*IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*
*e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 5, Ver. II (Sep - Oct .2015), PP 14-18*
*www.iosrjournals.org*

# A Survey on DNA Based Cryptography using Differential Encryption and Decryption Algorithm

[1]Hariram S, [2]Dhamodharan R
*[1,2]Department of Electronics and Communication engineering Sree Krishna College of Engineering Vellore, Tamilnadu*

***Abstract:*** *As modern encryption algorithms are bust to attacks, the world of information security give the impression of being in new directions to protect the data transmission. The concept of using DNA computing in the fields of cryptography and steganography has been identified as a possible technology that may bring forward a new anticipation for unbreakable algorithms. Nowadays Government agencies and the semiconductor industries have raised serious concerns about malicious modifications to the integratedcircuits.The added functionality known as hardware Trojan. DNA cryptography is a new field of cryptography which gives a new hope to detect and overcome the Trojan. This paper gives an overview of cryptography, DNA cryptography and how it's helpful to rectify the Trojan effect.*
***Keywords: Trojan****, DNA, DNA based cryptography, DNA digital coding*

## I. Introduction

### 1.1 Cryptography:

The major role of cryptography is to secure the data from any attackers. It has two main terms-plain text and cipher text. The original message which has been passed by the user is known as plain text and after added the key with the original message that text is called as cipher text. Encryption techniques are classified as symmetric and asymmetric key encryption techniques. In symmetric key cryptography common key can be used for both transmitter and receiver side. Some of the symmetric key cryptography algorithms are AES, DES and 3DES. In asymmetric key cryptography the public key of the user1 used in transmitter side and the private key of the user2 was used in receiver side. Some of the asymmetric key cryptography algorithms are RSA, Diffie-hellman, ECC, Digital signature algorithm. Compare with DES, AES has effective in both software and hardware. With minimum number of rounds AES encrypts the message with the key length of 128-bits, 192bits, 256-bits.The comparison of symmetric key algorithms are shown below:

**Table 1.Comparison Of Symmetric Key Algorithms [1]**

| METHOD | DES | 3DES | AES |
|---|---|---|---|
| Developed By | IBM and US government | IBM | National Institute of Standard and Technology (NIST) |
| Structure Algorithm | Fiestel network | Fiestel network | Substitution and Permutation method |
| Key Network | 56bit | Three 64 bit keys with overall key length of 192 bit | 128 bit<br>192 bit<br>256 bit |
| Block size | 64 | 64 | 128 |
| No.of rows | 16 | 48 | 9 |
| Vulnerability | Brute force attack | Some theoretical call attack | Side channel attack |
| Efficiency | Slow | Relatively slow in software | software and hardware |

The comparison of asymmetric key cryptography algorithms are shown below:

**Table 2: Comparison Of Asymmetric Key Algorithm**

| **METHOD** | **RSA** |
|---|---|
| FEATURE | Both encryption and decryption used the following equation: $C=M^e \bmod(n)$ $M=C^d \bmod(n)$ C=>cipher block C M=>PlaintextblockM[2] |
| ADVANTAGES | 1.Reverse process of e is difficult 2.Difficult to produce private key & modulus from public key |
| DISADVANTAGES | 1.Quite slow 2.Key generation is complex 3.Large number factorization is difficult |
| **METHOD** | **DIFFIE-HELLMAN** |
| FEATURE | Secret key sharing is used for both encryption and decryption |
| ADVANTAGE | Short length key(256bit) so it is fast |
| DISADVANTAGE | Man-in-the-middle attack |
| **METHOD** | **ECC(Elliptical Curve Cryptography)** |
| FEATURE | Compute the key through elliptical curve equation |
| ADVANTAGES | 1.Utilize less power 2.Using 164bit key for better security |
| DISADVANTAGE | Difficult to implement compare with RSA |
| **METHOD** | **DSA(Digital Signature Algorithm)** |
| FEATURE | It consists of a pair of large numbers computed based on some algorithm to authenticated algorithm[3] |
| ADVANTAGES | 1.Very fast 2.Secures the data from man-in-the-middle attack 3.Provide non-reputation and authentication |
| DISADVANTAGE | It has short life span |

**1.1.Trojan:**

A Trojan in computing is generally a malware program contains malicious code. It act as a backdoor which contains the controller, it gives a remote access to a hacker for unauthorized access in a particular computer. Some types of Trojan takevulnerability in older version of internet explorer and Google chrome to use the host computer as an anonymizer. To detect and secure the data from Trojan, blended threat, DNA cryptography gives a forward step towards it.

**1.2. DNA**

Before delving into the principles of DNA computing, we must have a basic understanding of what DNA actually is. All organisms on this planet are made of the same type of genetic blueprint which bind us together. The way in which that blueprint is coded is the deciding factor as to whether you will be bald, have a bulbous nose, male, female or even whether you will be a human or an oak tree. Within the cells of any organism is a substance called Deoxyribonucleic Acid (DNA) which is a double-stranded helix of nucleotides which carries the genetic information of a cell. This information is the code used within cells to form proteins and is the building block upon which life is formed.

DNA is abbreviated as Deoxyribo Nucleic Acid. Every cell in human body has a complete set of DNA [4].DNA is made of chemical building blocks called nucleotides. These building blocks are made of three parts: phosphate group, sugar group, nitrogen bases. To form a strand of DNA, nucleotides are linked into chains with the phosphate and sugar group alternating. Nitrogen bases are Adenine, Thymine, Cytosine, and Guanine.Nitrogenbasesare very important to the human body activity.

**Basics and Origins of DNA Computing:**

DNA computing or molecular computing are terms used to describe utilizing the inherent combinational properties of DNA for massively parallel computation. The idea is that with an appropriate setup and enough DNA, one can potentially solve huge mathematical problems by parallel search.Utilizing DNA for this type of computation can be much faster than utilizing a conventional computer, for which massive parallelism would require large amounts of hardware, not simply more DNA.

Leonard Adleman, a computer scientist at the University of Southern California was the first to pose the theory that the makeup of DNA In early 1994, he put his theory of DNA computing to the test on a problem called the Hamiltonian Path problem or sometimes referred to as the Traveling Salesman Problem. The 'salesman' in this problem has a map of several cities that he must visit to sell his wares where these cities have only one-way streets between some but not all of them. The crux of the problem is that the salesman must find a route to travel that passes through each city (A through G) exactly once, with a designated beginning and end.

## II. DNA Computing

DNA computing is also known as molecular computing. Compare with quantum cryptography, DNA cryptography is suitable for higher data storage in compact manner. It is mainly gives a solution to NP-complete problem and conventional problems of cryptosystems. Adleman introduced the DNA computing in 1994 to make the bridge between DNA molecule and computer. He analysed that DNA computing is faster than electronic circuit. By using DNA computing he solved the Hamilton path problem [5] then Lipton extended the work of Adleman and investigated the solution of NP-complete problem and he finds the new opportunities of DNA computing [6]. Boneh found an approach of DNA cryptography and he break the DES in 1995 [7]. In 1999, C.T.Chelland proposed a new method by combining steganography with DNA to hide secret message encoded as DNA strands [8]. In 2000, Prof.Gehani designed an encryption method using one-time pad and substitution method [9]. Andre Lier developed an two different approach-first approach is to hid the information and second approach is to design molecular checksum [10]. In 20003, Jie chen proposed carbon nano-tube based message transformation and DNA-based cryptosystem [11]. Lumingxin designed a symmetric key cryptosystem using DNA biotechnology and microarray [12]. Zheng zhang proposed a technique to encrypt the information using bio molecular automaton [13]. Xingwang approach an new encryption scheme by using DNA computing and traditional cryptography and RSA algorithm [14]. G.cui used the technologies of DNA synthesis, PCR amplification, DNA digital coding and traditional cryptography to design a new encryption scheme [15]. LAI Xuejia designed an asymmetric encryption method and signature cryptosystem by combining genetic engineering and cryptology [16]. In 2014 Deepak singh chouhan developed the new encryption scheme by combining molecular technique and RSA. Using this method they tested the efficiency and reliability of the system [17].

## III. Image Security Using Dna Sequence

The method to secure the data may not suite to secure the image. To secure the image using DNA sequence can performed based on Watson-crick rule. It describes that the nitrogen bases A (Adenine) pair with T (Thymine) and C (Cytosine) will pair with G (Guanine). Shujun Li.et al designed a highly secured image by combining other encryption techniques and they preferred the secret permutation techniques [18]. Mitra.A.et al approaches a random combinational image encryption technique using bit, pixel and block permutation [19].

Zhi-hong Guan et al [20] has found a new image encryption technique based on shuffling and confusion concept. Sinha A and singh k [21] used Fractional Fourier Transform and Jigsaw transform and they formed a new image encryption scheme. Maniccam S.S and Bourbakis NG [22] proposed image and video encryption based on permutation and substitution method. Permutation can be done using SCAN pattern and product ciphers can be iterated using substitution method. Then Ozturk I and Sogukpinar I [23] approach an new scheme by combining mirror-like image encryption and visual cryptography algorithms for better security. M.V and Benedett R[24] have proposed two encryption technique for image selective encryption and multiple selective encryption and they got stronger encryption with less correlation. Mohammad Ali Bani Younes [25] introduce a new image encryption technique by combining image permutation and the RijinDael algorithm.

Hiral rathod et al[26] introduce a new method to secure an image by combining permutation and Hyper Image Encryption Algorithm. The binary value block will get from original image and it can be rearranged using permutation process then they generate the cipher image. Rasul Enayatifar et al [27] proposed a new novel image encryption scheme based on DNA masking, genetic algorithm and logistic mapping and the resulting of this method have better masking technology. Ritu gupta et al [28] generates a secret key using DNA computation and molecular arithmetic operation. Then the secret key is used to encrypt the every pixel in the image. Qiang zhang [29] developed an image encryption by using permutation and diffusion process.

Permutation can be implemented using Hao's fractal sequence representation. In 2015 Saranya M R

[30] developed an enhanced image security by using chaotic sequence, DNA, genetic algorithm. By using this method it can produce high entropy with low correlation value of original image.

**Advantages:**

To Adleman, the following advantages of DNA computing became evident;

**Speed** - Conventional computers can perform approximately 100 MIPS (millions of instruction per second). Combining DNA strands as demonstrated by Adleman, made computations equivalent to $10^9$ or better, arguably over 100 times faster than the fastest computer. The inherent parallelism of DNA computing was staggering.

**Minimal Storage Requirements** - DNA stores memory at a density of about 1 bit per cubic nanometer where conventional storage media requires $10^{12}$ cubic nanometers to store 1 bit. In essence, mankinds collective knowledge could theoretically be stored in a small bucket of DNA solution.

**Minimal Power Requirements** - There is no power required for DNA computing while the computation is taking place. The chemical bonds that are the building blocks of DNA happen without any outside power source. There is no comparison to the power requirements of conventional computers.

## IV. Conclusion and Future Work:

The field of DNA computing is still in its difficult computation and the applications for this technology are still not fully understood. The world of information security is always on the pay attention for resilient encryption to protect the data that we transmit over non secured communication but it appears that every encryption technology meets its tendency as the computing technology of our world evolves. It appears we are involved in a inconsistency where the best encryption technology of the day is only as good as the computing power that it is tested upon and the practicality of its application. The attractiveness of these DNA research trends is found in the possibility of mankind's utilization of its very life building blocks to solve its most difficult problems. In any case, we will not be tossing out those PC's for test tubes of DNA anytime soon and the use of DNA computing with a greater security focus other than in merchandise authentication methods is a long way off.

## References:


[1] Sourabh Chandra,SK Safikul alam,Smita Paisa,Dr.(prof).Goutam Sanyal, "A Comparison survey of symmetric and asymmetric key cryptography",International conference on Electronics communication and computational Engineering(ICECCE)

[2] William stallings, "cryptography and network security principles and practise", 5th edition 2011

[3] searchsecurity.techtarget.com/definition/Digital-signature-standard

[4] Grasha Jacob,A.Murugan, "DNA based cryptography An overview & analysis", International Journal of emerging science 3(1),(36-42) march 2013

[5] L.Adleman, "Molecular computation of solutions to combinational problems",science, JSTOR,vol.266,1994,pp-1025-1025.

[6] R.J.Lipton "Using DNA to solve NP-complete problems",science vol.268 pp.542-545,1995

[7] D.Boneh,C.Dunworth and R.Lipton, "Breaking DES using a molecular computer", In proceeding of DIMACS workshop on DNA computing,1995,pp.37-65

[8] C.T.Celland,V.Risca and Bancroft C., "Hiding message in DNAmicrodots",Nature ,vol399,pp.533-534,1999

[9] A.Gehani,T.H.Labean and J.H.Reif, "DNA based cryptography-DNA based computers v.providence American Mathematical society,vol54,2000. pp.233-249

[10] A.Leier,C.Richter and W.Banzhaf, "cryptography with DNA binary strands",Biosystems,2000.pp-13-22

[11] J.Chen, "A DNA-based,biomolecular cryptography design",circuits and systems ISCAS apos,2003,pp.822-825.

[12] M.X.Lu, "Symmetric-key cryptosystem with DNA technology",science in china series information science,vol.3,2007,pp.327-333

[13] Zheng Zhang,Xiaolong shi,JieLiu,"A method to encrypt information with DNA computing",3rd international conference on bio-inspired computing.Theories and application 2008.pp.155-160

[14] Xing wang,Qiang zang "DNA computing based cryptography",Fourth international conference on bio-inspired computing BIC-TA2009 pp1-3.

[15] G.Cui,L.Cuiling,L.Haobin and L.Xiaoguang, "DNA computing and its application to information security field",IEEE 5th international conference in National computation,Tianjian china,Aug 2009,pp.148-152.

[16] L.Xuejia,L.Mingxin,Q.Lei,H.Junsong and F.Xinven, "Assymmetric encryption and signature method with DNA technology",science in china: Information Science,vol.53,2010,pp.506-514.

[17] Deepak singh chouhan,R.P.Mahajan, "An architectural framework for encryption and generation of digital signature using DNA cryptography",International Conference on Computing for Sustainable Global Development(INDIACom),2014.

[18] Li.Shujun,X.Zheng, "Cryptanalysis of a chaotic image encryption method",Inst.of image process.Xian Jiaotong univ,Shaanxi,This paper appears in:Circuits and systems ISCAS 2002.IEEE international symposium on publication Data:2002,vol.2.2002,pp.708-711

[19] A.Mitra,Y.V.Subba Rao and S.R.M.Prashna, "A new image encryption approach using combinational permutation techniques",Journal of computer science,vol.1,no.1,2006,p.127,http://www.enformatika.org

[20] G.Zhi-Hong,H.Pangjun and G.Wenjie, "Chaos-based image encryption algorithm",Department of Electrical and Computer Engineering, University of waterloo,ON N2l 3G1,Canada,published by:Elsevier,2005,pp.153-157

[21] A.Sinha,K.Singh, "Image encryption by using fractional fourier transform and Jigsaw transform in image bit planes",Source:optical engineering,spie-int society optical engineering vol.44,no.5,2005,pp.15-18

[22] S.S.Maniccam,N.G.Bairbakis, "Image and video encryption using SCAN patterns",Journalof pattern recognition society,vol.37,no.4,pp.725-737,2004

[23] Ozturk and I.Sogukpinar, "Analysis and comparison of image encryption algorithm",International Journal of Information technology,vol.1.no.2.pp.64-67 http://www.waset.org

[24] M.Van Drogenbroeck and R.Benedett, "Techniques for a selective encryption of uncompressed and compressed images",In ACIVS'02,Ghent,Belgum,Proceedings of advanced concepts for intelligent vision systems 2002
[25] Mohammad Ali Bani Younes,Aman Jantan, "An image encryption approach using a combination of permutation technique followed by encryption",IJCSNS International Journal of Computer Science and Network Security,vol.8.no4april.2008
[26] Hiral Rathod,Mahendra singh sisodia,Sanjay kumar sharma "Design and implementation of image encryption algorithm by using block based symmetric transformation algorithm (Hyper Image Encryption algorithm)", International Journal of Computer technology and Electronics Engineering(IJCTEE)vol.1,Issue3
[27] Rasul Enayatifar,Abdul Hana Abdullah,Ismail Fauzi Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence",optis and Laser in engineering 56(2014)83-93
[28] Ritu gupta,Anchal Jain,"A new image encryption algorithm based on DNA approach",International Journal of computer application vol.85-no.18.jan2014
[29] Qiang zhang,Shihua zhou,Xiaopeng wei, "An efficient approach for DNA fractal-based image encryption", Internation Journal of applied Mathematics and informatics and information sciences 2011
[30] Saranya M R,Arun K Mohan, K Anusudha, "Algorithm for enhanced image security using DNA and genetic algorithm", International conference on Signal processing, Informatics, Communication and Energy systems(SPICES),2015.