International Journal of Computer Networks and Communications Security

VOL. 6, NO. 9, SEPTEMBER 2018, 196–200
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

A Review of DNA-Based Block Cipher

Chng Chern Wei[1], Sharifah Md. Yasin[2], Mohd. Taufik Abdullah[3] and Nur Izura Udzir[4]

[1, 2, 3, 4] Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 UPM, Serdang, Selangor, Malaysia

[1]cwchng2u@yahoo.com.my, [2]ifah@upm.edu.my, [3]taufik@upm.edu.my, [4]izura@upm.edu.my

ABSTRACT

Nowadays, e-commerce growing rapidly such as online banking, government affairs through online and business transactions over the internet has become a popular trend and is considered important aspect for society of life in the world. Security in the world of communication through the network is an important aspect of the content in the communication that can be kept confidential for both senders and receivers. To counteract the advantages and the weaknesses of DNA-Based cryptographic, we are to discuss and provide a thorough description of the cryptography algorithm of DNA-Based cryptographic, the uniqueness of the algorithm, the safety of algorithms and also a review of analysis on the performance of DNA-based algorithms with DNA characteristics.

Keywords: *Cryptography, Security, Block Cipher, DNA, DNA-Based.*

1 INTRODUCTION

The growing development of computer systems and interconnection between computer worlds through computer networks such as the internet has led to the satisfying comfort of communication in sharing information.

To reinforce the beliefs of societies on the effectiveness of online transactions, security in the network should be considered. Therefore, the security of current data in network communication should be emphasized [15].

Variety of techniques and network security algorithms have been widely used to maintain current transaction content in network communication, examples of cryptographic algorithms such as DES, 3DES, Blowfish and AES. From the algorithms listed above, it is arguably as a traditional algorithm of cryptography. Now DNA-based algorithms are increasing rapidly and have proven that these DNA sequences techniques succeed in producing high-confidence cryptographic algorithms [5][6][7][8][9][10][11][12].

Due to the rapidly development of DNA-based cryptography, it is an emerging instinctive cryptographic field and is increasingly popular among researchers in network computing security research primarily using DNA sequences.

All DNA-based cryptography algorithms have satisfactory the network security limitations because the algorithm design using DNA characteristics cryptography techniques to provide the strength of the encrypting and decrypting messages and able to provide randomness results when the cryptographic algorithms is tested via NIST 15 Test Suite and proved to be appropriate in a digital computing arena [5][6][7][8][9][10][11][12].

1.1 DNA Background

DNA Deoxyribonucleic acid or DNA is a type of biological molecule known as nucleic acids. It is formed from 5-carbon deoxyribose sugar, phosphate, and nitrogenous base. However, the Double-stranded DNA consists of two spiral nucleic acid chains that are twisted into double helix structure [14]. This Double Helix structure is rotating and allows DNA to become denser. In order to allow DNA to be loaded inside the nucleus, DNA is wrapped in a coiled structure called chromatin. Chromatin tends to form chromosomes during the process of cell division. Before DNA replication, loose chromatin provided access to cell replication machinery to DNA strands [1][2].

DNA is stored as a code made up of four chemical bases [2], known as DNA Double-Helix Structure [1][2][3]. The four chemical bases of DNA are Adenine (A), Guanine (G), Cytosine (C), and Thymine (T). Figure 1 and Figure 2 show the

DNA structure and DNA Double-Helix structure [14], respectively.

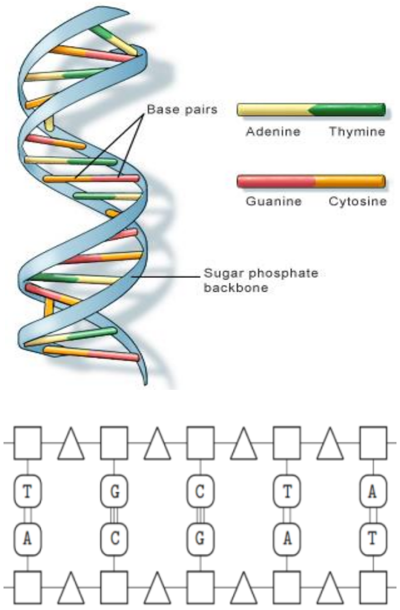

Fig.2. DNA Double – Helix Structure [15]

2 DNA REPLICATION

DNA must be copied when DNA cells are divided. This cell division process is known as Replication. This process occurs during Interphase.

The Double Helix is untwisted and the antiparallel unzipped strands. The Hydrogen bonds between the bases are broken. The floating nucleotides will combine with exposed Nitrogenous Bases, and then they will form hydrogen bonds - this part of the 'reason' for Complementary Base Pairing. New nucleotides are tied together with enzyme DNA polymerase, which form complete strands contrary to the original strands. This will produce two new DNA molecules that form Double Helices.

3 DNA SECURITY IN COMPUTING

Based on opinions from Y.Zhang, L.He & B.Fu (2012) that in general do not have the arbitrariness and connection between the relationship between cryptography and DNA sequences, but with the in-depth study of the latest modern biotechnology and DNA computing, these two disciplines are increasingly popularly reviewed by researchers [14].

Tausif Anwar al. et. (2014) in his paper mentions, that Cryptography uses DNA methods to encrypt messages in communication to deliver high security level on the network. DNA cryptography is capable of hiding data and information; hidden data and information can only be recognized by both senders and recipients by using the same key. DNA computing is proven to solve many problems not only in cryptography and cryptanalysis and even steganography. Data encryption and information based on DNA sequences seems to have been a high-tech technique to meet current information security standards [13].

4 LIMITATION OF DNA SECURITY IN COMPUTING

According to Mohammadreza & Nazanin (2015), discussed his paper mentions that the mutation of DNA in DNA is look difficult to implementation in the actual DNA system [17].

However, H. A. Auday al. et. (2015), emphasized in his review paper that, DNA cryptography contained some limitations as he discussed in the real dissemination of DNA that DNA is required high-tech equipment and manpower and it may involve huge funds and time constraint for the implementation [11].

N.H.UbaidurRahmana, C. Balamuruganb & R. Mariappanc (2015), in their paper discussed that, some of the algorithms found in DNA Cryptography have many disadvantages because the algorithm is designed by modular arithmetic cryptography with a simple step or the algorithm is based on an unsuitable biological concept in a digital computing world [18].

From the perspective of K.Kainth & G.Singh (2015), Cryptography of DNA brings many advantages in producing safe applications and provides high security for information security coupled with products produced using traditional cryptographic techniques. Despite its advantages, this DNA cryptography also has some issues such as the design and implementation of the DNA approach in the computer world is quite difficult and complicated compared to traditional cryptographic techniques [16].

5 CATEGORIES OF DNA CRYPTOGRAPHY

DNA cryptography is a new field of cryptography research, and it is one of the fastest growing technologies in the DNA computing concept. With this latest technique, the cryptography method able to encrypted the data in communications by combining the biological structure of DNA with computing. However, the cryptography of DNA has grown rapidly; it has been divided into a number of types in methodology. Here, lets we discuss the types of methodology for the cryptography of the DNA [19][20][21].

5.1 *Molecular bio*

The Bio molecular structure exists in all living microorganisms in the world including humans. Benefits of the living organisms in the world have a unique DNA molecule to store information about the characteristics of the living organisms so that they are different from other organisms. The extensive bio-molecular structure used as popular cryptography techniques is like polymerase chain reaction, DNA hybridization, DNA fabrication, DNA fragmentation technique. The technique of bio-molecular structure can be applied to encrypt and decrypt messages in enhancing security in the world of network communication.

5.2 *One Time Pad (OTP)*

Vernam is a computer science researcher who introduces OTP. OTP generates keys randomly, which are used in encryption and decryption processes. After that, the technique was expanded by Shanon. Shanon explains that the key size affects the output of ciphertext and the size of the keys should be greater or equal to plaintext. An importance attributes for the key must in unique and the keys cannot be reused in encryption.

5.3 *DNA chip technology*

DNA chip technology is a method for identifying independent biological samples. This technique is difficult because it to be use a microscopic DNA array technology on solid surfaces to study biochemical samples.

DNA chip microarray can produce a positive impression with array molecules by using high density. As a result of DNA chip microarray able to provide two levels of security for other biotechnology limitations for security in computing.

5.4 *DNA Fragmentations*

The concept of DNA fragmentation for the first time was represented by Williamson in 1970. Notice that he found the fragment began at the beginning of a cell death. In that process, DNA fragmentation breaks the DNA strand into smaller pieces. Therefore, the DNA can be extended the goodness of characteristic to the next generation to get inherited.

5.5 *Polymerase chain reaction (PCR)*

Polymerase chain reaction (PCR) is a rapidly strengthening DNA technology. Due to the difficulty in manning a small number of DNA, the amplification procedure was introduced. The PCR has a high strengthening efficiency, therefore it is appropriate to be applied to strengthen and convert of DNA. In DNA amplification using the PCR method, the DNA segment should be cloned into vectors.

6 LITERATURE WORK OF DNA CRYPTOGRAPHY

Guangzhao Cui et al. (2008), proposed an asymmetri key for encryption scheme using DNA Technology. In this paper, the authors discuss the DNA synthesis process, DNA digital conversion and PCR replication. Based on the research, the findings able to provide high degree on protecting message by provide a double security protection for the cryptosystem [5]. However, this cryptosystem only depend on the single keys which is not enough to provide the security for the big data.

Lai Xuejia et al. in 2010, had proposed DNA public key cryptographic methods. This method is an asymmetric encryption and signature cryptosystem. DNA code used to perform an encryption and DNA signature [12].

Deepak Kumar et al. (2011), discussed their research work for encrypting data using DNA sequences. This cryptosystem is based on the symmetric key in One Time Pad DNA methodologies. The advantages of the cryptosystem are able to reduce the (deficiencies) weak key for the cryptosystem [6]. However, this cryptosystem is only dependence on the key to provide security.

Yunpeng Zhang et al. (2012), present their work in IEEE International Conference with highlighted a DNA Fragmentation method on DNA Cryptography. This methodology is based on symmetric key cryptosystem and able to generated shortest secure ciphertext [7]. However, these advantages also become it disadvantages because the shortest of DNA fragmentation length might containing risk of attack in the short time.

Qing Zhang, Ling Guo & Xiaopeng Wei (2013), introduced a novel image fusion cryptosystem based on DNA sequence operation. According to Qiang, the proposed algorithm able to generated an pseudo-random sequence and it results the ciphertext is difficult to be analysed and attacks. The advantages of this algorithm are able to provide larger memory of secret keys and also capable to produced high degree of sensitive secret keys. With this characteristic of this algorithm are able to gain various attacks. However, this algorithm is only suitable for image encryption and not suitable for big data encryption [8].

Fatma et al. (2014), discussed a new symmetric key-based DNA cryptographic algorithm with DNA properties and coding of amino acids. This technique improves the safety level of the classic OTP method [9].

Noorul Hussain et al. (2015), has proposed a DNA-based encryption and decryption techniques. The advantages of this technique is the Plaintext will divided into two block with the same block size and encode it into DNA sequences using the unique generation of DNA coding for each session to produce a secure cipher codes [10].

Auday Al-Wattar et al. (2015), has proposed a DNA-based Advanced Encryption Standard (AES). In this paper highlighted that, the DNA-based S-Box designed according to the Biology DNA techniques. This is suitable to applying in symmetric key block cipher. The advantages of the DNA-based cryptosystem are able to provide high degree of security protection gain attacks [11]. However, this algorithm might consist of risk of attacks. This is because the method of constructing of S-box is simple and no mathematical approach is involved. Therefore, the attack of this algorithm might use only a short time. This algorithm can be improve by apply mathematical approach in enhance the strength of the algorithm.

7 CONCLUSION

The development of computing cryptographic algorithm using DNA Biochemistry techniques has paved the direction for cryptographic researchers to suppress the DNA aspects in creating a sophisticated computing network security algorithm.

The development of cryptographic computing using DNA-based sequences techniques has paved the way for cryptographic researchers to suppress DNA aspects in creating a sophisticated computing network security algorithm.

DNA with these properties and features can ensure good cryptographic factors for an application in computing.

Therefore, DNA-based sequence is ideally applicable in the world of cryptography to design and create computing security algorithms with a variety of purposes such as network security, image and Information encryption and decryption to meet objectivity of information confidentiality and data privacy.

As the results, DNA-based cryptography can overcome a wide range of traditional cryptographic weaknesses and can also give a high degree of confidence to the encryption result in making data and information secure.

8 ACKNOWLEDGMENT

We would like to special thanks to Ministry of Higher Education of Malaysia to support this work. (No.: FRGS 08-01-15-1717FR, Vote No.: 5524822).

9 REFERENCES

[1] S. M. Metev and V. P. Veiko, Laser Assisted Microtechnology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[2] J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[3] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, “A novel ultrathin elevated channel low-temperature poly-Si TFT,” IEEE Electron Device Lett., vol. 20, pp. 569–571, Nov. 1999

[4] M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, “High resolution fiber distributed measurements with coherent OFDR,” in Proc. ECOC’00, 2000, paper 11.3.4, p. 109.

[5] Cui, Guangzhao, Liming Qin, Yanfeng Wang, and Xuncai Zhang, "An encryption scheme using DNA technology," In Bio-Inspired Computing: Theories and Applications, IEEE International Conference on, pp. 37-42, (2008).

[6] Deepak Kumar, and Shailendra Singh, "Secret data writing using DNA sequences," In Emerging Trends in Networks and Computer Communications (ETNCC), IEEE International Conference on, pp. 402-40, (2011).

[7] Yunpeng Zhang, Bochen Fu, and Xianwei Zhang, "DNA cryptography based on DNA Fragment assembly," In Information Science and Digital Content Technology (ICIDT), IEEE International Conference on, vol. 1, pp. 179-182, (2012)

[8] Q. Zhang, L. Guo, and X. Wei, "A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system," Optik-International Journal for Light and Electron Optics, 2013.

[9] Fatma E. Ibrahim, M. I. Moussa and H. M. Abdalkader, “A Symmetric Encryption Algorithm based on DNA Computing”, International Journal of Computer Applications (0975 – 8887) Volume 97– No.16, pp. 41-45, July 2014.

[10] Noorul Hussain Ubaidur Rahman, Chithralekha Balamurugan, and Rajapandian Mariappan, “A

Novel DNA Computing based Encryption and Decryption Algorithm?, Procedia Computer Science 46 pp. 463 – 475, 2015.

[11] A. H. Al-Wattar, R. Mahmod, Z. A. Zukarnain, and N. I. Udzir, "Generating A New S-Box Inspired byBiological DNA," International Journal of Computer Science and Application vol. 4, p. 10, April -2015 2015.

[12] X.J.Lai, M.X.Lu, L.Qin, J.S.Han & X.W.Fang, "Asymmetric encryption and signature method with DNA technology", Science China: Information Sciences, Vol.53(3), March 2010

[13] A.Tausif, P.Sanchita & K.S.Shailendra, "Message Transmission Based on DNA Cryptography: Review", International Journal of Bio-Science and Bio-Technology, Vol.6(5), 2014, pp.215-222

[14] Y.Zhang & L.H.B.Fu, "Research on DNA Cryptography", Intech: Applied Cryptography and Network Security, 2012

[15] C.W.Chng, “DNA approach for password conversion generator,” IEEE, 2014

[16] K.Kamaljit & S.Gurpreet, "A Review to an invincible cryptographic approach: DNA Cryptography", Internation Journal of Advanced Research in Computer Communication Engineering, Vol.4(1), Jan 2015.

[17] M. Najaftorkaman & N.S.Kazazi, "A Method to Encrypt Information with DNA-Based Cryptography",International Journal of Cyber-Security and Digital Forensics, Vol.4(3), 2015.

[18] N.H.UbaidurRahman, C.Balamurugan & R. Mariappan, "A Novel DNA Computing Based Encryption and Decryption Algorithm", Procedia Computer Science, Vol.46, 2015

[19] A.Tausif, K.Abhishek & P.Sanchita, "DNA Cryptography Based on Symmetric Key Exchange",International Journal of Engineering and Technology (IJET), 2015.

[20] M.Ritu & K.Praveen, "A Review Paper of DNA Based Cryptographic", National Conference on Innovative Trends in Computer Science Engineering: Proceedings, 2015.

[21] Manisha & A.Pooja, "A Survey on DNA Based Cryptography", International Journal of Scientific Engineering and Research, Vol.3(4), April 2015.