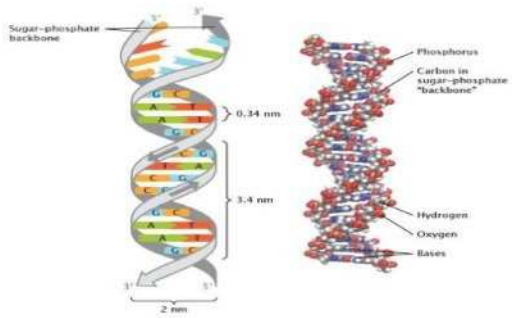

Fig. 1: Double Helical Structure of DNA

DNA cryptography is a latest promising area in cryptography research that has emerged with the evolution of DNA computing (Sanjeev Dhawan, Alisha Saini, 2012). DNA can be used for storing, transmitting information and performing computation. The extensive parallelism and extraordinary information (Kritika Gupta, Shailendra Singh) density inbuilt in this molecule can be exploited for cryptographic process. Several DNA based algorithms has been proposed and implemented for encryption, authentication etc. This paper, the research conducted by a number of authors related to this discipline of DNA Cryptography is considered (Anu Priya Agarwal, Praveen Kanth, 2014).

Proposedalgorithm:

Proposed algorithm explains a novel encryption algorithm based on random key generation of DNA pattern (Bonny B Raj, V. Panchami, 2014). So far there are different concepts that evolved for encryption of information using traditional mathematical operations and/or data manipulating DNA molecules. Whenever an encryption algorithm has been implemented and transmitted via the transmission media, there are possibilities for data attacks and modifications by eavesdropper. To avoid this check the data thoroughly for any kind of manipulation at the receiver's end.

A. Steps For The Encryption:

Step 1: The binary data, text, string or image is used under the form of ASCII code (in decimal format) (Sanjeev Dhawan, Alisha Saini, 2012).

Step 2: These numbers are then grouped in blocks for encryption

Step 3: Convert Encoded message to binary format.

Step 4: These digits are grouped into two and substituted as A for 00, T for 01, G for 10, and C for 11.

Step 5: Message is ready for encryption

B. Random Key Generation:

Random key is generated for further encryption, which is a combination of ACTG and it is assigned in random for extended ASCII characters. This Public Key is exchanged between the sender and receiver for further encryption and decryption process.

1. Program For Random Key Generation:

Algorithm*:* Random Combination of a given database

{"A","C","T","G"}

Step 1: Assign a database with 4 initial characters as strings in a string array *database*.

{"A","C","T","G"}

Step 2: With all items in the database make possible combination of items, each time, with increasing *the length of every item* to be stored in the result string array, using ***getAllLists*** algorithm, until the length of each item becomes 4(i.e., length of the given database.)

Step 3: Copy the result string array in an array list named, *combinationLists,* for easy pick of a random string combination.

Step 4: Pick out a random string using *get()* method by selecting a random number index using ***getRandomNumber*** algorithm.

Step 5: Print the random string which is been picked out.

1.1 Algorithm:

getAllLists, which takes elements string array and length of each item in the array.

Step 1: Allocate memory for *allLists* String array to store all possible combination of the database elements and the substring list.

Step 2: If, for this time, *the length of an item* in the elements array is 1, (i.e., if the elements are single character strings), then return elements array. Else do step 3.

Step 3: G*et a*ll lists with items length 3, 2 and 1, in *allSubLists* by recursively invoking ***getAllLists*** algorithm each time decreasing the length of an item, until it becomes 1.

Step 4: Concatenate each element in the *element* array with each item in the *allSubLists* array, and store as *allLists*.

Step 5: Return the combination of items as *allLists*.

1.2 Algorithm:

getRandomNumber

Step 1: Generate an integer number for index, subjecting Math.random() under a simple math calculation.

Step 2: Return the resulting integer

C. Steps For Decryption:

Step 1: Read sequence of encrypted message(DNA Format).

Step 2: Convert DNA to Binary Sequence.

Step 3: Convert Binary Sequence to ASCII (in Decimal Format)

Step 4: Convert ASCII to binary data, text or image .

Mplementation:

Hardware and Software Requirements

Languages Used: JAVA Platform: Windows 7

Future Scope And Conclusion:

In this system, we use DNA based encryption systems which deals with plaintext. The proposed method of encoding is far better and faster than conventional cryptography like DES and other DNA based encryption algorithms. The proposal can be further enhanced to include in security mechanism of wireless networks and analyzing its performance to basic cryptanalytic attacks and comparing it with existing cryptosystems to know exactly how much improvement is achieved.

REFERENCES

Anu Priya Agarwal, Praveen Kanth, 2014.“Secure Data Transmission using DNA Encryption” Computer Engineering and Intelligent Systems, 5: 51-59.

Bonny B Raj, V. Panchami, 2014. “ DNA Based Cryptography Using Permutation and Random Key Generation Method” International Journal of Innovative Research in Science, Engineering and Technology, 3: 263-267.

Camelia, Mihaela Pintea, 2014. “Advances in Bio- inspired Computing for Combinatorial Optimization Problems Intelligent Systems” Reference Library, 57: 21-28.

Kritika Gupta, Shailendra Singh, International Journal of Advanced Research in Computer Science & Software Engineering, 3(3): 36-42.

Sireesha, K., V. Srujana, 2013. “An overview and Analysis of Private & Public Key”, International Journal of Technological Exploration & Learning, pp: 281-283.

Sanjeev Dhawan, Alisha Saini, 2012. “Secure Data Transmission Techniques Based on DNA Cryptography”, International Journal of Emerging Technologies in Computational and Applied Sciences, 2: 95-100.

Priyadharshini, V., P., Divya, D. Preethi, N. Pazhaniraja, P. Victer Paul, 2015. “Bio- inspired Algorithm based Web servicesOptimization – A Survey”. 10: 13231-13242.