International Journal of Current Research and Modern Education (IJCRME)
ISSN (Online): 2455 – 5428 & Impact Factor: 3.165
Special Issue, NCFTCCPS - 2016

DNA BASED ENCRYPTION AND DECRYPTION USING FPGA

A. Kamaraj*, A. P. Bhrintha & M. Bhavithara****
* Assistant Professor, Department of ECE, Mepco Schlenk Engineering College, Sivakasi, Tamilnadu
** UG Scholar, Department of ECE, Mepco Schlenk Engineering College, Sivakasi, Tamilnadu

Abstract:

In today's world, Information Security is very fundamental and significant issues of data transmission. Hypersensitive data such as financial transactions, medical and personal records is transmitted through public communication facilities. The security of the hypersensitive information poses a great threat by an unauthorized recipient. Cryptographic techniques help in ensuring the security of such hypersensitive information [5]. Advancement in technology is occurring daily in order to find a new cryptographic algorithm. DNA Cryptography is a new inherent cryptographic field that has emerged from the experimentation of DNA computing. It is a data carrier for transferring message from sender to receiver. For secure transmission and reception, it is not only to encrypt message but also necessary to hide encrypted message [1]. Hidden message is known only to sender and receiver. DNA cryptography is used to solve conflicts in cryptography .DNA sequences based data encryption seems to be an assuring technique for fulfilling the current information security needs.

Key Words: Security, Hypersensitive Information, DNA Cryptography, DNA Computing & Cryptanalysis

1. Introduction:

In Network security, a threat is a possible danger that might exploit a hype sensitivity to breach security and therefore cause possible loss [2]. A threat can be either willfully. (i.e. hacking: an individual cracker) or accidental (i.e. due to computer malfunctioning, due to a natural disaster such as an earthquake , a fire , or a tornado) , due to loss of important services (electrical power , telecommunication, air conditioning) , compromise of information (eavesdropping , test of media , retrieval of discarded materials) , technical failures (equipment , software , capacity saturation) , compromise of function (error in use , abuse of rights , denial of actions).

The result can potentially compromise the confidentiality, originality or availability properties of resources (potentially different that the vulnerable one) of the organization and others involved persons (customers, suppliers) [6]. The so-called CIA (Confidentiality, Integrity, and Availability) is the basis of security [8].The attack can be active when it attempts to change the system resources or changes their operation and it reduces the Availability or Integrity. The attack can be passive attempts to learn or make use of data from the system but does not harm system resources: so it compromises Confidentiality. There are lots of cryptanalytic attacks, and they can be classified in several ways. A common variation turns on what Eve (an attacker) knows and available capabilities. In ciphertext-only attack, Eve can access only to the ciphertext (good recent cryptosystems are usually effectively resistant to ciphertext-only attacks). In a known-plaintext attack, Eve can access both the plaintext and ciphertext. Eve can choose a plaintext and learn its corresponding ciphertext in chosen-plaintext attack which is used by the British at the time of WWII. In a chosen-ciphertext attack, Eve can choose ciphertexts and learn their corresponding plaintexts. Finally in a man-in-the-middle attack Eve tries to get in between the sender

and the recipient, reads the message and modifies the traffic and then forwards it to the recipient.

The word cryptography is a Greek word which is a "secret way of writing" and is the art of hiding meaning. In the modern generation, cryptography deals with confidentiality in message by encryption which means conversion of messages from a readable into a non-readable one and back again at the other end, making it unreadable by intruders or eavesdroppers [4]. Encryption tries to ensure secrecy and confidentiality in communications. In recent decades, the field of cryptography has expanded beyond confidentiality concerns to include methods for message integrity checking, transmitter / receiver identity authentication, digital signatures, interactive proofs and secure computation. In conventional information security theory and cryptography, the information given is always checked or can undergo deggradations easily as there is no safety [3]. A security system uses 2 main blocks which is encryption and decryption. Encryption is basically protecting information, i.e. readable data is transferred into unreadable data in order to ensure confidentiality and also keeps the information safe. The reverse process of encryption i.e, Decryption, uses the cipher text and transforms it into understandable form. A key is transmitted between encryption and decryption system which provides a secure channel for communicating information. In neoteric years, much experimentation work has been done on DNA based encryption schemes. Most of them use organic properties of DNA sequences. Experts in cryptography have worked on DNA cryptography to clear up common limitations to make a system which is resistant to popular attacks.

1.1 Block Diagram:

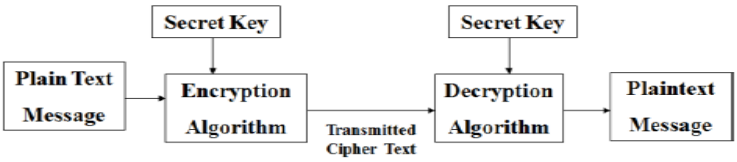

Figure 1: Block diagram of cryptography system.

The plain-text is encrypted with the help of secret key to a cipher-text at the sender is called as Encryption.[9]The Cipher text is transferred from the sender to the receiver through the channel. The cipher-text is decrypted with the help of the same secret key to obtain the input plain-text at the receiver which is shown in Fig.1.

1.2 DNA:

A DNA sequence is a sequence which consists of four alphabets: A, C, G and T [7]. It stands for Deoxyribo Nucleic Acid. DNA represents the genetic blueprint of living creatures. The structure of DNA is shown in Fig. 2

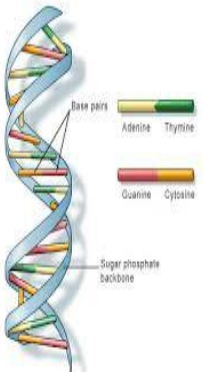

Figure 2: Structure of DNA

DNA contains “instructions” for assembling cells. Each and Every cell in the body of human has a complete set of DNA [13]. It is unique for every individual. The monomer units of it are nucleotides, and the polymer is known as a "polynucleotide". Every nucleotide has a 5-carbon sugar (de-oxyribose), nitrogen which includes a base attached to the sugar, and a phosphate group. Every nucleotide consists of three basic units: de-oxyribose sugar, phosphate group and a nitrogenous base. The nitrogenous base is of two types: purins (Adenine and Guanine) and pyrimidins (Cytosine and Thymine).

Figure 3: Four Nitrogen Bases

2. Proposed Methodology:

Proposed method is a new cryptography algorithm based on DNA computing technique .It comprises of two stages: Encryption and Decryption. Encryption converts the data to cipher text at the sender whereas the Decryption converts the cipher text back to the data at the receiver.

2.1 Encryption:

The process Encryption includes the following steps.

Step 1:

The input message is in the form of normal text. It is given to the FPGA through PS 2 keyboard. The PS 2 keyboard is interfaced with FPGA Spartan 6. The message which is given through keyboard is read by FPGA as ASCII codes. It is converted into Triplet code (codon) with the help of the codon table shown in Table.1.

Table 1: DNA code set

A=CGA	K=AAG	U=CTG
B=CCA	L=TGC	V=CCT
C=GTT	M=TCC	W=CCG
D=TTG	N=TCT	X=CTA
E=GGC	O=GGA	Y=AAA
F=GGT	P=GTG	Z=CTT
G=TTT	Q=AAC	=ATA
H=CGC	R=TCA	,=GAT
I=ATG	S=ACG	.=GAT
J-AGT	T=TTC	;=GCT

Step 2:

In this step, the codon is encrypted with key using vignere cipher, the most advanced encryption algorithm. The row of the following table is considered as key and the column as the codon in Table.2. The Algorithm is shown in Fig.6

Table 2: DNA Vigenere table

	A	T	C	G
A	A	T	C	G
T	T	C	G	A
C	G	C	A	T
G	G	A	T	C

2.2 Algorithm of Encryption:

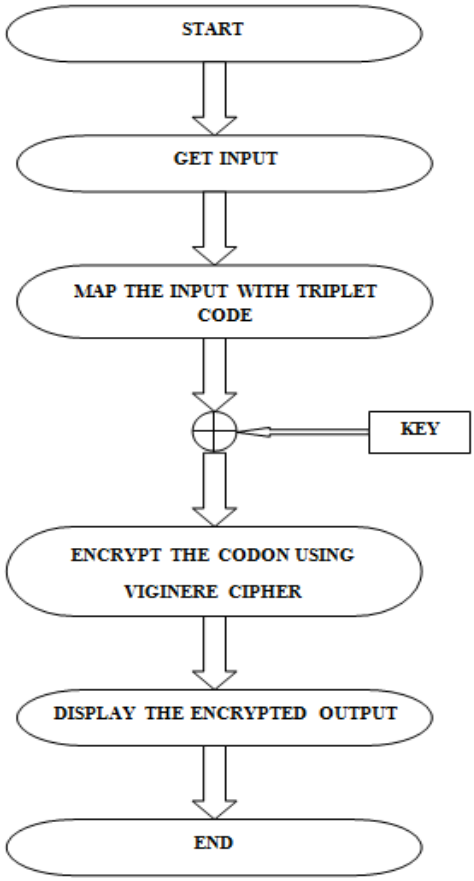

Figure 6: Proposed Flowchart for Encryption

2.3 Decryption:

The process Decryption includes the following steps.

Step 1:

The receiver gets the cipher text from the sender .It decrypts the cipher text by inverse mapping of key and cipher with codon with the help of vignere mapping table. As a result, the codon is obtained which is equivalent to the codon of sender side.

Step 2:

The codon is converted to plain text message with the help of the codon mapping table which is used in the step 2 of encryption. As a result, the input message sent by the sender is received at the receiver and is displayed in the LCD seven segment displays. The Algorithm is shown in the Fig .7

2.4 Algorithm of Decryption:

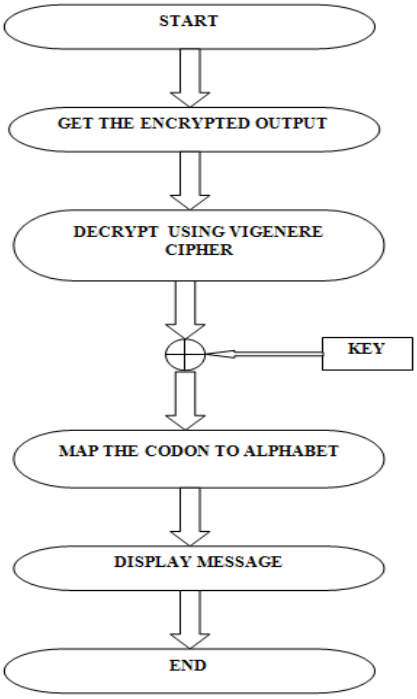

Figure 7: Proposed Flowchart for Decryption

3. Software's:

3.1 Model Sim:

Model Sim is one of the simulation and debugging tool for VHDL, Verilog, and mixed-language designs. ModelSim SE provides high-performance and advanced debugging capabilities, whereas ModelSim pe is the entry-level simulator for hobbyists and students [11]. ModelSim SE can be used in large multi-million gate designs, and is also supported in Microsoft Windows and Linux, in 32-bit and 64-bit architectures.

ModelSim XE stands for Xilinx Edition. It is specially designed for integration with Xilinx.ise. It enables testing of HDL programs written for Xilinx Virtex/Spartan series FPGA's without needed physical hardware.

3.2 Project Flow :

A project is a collection mechanism for an HDL design which is under specification or test. Although you don't have to use projects in ModelSim, they ease the interaction with the tool and is useful for organizing files and specifying the settings regarding simulation [12].The project flow is shown in Fig .8

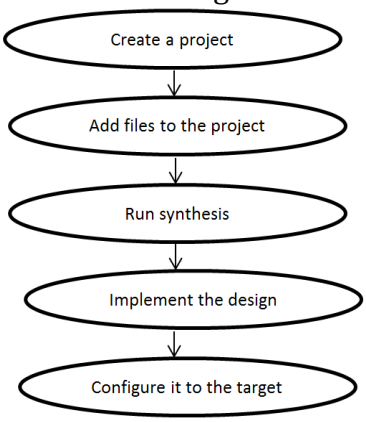

Figure 8: Software Design Flow

4. Conclusion:

This paper proposes an idea of introducing double layered security by encrypting the message twice with a symmetric key of length 1000 at the sender and the reverse process at receiver to retrieve the original message. DNA plays a vital role in encapsulating the complete information with only four characters A, G, T, C which increases the strength of the algorithm. The introduction of rapid DNA sequencing method may exponentially increase biological and medical research and discovery. This algorithm increases the complexity of doing cryptanalysis. Our idea can be extended in many ways and can be used in wide applications where confidentiality is concerned by analysing the performance of this algorithm designed to several cryptanalytic attacks.

5. References:

1. Mohammadreza Najaftorkaman, Nazanin Sadat Kazazi, A Method to Encrypt Information with DNA-Based Cryptography, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(3): 417-426 417 The Society of Digital Information and Wireless Communications, 2015 (ISSN: 2305-0012).
2. Naveen Jarold K, P Karthigaikumar, N M Siva Mangai, Sandhya R, Sruthi B Asok, Secure Communication Using DNA Cryptography, IJCST Vol. 4, I SSue 1, Jan - MarCh 2013.
3. Bonny B. Raj, J. Frank Vijay, PhD, T. Mahalakshmi, PhD, Secure Data Transfer through DNA Cryptography using Symmetric Algorithm, International Journal of Computer Applications (0975 –8887)Volume 133 – No.2, January 2016.
4. Prema T.Akkasaligar, Farhat Mulla, A Survey On Data Encryption Using Dna Technique, International Journal of Advanced Technology in Engineering and Science,Volume No 03, Special Issue No. 01, April 2015.
5. Sarvdeep Kushwaha, Ravi Kant, Chandresh Pandey, Dr. Vijay Kumar Chaurasiya, Dna Based Cryptogrphy For Secure Data Communication, International Journal For Technological Research In Engineering Volume 2, Issue 9, May-2015.
6. Andre´ Leier, Christoph Richter, Wolfgang Banzhaf, Hilmar Rauhe, Cryptography with DNA binary strands,
7. Received 21 January 2000; received in revised form 10 April 2000; accepted 14 April 2000.
8. Cui, G., L. Qin, Y. Wang, and X. Zhang.Information security technology based on DNA computing. in Anti-counterfeiting, Security, Identification, 2007 IEEE International Workshop on. 2007. IEEE.
9. Shivani Sharma, Amardeep singh, DNA Sequence Alignment based on Bioinformatics, IJCSET Sharma |July 2012| et al Vol 2, Issue 7,1305-1309.
10. Heider, D. and A. Barnekow, DNA-based watermarks using the DNA-Crypt algorithm.BMC bioinformatics, 2007. 8(1): p. 176.
11. Roweis, S., et al., A sticker-based model for DNA computation. Journal of Computational Biology, 1998.5(4):p. 615-629.
12. Sasikumar, S. and P. Karthigaikumar. VLSI implementation of DNA cryptography using quantum key exchange. in Electronics and Communication Systems(ICECS), 201 4 International Conference on. 2014. IEEE.
13. Lu, M., X. Lai, G. Xiao, and L. Qin, Symmetric-key cryptosystem with DNA technology. Science in China Series F: Information Sciences, 2007. 50(3): p. 324-333.