International Journal of Engineering & Technology, 7 (1.5) (2018) 62-70

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Reconfigurable pseudo biotic key encryption mechanism for cryptography applications

B.Murali Krishna[1], Habibulla Khan[2], G.L.Madhumati[3]

[1]Research Scholar, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India-522502
[2]Professor & Dean Student Affairs Department of ECE Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India-522502
[3]Professor & H.O.D Department of ECE, Dhanekula Institute of Engineering & Technology, AP, India;
*Corresponding author E-mail: *muralikrishna@kluniversity.in*

Abstract

Pseudo biotic cryptography will be an advanced crypto-analytic model, as it is presently increasing bimolecular computation, since its process energize and can verify future generation network computing. Nowadays, the data protection has become very important such that an unbreakable encryption technology should be designed in order to provide security for the data. A new paradigm in cryptography to secure information was introduced through biological structure called central dogma of molecular biology. DNA cryptographic system gains more popularity with enhanced features like, high storage capacity, security level, and more time to break the crypto system. This paper proposes new pseudo biotic DNA based crypto mechanism. This DNA computing created good path for storing large information, correspondence and high energy efficiency. The proposed method, message is converted to Deoxyribonucleic Acid (DNA), Messenger Ribonucleic acid (MRNA), and Transpose Ribonucleic acid (TRNA) standards. A part of converted message is spliced unsymmetrical to produce a random key at each stage. The sliced unsymmetrical key generation mechanism relies on the genetic information. The process involves in splicing the message and generating multiple sequence of keys from different stages which are random in order to enhance the degree of security. Cracking possibility of the algorithm is less due to pseudo random key generation mechanism and cipher both were merged in protein form. Proposed Algorithm utilizes less public key infrastructure, and communicated between Alice and Bob. Algorithm was designed, using Verilog HDL; Synthesized & Simulated in Vivado and hardware implementation is targeted to Zync FPGA architecture.

Keywords: *DNA cryptography with symmetric key, DNA, mRNA, FPGA.*

1. Introduction

The modern world is evolving with advanced technologies such as e-commerce, net banking and social networking. The faster growth in the internet technology allows the user to access the entire information that is transmitted through the internet and information on network can withstand to several attacks such as brute force attack, black hole attack, spoofing of IP etc. Evolution in internet led to increase in number of hackers, attackers and network security has become a major issue in present era and therefore high cryptographic algorithms are to be used to provide a secure transmission of data. Transfer of personal information through communication channel is necessary. We are not sure about whatever information that was transferred through the communication channel is secured. In such situation, network security is mandatory to overcome unauthorised access of confidential information. In order to offer high security 1.Cryptography and 2.Steganography are the two prominent and efficient methods. (1) Cryptography is an art of transferring information secretly over vulnerable channels. It is used for communicating through an untrusted network which can be understandable only by the admin.(2) Steganography is an art of hiding the actual data using duplicate data. There are handful numbers of algorithms for providing information security over communication channels. Security is the main factor for the transfer of information among several people using those algorithms. However, those algorithms are not enough to provide security for the information. A great work has already done on the pictography, resulting many security algorithms which include RSA, DES and ECC have been design to attain secrecy. Despite these algorithms need very complex mathematical computation of higher order prime numbers and the problem related to elliptical curve, for which research is still going on to find required solution. In addition the RSA algorithm is the best one to calculate high prime factors depending on intractability. Therefore to protect the information, it is very much necessary to develop an unbreakable cryptosystem. Therefore new cryptographic algorithms are required. DNA cryptography is the emerging and unbreakable cryptographic technique which provides high security introduced by Adleman.

2. Literature survey

Every stream of network security is searching for the development of unbreakable cryptosystems in order to safeguard the data during transmission through network. DNA computing has been studied in different fields over many years. For example, in 2016 [1] E.Suresh Babu, developed a Inspired Pseudo Biotic DNA Based

Cryptographic Mechanism Against Adaptive Cryptographic Attacks. which consists of key slicing from message, provides high confidentiality for the algorithm[2]. In 2015 [3] Asish Aich, Alo Sen, Satya Ranjan Dash and Satchidananda Dehuri developed a cryptographic algorithm consisting of two stages. First stage is to encrypt the plain transcript using a random key generator and second stage is to re-encrypt the encrypted information with the DNA sequence to generate the cipher text. DNA molecules are inbuilt having exceptional energy efficiency, huge parallelism and immense information density. These characteristics will add on security like authentication, encryption and many more. There are few theories and studies by researchers explained briefly. [4] Sreeja C.S in 2014 discussed various DNA cryptography methods and proposed a pseudo biotic DNA based cryptographic algorithm which consists of both slicing and padding techniques with complimentary procedures which provides high confidentiality for the algorithm.[5] Sabari Pramanik in 2012 developed a cryptographic method using padding, DNA structure and DNA hybridisation scheme which lessens the time complexity.[6] Darpan Anand in 2013 analysed digital signature algorithms and applications of identity based cryptography based on bilinear computation. This paper also viewed encryption applications in mobile networks and other wireless systems. [7] Mandeep Singh Narula in 2014 developed an enhanced version of Triple-DES and DES as they are extensively used and implemented the cryptographic circuit using Verilog HDL.

3. Scope of DNA based cryptography

Cryptanalyst are capable of cryptanalyzing the modern cryptosystems and now the globe is searching for new methods to have secrecy for the information it carries. In order to bring trustable technology for unbreakable procedures, cryptography is mainly used in the areas of bimolecular computation. The process of DNA computing involves in bimolecular computation, which uses biological methods in order to perform massive sequential computations. Nowadays, the importance of parallelism is tremendously rising. The cryptanalyst can easily cryptanalyze the advanced systems and today the whole globe is waiting for different ways to provide network security to get the entire information, in order to secure the data it translates. The main reason for using bimolecular computation along with cryptography is to provide the technology having unbreakable algorithms. This cryptography could be an advanced cryptanalytic model from newly rising bimolecular computation as this process can verify upcoming computations [8].

4. Central dogma of molecular biology

Data Communication between alice and bob protected from hackers uses several cryptography techniques [9]. Central Dogma of Molecular Biology (CDMB) spreads the complexity and inserts some biological properties in cryptography like DNA replication, transcription and translation methodologies shown in figure 1. Among the existing techniques DNA cryptography techniques have high security level, storage capacity, and more time for hackers to break the crypto system to decrypt the original message from cipher.

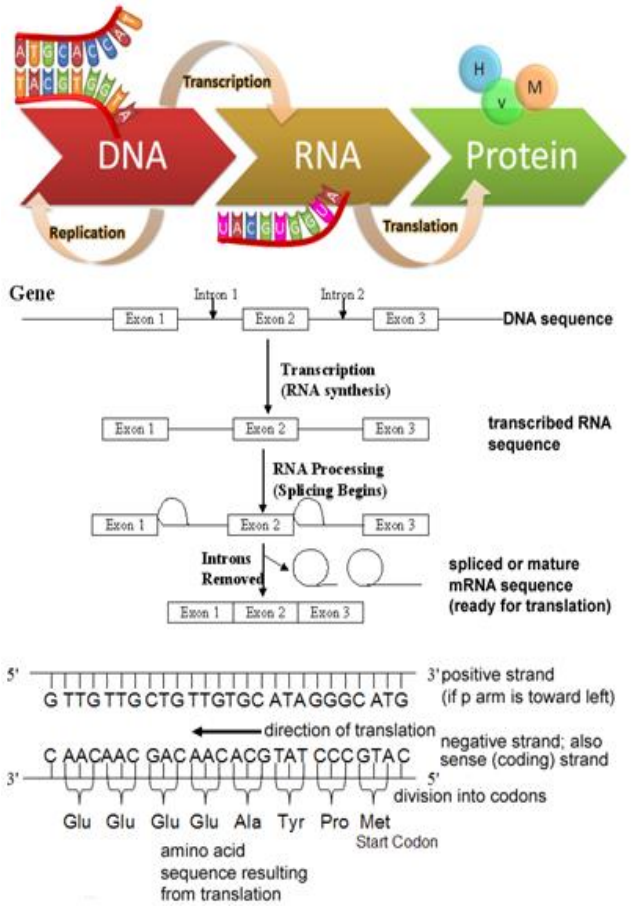


Fig. 1: Central Dogma of Molecular Biology

4.1 Background of CDMB

The process of converting DNA molecules into protein sequence by excluding Introns and merging Exons is called Central Dogma of Molecular Biology [10]. Genetic code is made up of Codons which are three letter codes. Biological molecules DNA and RNA have triplets which are called as codons. The conversion involves in two stages Transcription and Translation. Transcription is the process of converting DNA sequence to mRNA sequence and Translation is the process of converting mRNA to protein sequence.

4.2 Nucleic Acid

Nucleic acids are a cluster of biomolecules which are being part of the cell nucleus. These nucleic acids are long polymers made up of monomeric elements (units) known as nucleotides: A (adenine), C (cytosine), G (guanine), T (thymine) and U (uracil). There are two types of nucleic acids present in the cell nucleus: They are DNA and RNA.

4.2.1 DNA (Deoxyribonucleic Acid)

The DNA is the biological molecule that possesses all the genetic information of the cell and it is responsible for transfer genetics from the parents, to their offspring.

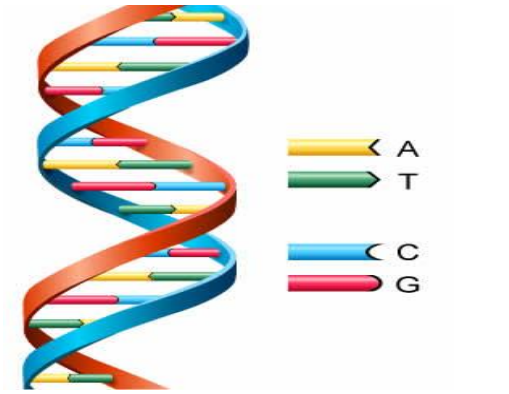


Fig. 2: DNA Structure

Its molecule is composed with 4 nucleotides (A, C, G, T) having double-helix structure shown in figure 2. Because of chemical affinity Adenine pair up with Thymine and Cytosine with Guanine. Table 1 shows the Nucleotide to Binary Conversion of nucleotides (A, C, G, and T).

Table 1: Nucleotide to Binary Conversion

Nucleotide	Binary Equivalent
A	00
C	01
G	10
T	11

4.2.2 RNA (Ribonucleic Acid)

The RNA is also a biological molecule composed of the nucleotides C, A, G, and U. The only difference between DNA and RNA is Thymine is replaced with Uracil. There are two types of RNA. They are mRNA and tRNA. In this study we make use of mRNA form. Mainly works on basis of complementary rule [11].

A. MRNA

Messenger RNA is a xerox copy of DNA, except the T (Thymine) is replaced with nucleotide U (Uracil). The process of converting DNA to MRNA is called a transcription. MRNA is a Single Standard [12].

B. TRNA

Transfer RNA is the key to decrypt the code word in mRNA. tRNA reads the codons and binds to particular amino acid.

C. Codons

During Protein synthesis three DNA or RNA nucleotides maps to suitable amino acids called codons.

D. Anti-Codons

Transfer RNA contains a covalent bond attachment of aminoacid that corresponds to anticodon sequence shown in figure 3. Codons in mRNA, Anticodons in tRNA match amino acid is added to growing protein.

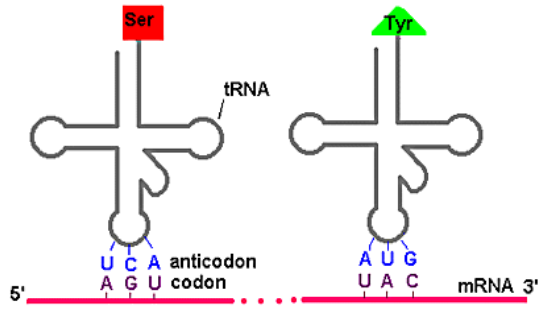


Fig. 3: Codons & Anticodons

E. Protein sequence

Three nucleotides in DNA and mRNA sequence maps to appropriate amino acids forms into one protein. The process of converting mRNA into protein form is called translation shown in figure 4.

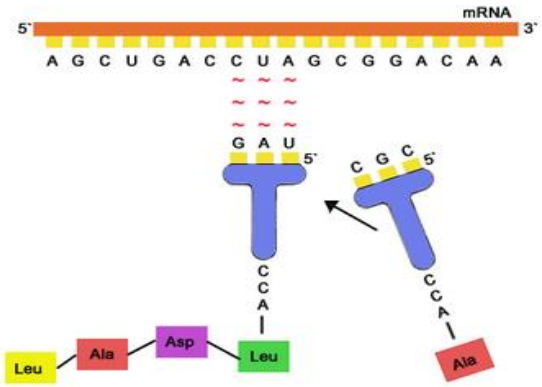


Fig. 4: Translation

4. Proposed Model

The private key cryptographic working algorithm based on pseudo biotic DNA is addressed in this paper against some particular cipher attacks. The pseudo biotic key encryption mechanism of DNA based cryptography uses DNA computation by knowing that it had created good path in large correspondence. This biotic cryptography depends on genetic information. When compared to the actual biological DNA sequence, the proposed mechanism utilise DNA terminology and mechanism of DNA. This experimental analysis shows that it is very efficient in computation, storage, transmission and protects from attacks. Key generation mechanism plays a crucial role in securing data in any cryptography techniques. From literature survey authors proposed key slicing mechanism and simulated on software. In this paper two methods were proposed namely Pseudo Biotic Three Stage Key Generation Mechanism (PBTSKGM). Pseudo Biotic Single Stage Key Generation Mechanism (PBSSKGM).

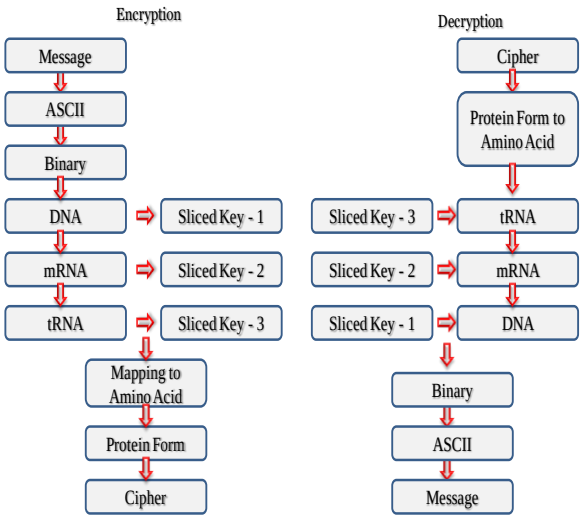


Fig. 5: Pseudo Biotic Three Stage Key Generation Mechanism

PBTSKGM the proposed design using RNA splicing introns are removed and all exons are concatenated and converted into protein form. Message is converted into DNA, mRNA and tRNA forms. In this method the message is converted to Deoxyribonucleic Acid (DNA), Messenger Ribonucleic acid (MRNA), and Transpose Ribonucleic acid (TRNA) standards. A part of converted message is spliced unsymmetrical to produce a random key at each stage. Final Key in protein form is generated from three random keys and encrypted to protect from cipher attacks. Key generation can be done using manual method and arbitrary method from DNA-mRNA-tRNA sequences shown in figure 5. In manual method

user can have a priority to generate random key and cipher in protein form. In arbitrary method key is generated based on LFSR. In PBSSKGM keys are sliced at single stage concatenated mRNA stage in various positions after performing left and right circular shifts, and converted into protein form along with cipher and transmitted in channel shown in figure 6.

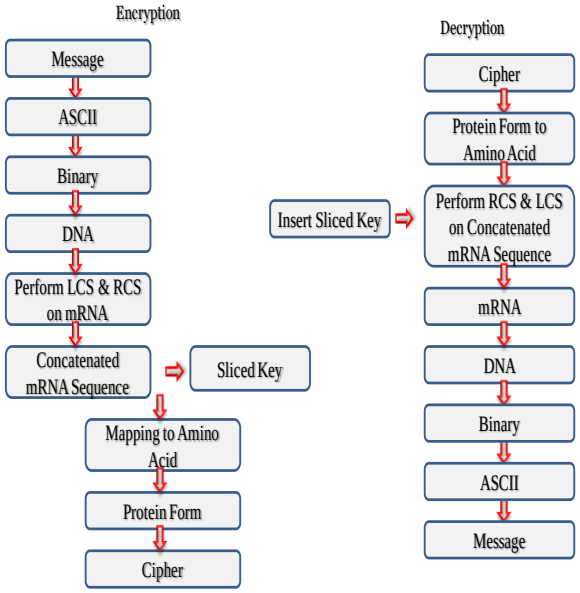


Fig. 6: Pseudo Biotic Single Stage Key Generation Mechanism

Pseudo Biotic Three Stage Key Generation Mechanism Encryption Example – Method - I:
MESSAGE: KL University

ASCII to Binary Conversion:
K L U n i v e r s i t y

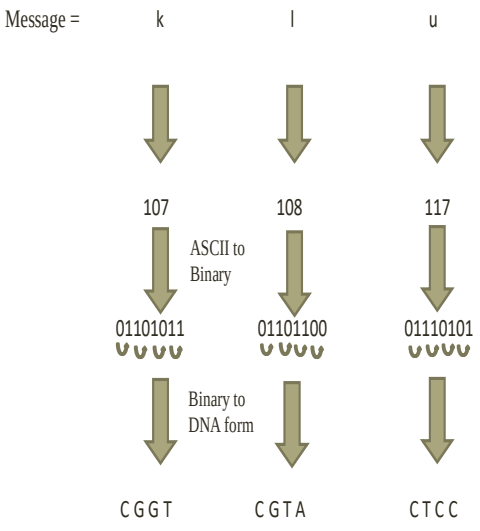
ASCII to Decimal
75 76 85 110 105 118 101 114 115 105 116 121

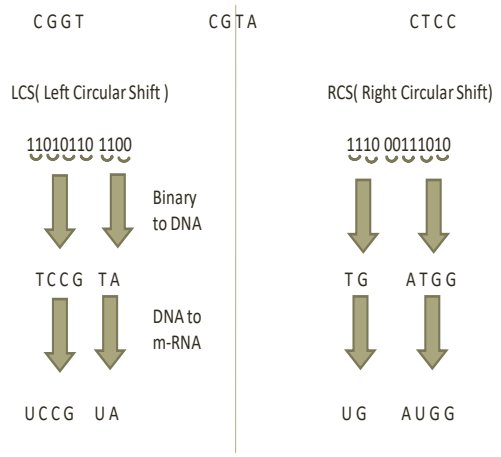
Decimal to Binary
01001011 01001100 01010101 01101110 01101001 01110110 01100101 01110010 01110011 01101001 01110100 01111001

Binary to DNA form
CAGT CATA CCCC CGTG CGGC CTCG CGCC CTAG CTCT CGGC CTCA CTGC

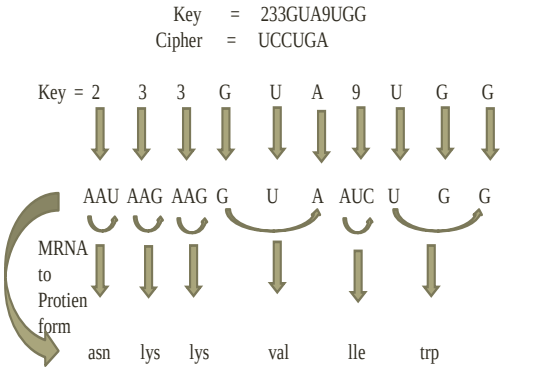
KEY K1: Slicing of the DNA sequences gives key K1
1 3 12 C G T
DNA Conversion
AAC ACT AGA CGT
Protein to Amino acid
asn thr arg arg
LEFT PART L1:
CAG TCA TAC CCC GCG GCC TCG CGC CCT AGC TAT CGG CCT CAC TGC
Protein to Amino acid
Gln ser tyr pro ala ala ser arg pro ser tyr arg pro his cys
STEP2 : m RNA Conversion
KEY K2 : Slicing of left part L1 gives key K2, then 1 3 30
UAU
AAC AAG CGT UAU
Protein to Amino acid
asn lys arg tyr
LEFT PART L2:
CAG UCA UAC CCC GCG GCC UCG CGC CCU AGC CGG CCU CAC UGC
Protein to Amino acid
Gln ser tyr pro ala ala ser arg pro ser arg pro his cys
STEP 3: Transpose
CAG UCA UAC CCC GCG GCC UCG CGC CCU AGC CGG CCU CAC UGC
DNA to Binary form
01 00 10 11 01 00 11 00 01 01 01 01 10 01 10 10 01 01 11 01 10 01 10 01 01 01 11 00 10 01 01 10 10 01 11 01 00 01 11 10 01

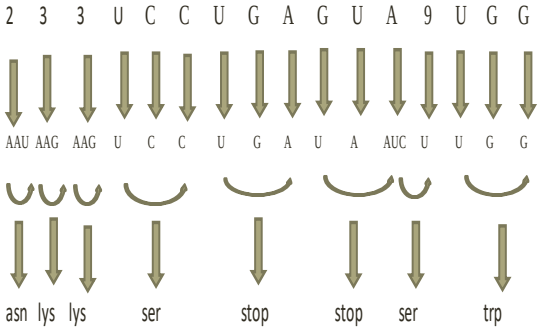
Transpose
10 11 01 00 10 11 00 11 10 10 10 10 01 10 01 01 10 10 00 10 01 10 01 10 10 10 00 11 01 10 10 01 01 10 10 00 10 11 10 00 01 10
Binary to DNA form
GUC AGU AUG GGG CGC CGG AGC GCG GGA UCG GCC GGA GUG ACG
KEY K3: Slicing of the transposed sequence gives key K3, then
1 3 15 CGG
DNA Conversion
AAC ACT AGG CGG
Protein to Amino acid
Asn thr arg arg
LEFT PART L3:
GUC AGU AUG GGG CGC AGC GCG GGA UCG GCC GGA GUG ACG
Protein to Amino acid
Val ser met gly arg ser ala gly ser ala gly val thr
Final Encrypted Key (K1 K2 K3)
asn thr arg arg asn lys arg tyr asn thr arg arg
Cipher :
val ser met gly arg ser ala gly ser ala gly val thr
Merged cipher and key :
Cipher is placed first and key is placed next, then merged data will be :
val ser met gly arg ser ala gly ser ala gly val thr asn thr arg arg asn lys arg tyr asn thr arg arg
The above example depicts encryption of method -1 by performing reverse operation decrypts the original message.
Pseudo Biotic Single Stage Key Generation Mechanism Encryption Example– Method - II:





KEY GENERATION:





Cipher is placed in even and key in odd positions are merged in protein form transmitted in a secure channel. The above example depicts encryption of method -2 by performing reverse operation decrypts the original message.

The steps to be followed to perform communication models with symmetric pseudo DNA dependent cryptography are,

1. Alice considers the plain text and it is converted in terms of 0‘s and 1’s which is in DNA form.
2. Plain text, which is in DNA form to produce random key of different lengths by developing number of splices from mentioned DNA pattern.
3. Introns are discarded from mentioned DNA sequence as initial round of key generating, to recognize intron places and discarded length of pattern code.
4. Alice would now convert DNA sequence to mRNA sequence.
5. After generating mRNA string, generate random key of different length by producing the number of splices from modified mRNA pattern using key splicing system.
6. Again, spliced mRNA string is converted into amino acids, those results in formation of protein sequence.
7. Later, using public channel the protein sequence can be sent to bob.
8. The random variable length key comprises of starting index, number of splices, pattern code length, intron position, intron places, introns cut out. 9. Now receiver can perform decryption process after he received random key and cipher text (protein form) from Alice using secure channel.
10. Bob decrypts cipher text message to trace mRNA sequence from protein sequence using random key reversible translation. He also recovers DNA sequence of data in reverse procedure as Alice performs encryption.
11. Receiver can then recover the binary form of information into original information sent by Alice.

The main advantage of biotic DNA symmetric cryptosystem is that hackers could not decrypt the encrypted algorithm as they do not know about the information of the key. In addition to this, it is very onerous to get random mRNA key sequence. A part of converted message is spliced unsymmetrical to produce a random key at each stage. Final a protein form of Key is generated from three random keys at different stages and encrypted with cipher to protect from attacks. Unless hacker acquire the skills about unravel cipher and a procedure for key decryption it is difficult regenerate the original message. Cracking possibility of the algorithm is less due to pseudo random key generation mechanism and cipher both were in protein form.

5. Security analysis

The technique must ensure that an algorithm is safe and free from any despiteful activities from the attackers outside. The two most important parameters to be considered primarily are time and computational toughness. The features that ensure that a plain text cannot be read from a cipher text, because each protein form has four mRNA triplets and which makes it impossible to differentiate given pair of messages are Semantic security and message indistinguishability.

6. Reconfigurable crypto system

In digital design reconfigurable hardware gains more popularity, it may be seen that FPGA’s are to be the target technology. Due to evolvable nature FPGA’s suitable for many applications like medical, image processing, configurable system on chip design for satellites, cryptography, digital logic design, gaming application and custom logic designs etc. FPGA internal architecture comprises of configurable logic blocks (CLB’s), routing resources and input output blocks. CLB complexity ranges from fine grain to coarse grain depend on architecture. Configuration can be classified into static and dynamic partial reconfiguration. Earlier FPGAs enable complete chip to reconfigure. With introduction to Partial Reconfiguration (PR), only some (architecture) devices in Xilinx and Altera and some open source tools support supports PR. PR is a portion of the chip to be reconfigured, among architecture while still remaining area of the chip retains their configured current design. Xilinx PR gains more popularity with technology trends like programmable SoC in Zync supports both integrated cortex a9 processor processing system with programmable logic and Phyton Supported new PYNC architectures.

7. Simulation

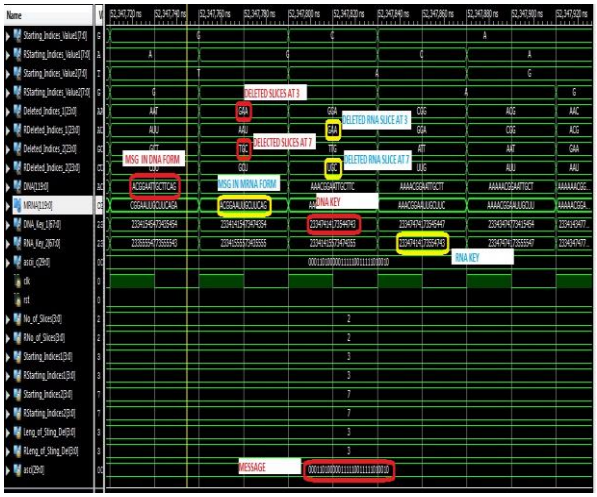


Fig. 7: Key Generation from DNA-mRNA-tRNA.

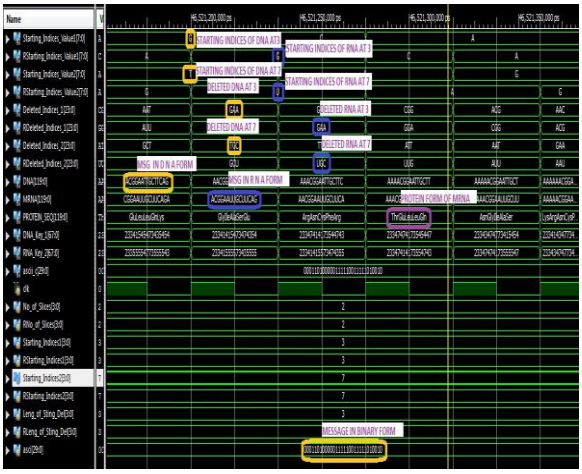


Fig. 8: Protein Form of Key Splicing.

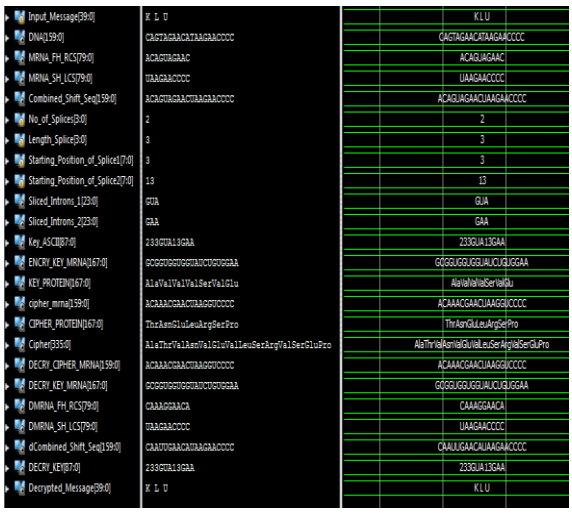


Fig. 9: Overall Process of Encryption and Decryption.

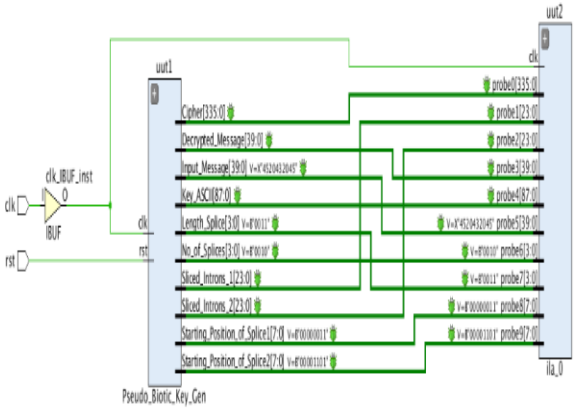


Fig. 10: RTL Schematic of proposed Pseudo Biotic Key Encryption Mechanism Algorithm with binding Chipscope Pro Logic Analyzer to monitor internal hardware signals.

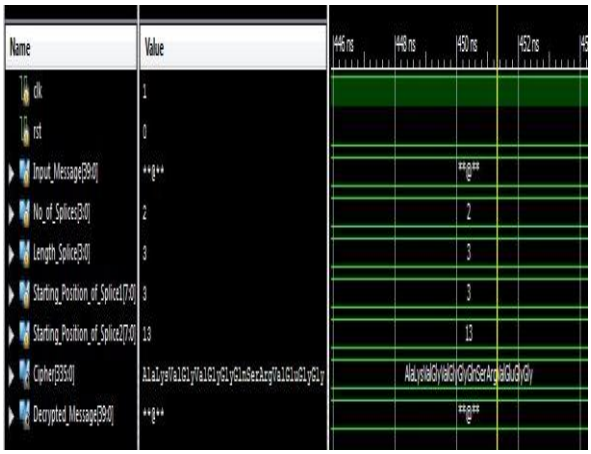


Fig. 11: Process of Encryption and Decryption when special characters are given as Input (**@**).

Figure 7 describes about the process of key generation. The generated key consists 3 splices, these slices are included into from DNA form of message, mRNA form the message and tRNA form of the message i.e., the first splice is taken from DNA form of message at random position. Second splice is produced from mRNA form and third splice is from tRNA form. This process deduces that final key is generated from message itself by applying biological properties in through central dogma of molecular biology and slicing from message at different stages.

Figure 8 illustrates about the procedure that is involved in the conversion of key into protein form. In key generation the positions from where splices are considered in numeric from. Now those numbers are converted into DNA form following mRNA form and tRNA form and finally the key represented in protein form which is a bit difficult to break.

Figure 9 clearly explains about overall process that takes place in this proposed algorithm. Consider an example KLU which is converted into DNA form. It is divided into two halves and it undergoes shifts in order increase complexity. After shifting these halves are combined together to form a DNA sequence. As per the description mentioned about figure 4 a key is generated from the DNA sequence. The keys spliced at different stages are converted into protein form along with the cipher text. The process of Encryption ends after merging key and cipher into protein form. Following the reverse process of Encryption is a Decryption process.

Figure 10 is the RTL Schematic of the proposed algorithm Reconfigurable DNA Crypto System through Pseudo Biotic Key Encryption Mechanism generated by simulating the algorithm in the Xilinx Vivado. Chipscope Pro Logic Analyzer is binded to algorithm to monitor internal hardware signals.

Figure 11 proves that the proposed algorithm is not only useful for encrypting the messages which are in the binary form and string form but also it encrypts special characters too. Message that is considered is **@**. The complete process of encryption and decryption are shown in this figure.

8. FPGA Implementation of DNA Crypto System

Figure 12 and Figure 13 illustrates the FPGA implementation of the algorithm when the input binary form of as well as strings and special characters. Hardware implementation is carried out on ZED board. Figure 14(a) shows the schematic diagram of the algorithm which is implemented in Vivado. Figure 14(b) shows the Floor Plan occupancy of proposed algorithm.

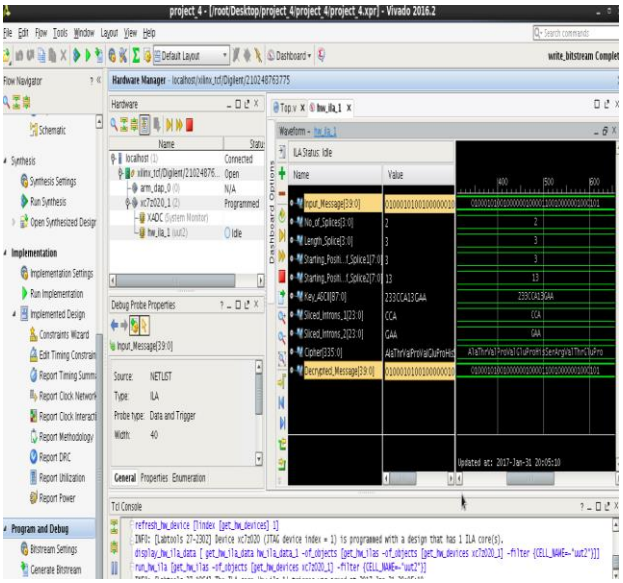


Fig. 12: FPGA Implementation of the proposed Algorithm when Input message is in binary form.

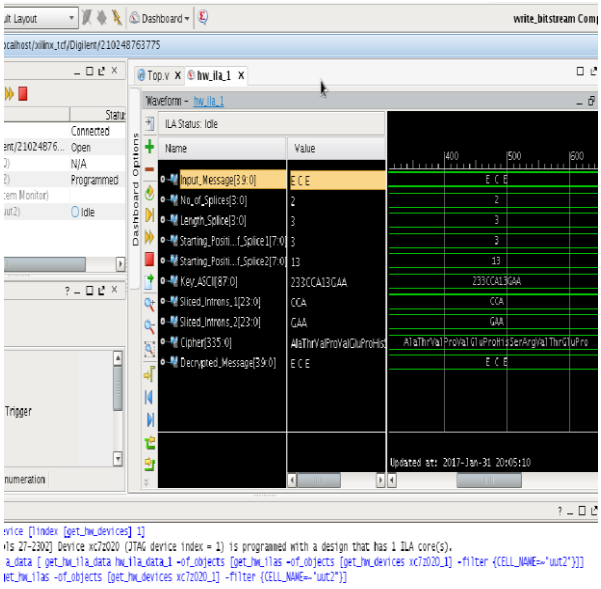


Fig. 13: FPGA Implementation of the proposed Algorithm when Input message is String / Characters.

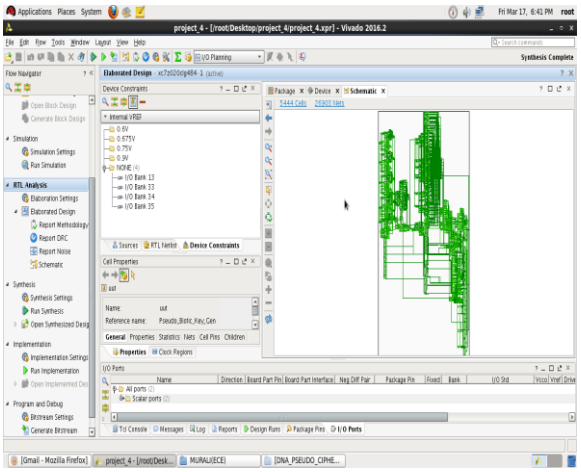


Fig. 14(a): Schematic diagram of the proposed algorithm in Vivado.

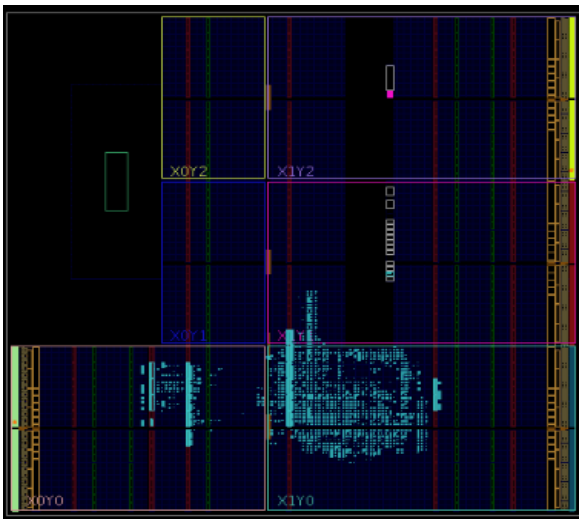


Fig. 14(b): Floor Plan Occupancy of the proposed algorithm in Xilinx Vivado.

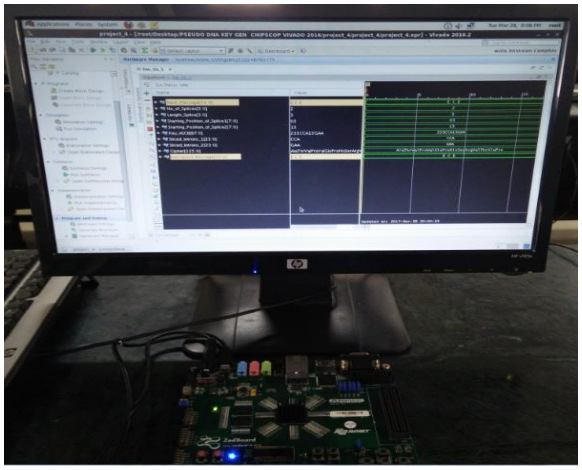


Fig. 15: Physical view of implementation Reconfigurable DNA Crypto System through Pseudo Biotic Key Encryption Mechanism on Zed Board (Zync Architecture).

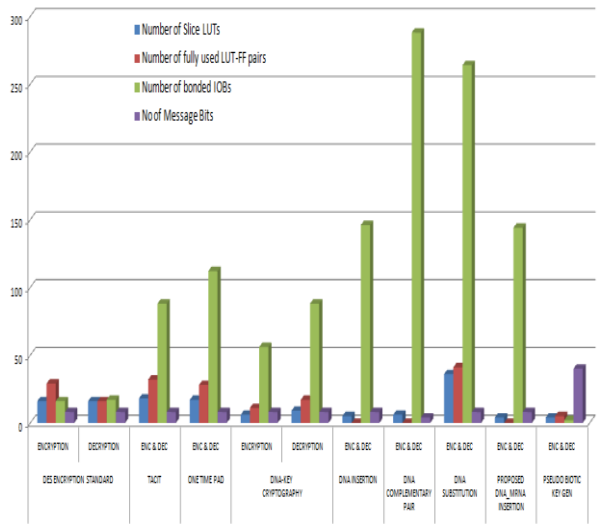


Fig. 16: Graphical Representation of Resource Utilization for Several Cryptography Techniques.

Figure 15 shows the Physical view of implementation Reconfigurable DNA Crypto System through Pseudo Biotic Key Encryption Mechanism on Zed Board (Zync Architecture). Internal signals like message, no. of splices, length of each splice, position of splice, generated random key from spliced unsymmetrical message, cipher and key merged in protein form or viewed using Chipscope Pro Logic Analyzer.

Figure 16 shows the Graphical Representation of Resource Utilization for Several Cryptography Techniques Proposed Algorithm, consumes less resources compared among several cryptography techniques with Spartan and Virtex FPGA architectures.

9. Conclusion

Proposed Reconfigurable DNA crypto system through pseudo biotic based key encryption algorithm is depending on genetic information. However, this prototype is a highly emerging field which made good strides of ultra compact data storage. As the internet technology is rising faster, users have become much capable in accessing the information that is carried through the internet and exposed to several attacks. Every stream of network security is searching for the development of unbreakable cryptosystems in order to safeguard the data during transmission through network. This inspired us to develop a pseudo biotic DNA based key encryption mechanism, which uses splicing scheme to generate cipher and key in protein form that makes the enciphered text tough to decipher. This experimental exploration indicates that proposed methods are powerful against attacks and there will be a secure transfer of data. Lastly, DNA cryptography is a developing area where research is possible in growth and enhancement. Cracking possibility of the algorithm is less due to sliced pseudo random key generation and cipher both were merged in protein form. Proposed Algorithm, consumes less resources compared among several cryptography techniques with Spartan and Virtex FPGA architectures. Hardware Implementation is targeted to Zync FPGA architecture proves that algorithm is feasible in real time environment which a message is encrypted an d decrypted between Alice and Bob.

References

[1] E.SureshBabu, C. Nagaraju, MHM Krishna Prasad “Inspired Pseudo Biotic DNA based Cryptographic Mechanism against Adaptive Cryptographic Attacks” Accepted in The Mediterranean Journal of Computers and Networks. ISSN 1744-2397.

[2] E.SureshBabu, C. Nagaraju, MHM Krishna Prasad “ Light-Weighted DNA Based Cryptographic Mechanism Against Chosen Cipher Text Attacks” Springer ,May 2015.

[3] AsishAich, Alo Sen, Satya Ranjan Dash and SatchidanandaDehuri “A Symmetric Key Cryptosystem Using DNA Sequence with OTP Key”Information Systems Design and Intelligent Applications in 2015, pp 207-215

[4] Sreeja C.S, Mohammed Misbahuddin “DNA for information security: A Survey on DNA computing and a pseudo DNA method based on central dogma of molecular biology” International Conference on Computing and Communication Technologies, IEEE in 2014.

[5] Sabari Pramanik, Sanjit Kumar Setua, “DNA cryptography”, International Conference on Electrical and Computer Engineering, 20-22 December,2012.

[6] DarpanAnand, VineetaKhemchandani, Rajendra K Sharma ,“Identity-based cryptography techniques and applications” , Computational Intelligence and Communication Networks (CICN), IEEE in 2013.

[7] Mandeep Singh Narula,Simarpreet Singh,” Implementation of Triple Data Encryption Standard using Verilog”, published in IJARCSSE in 2014.

[8] Vikas Agrawal, Shruti Agrawal, Rajesh Deshmukh, “Analysis and Review of Encryption and Decryption for Secure Communication”, International Journal of Scientific Engineering and Research (IJSER), Volume 2 Issue 2, February 2014.

[9] Harneet Singh, Karan Chugh, Harsh Dhaka, A.K.Verma, “DNA based Cryptography: An Approach to Secure Mobile Networks”, International Journal of Computer Applications, 2010.

[10] Advances in Intelligent Systems and Computing 340 J. K. Mandal, Suresh Chandra Satapathy, Manas Kumar Sanyal, Partha Pratim Sarkar, AnirbanMukhopadhyay(eds.)- “Information Systems Design and Intelligent Applications” pg 207 - 215 in the year 2015.

[11] X. Guozhen, L.U. Mingxin, Q. Lei, L. Xuejia, “New field of Cryptography: DNA Cryptography”.

[12] Naveen Jarold K, P Karthigaikumar, N M Siva Mangai, Sandhya R, Sruthi B Asok, “Secure Communication Using DNA Cryptography”, International Journal of Computer Science And Technology, Jan-March 2013.

[13] Dr. Seetaiah Kilaru, Hari Kishore K, Sravani T, Anvesh Chowdary L, Balaji T “Review and Analysis of Promising Technologies with Respect to fifth Generation Networks”, 2014 First International Conference on Networks & Soft Computing, ISSN:978-1-4799-3486-7/14,pp.270-273,August2014.

[14] Meka Bharadwaj, Hari Kishore "Enhanced Launch-Off-Capture Testing Using BIST Designs” Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.12, Issue No.3, page: 636-643, April 2017.

[15] N Bala Dastagiri, Kakarla Hari Kishore "Reduction of Kickback Noise in Latched Comparators for Cardiac IMDs” Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.43, Page: 1-6, November 2016.

[16] A Murali, K Hari Kishore, D Venkat Reddy "Integrating FPGAs with Trigger Circuitry Core System Insertions for Observability in Debugging Process” Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.11, Issue No.12, page: 2643-2650, December 2016.

[17] Mahesh Mudavath, K Hari Kishore "Design of CMOS RF Front-End of Low Noise Amplifier for LTE System Applications Integrating FPGAs” Asian Journal of Information Technology, ISSN No: 1682-3915, Vol No.15, Issue No.20, page: 4040-4047, December 2016.

[18] P Bala Gopal, K Hari Kishore, B.Praveen Kittu “An FPGA Implementation of On Chip UART Testing with BIST Techniques”, International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 10, Number 14 , pp. 34047-34051, August 2015

[19] S Nazeer Hussain, K Hari Kishore "Computational Optimization of Placement and Routing using Genetic Algorithm” Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.47, page: 1-4, December 2016.

[20] N Bala Gopal, K Hari Kishore "Analysis of Low Power Low Kickback Noise in Dynamic Comparators in Pacemakers” Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.44, page: 1-4, November 2016.

[21] Rajesh, M., and J. M. Gnanasekar. "Congestion control in heterogeneous wireless ad hoc network using FRCC."

Australian Journal of Basic and Applied Sciences 9.7 (2015): 698-702.

[22] S.V.Manikanthan and V.Rama"Optimal Performance Of Key Predistribution Protocol In Wireless Sensor Networks" International Innovative Research Journal of Engineering and Technology ,ISSN NO: 2456-1983,Vol-2,Issue –Special – March 2017.

[23] T. Padmapriya and V. Saminadan, "Distributed Load Balancing for Multiuser Multi-class Traffic in MIMO LTE-Advanced Networks", Research Journal of Applied Sciences, Engineering and Technology (RJASET) - Maxwell Scientific Organization , ISSN: 2040-7459; e-ISSN: 2040-7467, vol.12, no.8, pp:813-822, April 2016.