Journal of Theoretical and Applied Information Technology
31st May 2017. Vol.95. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FPGA IMPLEMENTATION OF DES ALGORITHM USING DNA CRYPTOGRAPHY

B.MURALI KRISHNA[1], HABIBULLA KHAN[1*], G.L.MADHUMATI[2], K.PRAVEEN KUMAR[3], G.TEJASWINI[3], M.SRIKANTH[3], P.RAVALI[3]

[1]Research Scholar, [3]U.G Student Department of ECE, K L University, AP, India:
[1*]Professor & Dean Student Affairs Department of ECE, K L University, AP, India;
[2]Professor & H.O.D Department of ECE, Dhanekula Institute of Engineering & Technology, AP, India;
E-mail: muralikrishna@kluniversity.in, praveenkumar205.pk@gmail.com

ABSTRACT

DNA Cryptography is the evolving cryptanalytic technology in the field of information security. Using this Cryptanalytic technology which involves in DNA Cryptography improves the security level to protect information from attackers. However all those methods which are proposed earlier remained theoretical concepts for enhancing security. In addition, Traditional Cryptographic methods have some demerits such as size of the input, computational speed and cost. To overcome these problems this proposed paper describes in detail about the advancements that are made in the DES Algorithm (Data Encryption Standard) using DNA cryptography. Moreover, this paper illustrates about the DES algorithm's encryption and decryption process which follows symmetric key system followed by DNA cryptography. Out of two stages in the proposed technique, in first stage the Cipher is generated using conventional DES algorithm, the key that is used to produce cipher is generated by using partial reconfiguration and later the key is also encrypted using dummy key. In second stage this encrypted key and cipher is subjected to DNA computing followed by the protein form i.e., the cipher is shown in the form of proteins which is unbreakable. This cryptographic technique is designed and simulated using Xilinx ISE and targeted on Zed board. The analysis of the results endorse that the proposed algorithm is immune from attacks, reliable and robust for transmission of information.

Key Words: *DNA Cryptography, Data Encryption Standard, RNA, Protein form, Zed Board FPGA.*

1. INTRODUCTION

The modern world is evolving with advanced technologies such as e-commerce, net banking and social networking. 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. Widely used cryptographic algorithms like DES, AES and RSA are vulnerable to attacks and have been broken; therefore new cryptographic algorithms are required. DNA cryptography is the emerging and unbreakable cryptographic technique which provides high security introduced by Adleman. The proposed technique DES algorithm using DNA cryptography has enhanced security. The analysis on this technique endorse that the proposed algorithm is immune from attacks,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

reliable and robust for transmission of information.

2. LITERATURE SURVEY

DNA computing has been studied in different fields over many years. For example, in 2016 [1] Asish Aich 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. Research has been done on DES algorithm and it is confirmed that it can be easily broken. We can overcome by including the concept of DNA with DES algorithm. 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. [2] 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.[3] Sabari Pramanik in 2012 developed a cryptographic method using padding, DNA structure and DNA hybridisation scheme which lessens the time complexity. [4]DarpanAnand 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. [5] 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. All these conventional developed methods undergo brute force attacks especially when DES algorithm is considered. Now the proposed algorithm is the hybrid algorithm which includes DNA cryptography and DES algorithm. With the inclusion of DNA cryptography the complexity to break or decode the algorithm increases. The proposed algorithm is immune from attacks, reliable and robust for transmission of information.

3. IMPORTANCE OF DNA COMPUTATION

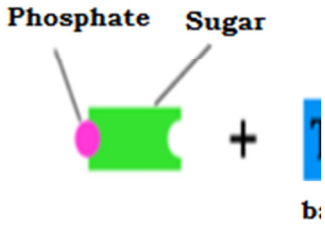
3.1 Nucleic Acid:

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.

3.1.1 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. Its molecule is composed with 4 nucleotides (A, C, G, T) having double-helix structure. Because of chemical affinity Adenine pair up with Thymine and Cytosine with Guanine.

Table 1: Nucleotide To Binary Conversion



Nucleotide	Binary equivalent
A	00
C	01
G	10
T	11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fig 1: Structure Of Nucleotide

3.1.2 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.

3.2 Background of Central Dogma of Molecular Biology:

The process of converting DNA molecules into protein sequence is called Central Dogma of Molecular Biology. 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.

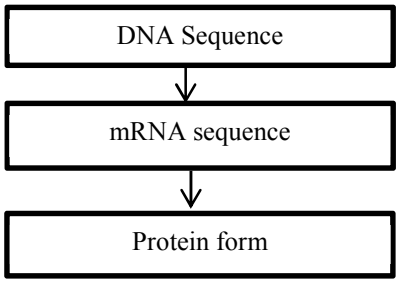


Fig 2: Process Of Conversion

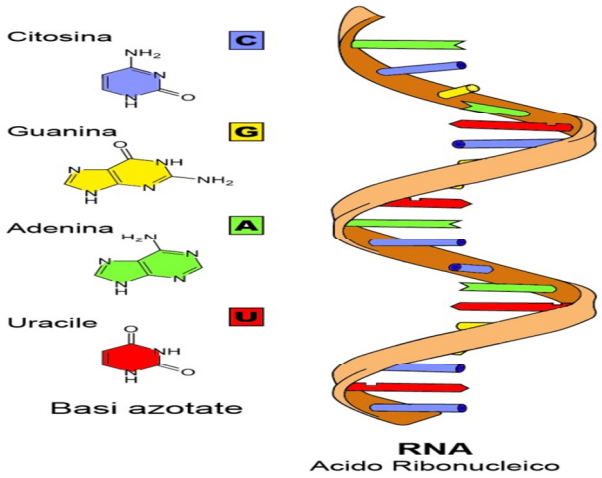
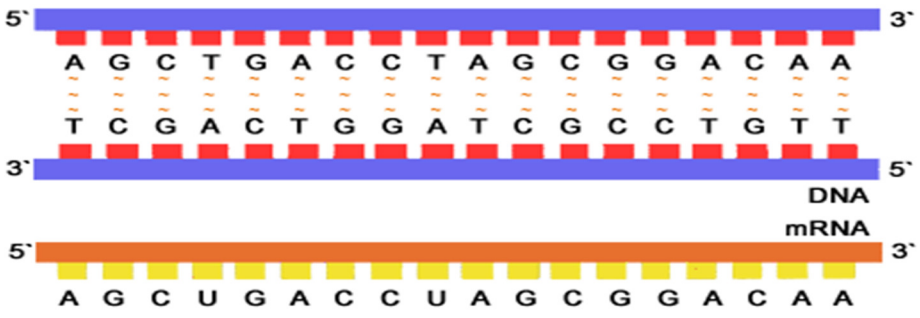


Fig 3: Structure Of RNA



ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fig 4: Transcription Of DNA To Mrna

4. KEY GENERATION PROCEDURE

Data Encryption Standard algorithm is subjected to linear crypto analytic attacks for the reason of having weak keys. In order to counterattack the brute force attacks, enhancement of key is required. Partial reconfiguration ability of the system is the emerging method to provide solution.

4.1 Partial Reconfiguration

Partial reconfiguration is a procedure of modifying an area in FPGA without changing any other applications. From the functionality of the design flow, it is divided into two types: Static PR and Dynamic PR. Dynamic partial reconfiguration is also known as active partial reconfiguration. It allows the change in functionality of a specific part of the device while the rest of the parts of FPGA is still running. Partial bit files are generated from the design flow using the process of Partial Reconfiguration.

Cryptography is responsible for formation of secure channel between sender and receiver. By using different algorithms encryption of information at sender with key takes place and decryption involves in retrieving the original information from the encrypted data with key at the receiver. Linear Feedback Shift Register (LFSR) is used to generate Key. It generates random keys by shift and XOR based mechanism. Key randomness can be improved by using seed value already loaded. Various types of LFSR's are existing based on the application. Partial Reconfiguration enhances the security level of DNA cryptography methods in runtime by altering the key using LFSR.

4.2 Importance of Dummy key

A binary key of known size is considered. Divide the key into two equal halves to generate a dummy key. If the length of left half of the key is odd, pad with 0 and if the right half of the key is odd, pad with 1. Concatenate the two halves which produce the dummy key. Original key is to be Ex-or with dummy key to give encrypted key. This key is Tran scripted to DNA form and then Translated to amino acid form. Thus final encrypted key will be obtained.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

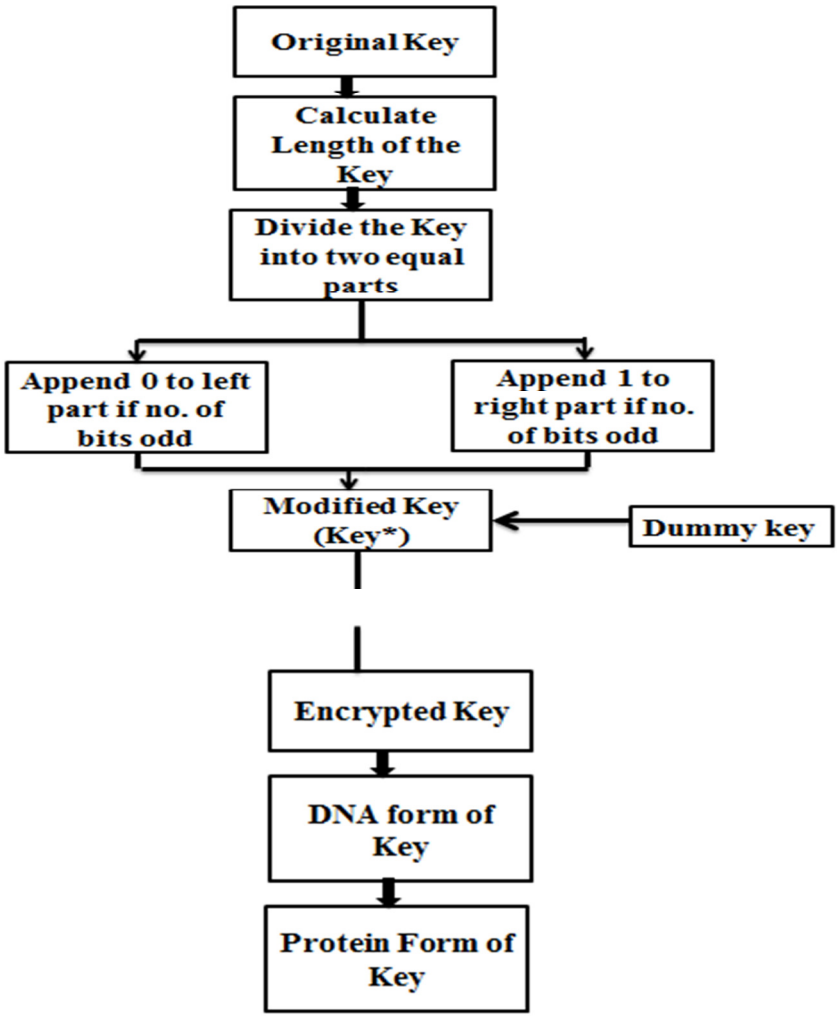


Fig 5: Flow Chart For Generating Final Encrypted Key

5. ALGORITHM

Step1: Consider a plain text message and Key of same size. Key is generated by using Partial Reconfiguration to enhance the security level of cryptography.

Step2: Reduce the key length to 56 bits using PC-1 and generate 16 sub-keys by shifting previous key.

Step 3: By using PC-2 the sub-keys length will be reduced to 48 bits.

Step 4: From the Initial Permutation table the message which is to be encrypted is permuted.

Step 5: This permuted message is now divided into two equal halves L0 and R0.

$$\boldsymbol{Ln = Rn - 1} \qquad (1)$$

$$\mathbf{Rn = Ln - 1 + F(Rn - 1, Kn)} \qquad (2)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

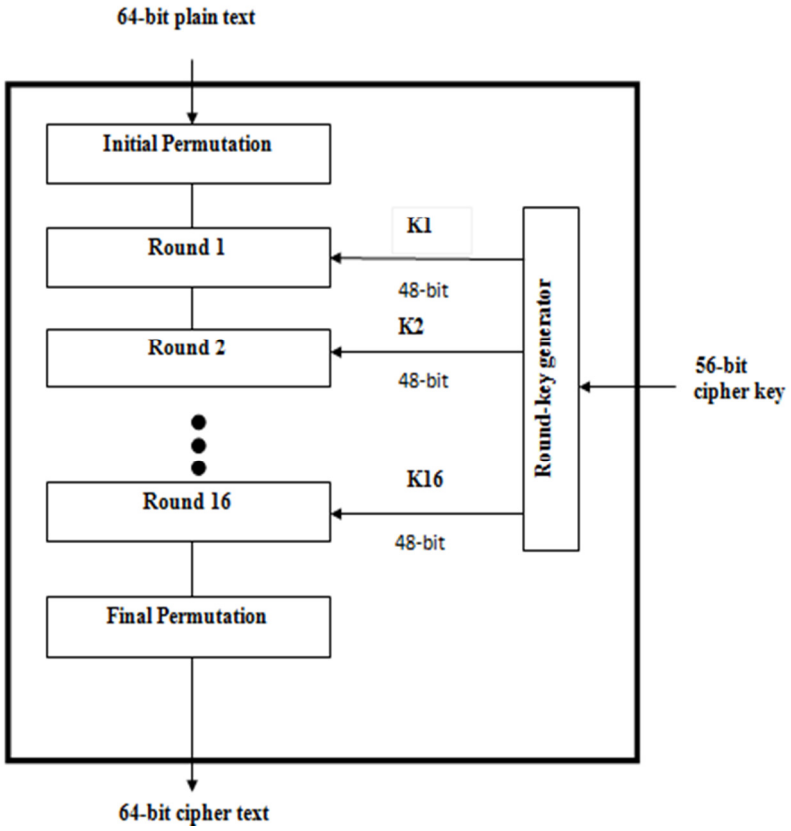


Fig 6: Design Flow Of DES Algorithm

where function F involves in 3 sub-tasks. In first task, expansion of Rn is performed using E-Bit Selection Table. In the next task R_{n-1} is XORedwith Kn (sub-key) whose bit length is 48.In the final task the output from second task is loaded into 8 s-boxes i.e., for each 6 bits.

$$\mathbf{Kn(+)E(Rn-1) = B1B2B3B4B5B6B7B8} \quad (3)$$

where (+) represents xor operation

Each block Bn is given as input to the S-Box as shown below

$$\mathbf{S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)}$$

------- (4)

Step 6: These 8 S-Boxes gives 4 bit output which results 32 bit block. Now this block is considered as Rn. This process is repeated 15 times resulting in the generation of R16 and L16. Concatenation of R16 and L16 generates cipher.

Step 7: Each character in the Cipher is represented in the form of **A,C,G,T**by using codon table.

Step 8: The DNA sequence is converted into mRNA sequence by replacing T with U.Finallyprotein sequence is generated from amino acids which are coded from RNA sequences.

Step 9: Key is divided into two halves Lk and Rk. If the bit length is odd for Lk, pad with 0 and if the bit length is odd for Rk pad with 1. After padding, concatenate Lk and Rk.

Step 10: Consider a dummy key along with the key obtained after padding. Perform XOR operation between key and dummy key.

$$\mathbf{Key *= key + dummy\ key} \quad (4)$$

Step 11: Repeat steps 7-9 for keywhich results in protein form. The protein form is then converted to amino acid form.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Step 12: Concatenate the protein form of cipher and protein form of key to generate the required Cipher.

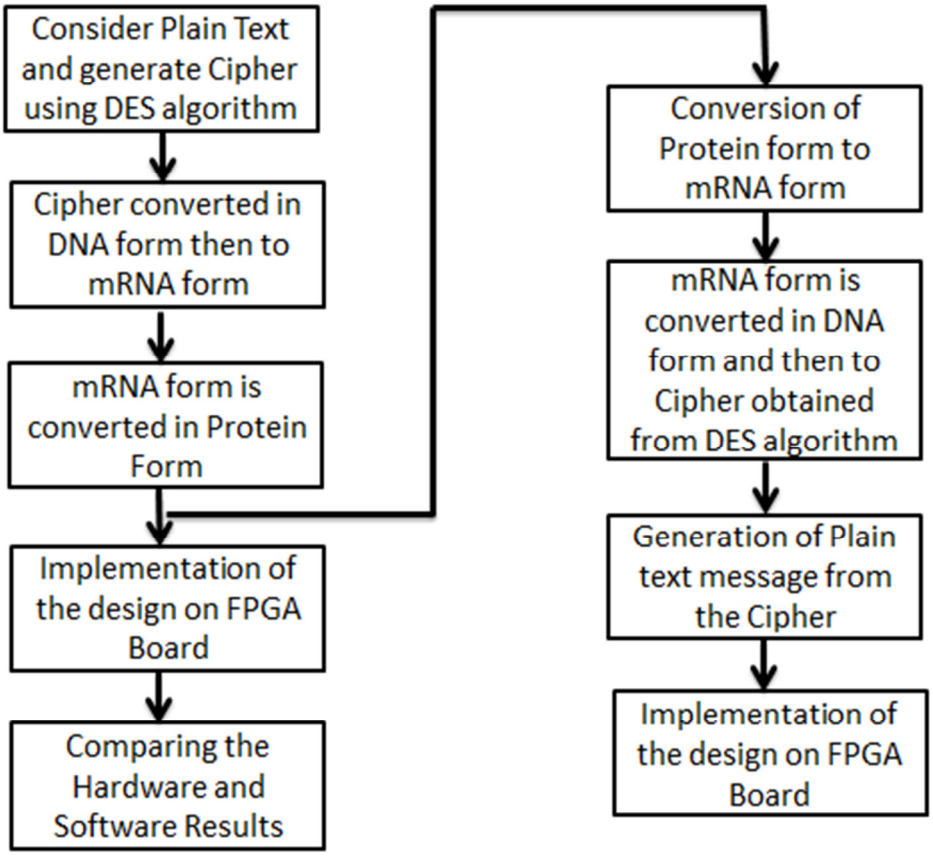


Fig 7: Flow Chart Of Encryption And Decryption For DES Algorithm Using DNA Cryptography.

6. SIMULATION RESULTS AND ANALYSIS

In this section, a lucid analysis of the simulation results has been explained. The comparison between the results shows that proposed algorithm is powerful than existing algorithm regarding security, power consumption and computational speed. As the protein form is very smaller than the bit length and DNA sequence, there is no need of using compression technique.

Simulation result shown in Figure 8 consists of Data, Key, Cipher_DNA, Key_DNA, Cipher Key_Merge. Data represents 64 bit original message, key resembles 56 bit key in hexadecimal form. Cipher DNA is 256 bit sequence which is in m-RNA form, derived from cipher of DES algorithm represented in binary form. Key DNA is 256 bit sequence which is in m-RNA form, derived from key used in DES algorithm. The cipher_key merge is a 528 bit sequence which is obtained by merging protein sequence of cipher and key.

Figure 9 designates the hardware implementation output of DES _DNA cryptography which is implemented on ZED board. It contains OData, OKey of 64 bit size, Cipher DNA and Key DNA of 256 bit size and Cipher_Key 528 bit size. Figure 10 shows the synthesised schema of DES

Journal of Theoretical and Applied Information Technology
31st May 2017. Vol.95. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

algorithm which is generated by synthesizing in Vivado tool.

The placing and routing occupancy of proposed algorithm is shown in figure 11. The occupancy of DES_DNA is less compared to DES algorithm. Figure 12 indicates the Design utilization summary that is produced after post implementation in the Vivado tool.

Figure 13 shows 5% of LUT's are consumed out of total available LUT"s. Only 7% of LUTRAM is used out of total available LUTRAM. The flip-flops used are only 6% out of all. Similarly, BRAM and BUFG are used 24% and 9% respectively. Only 1% of IO's are used overall. Figure 14 shows the physical view of DES_DNA algorithm on zync FPGA architecture.

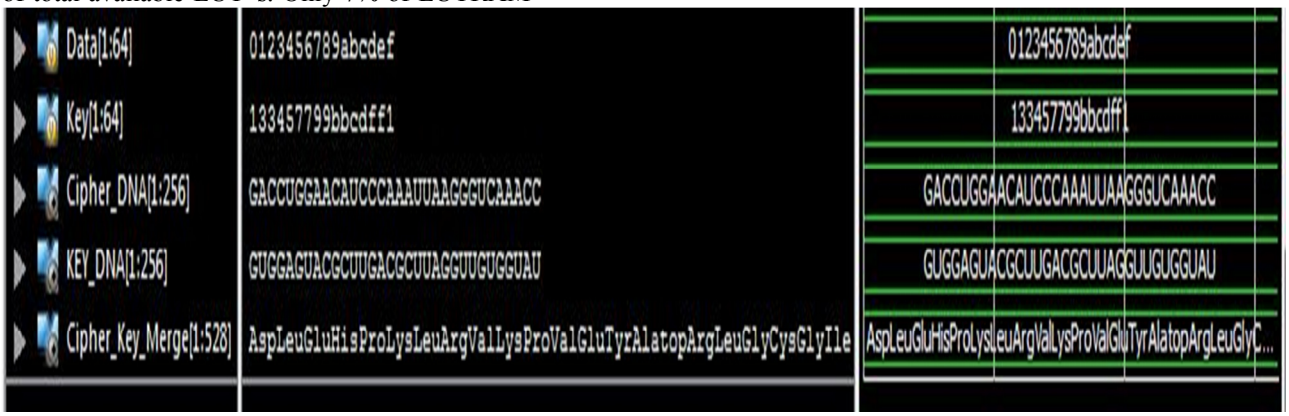


Fig 8: Software Simulation Of DES_DNA Encryption Output Using Xilinx ISE.

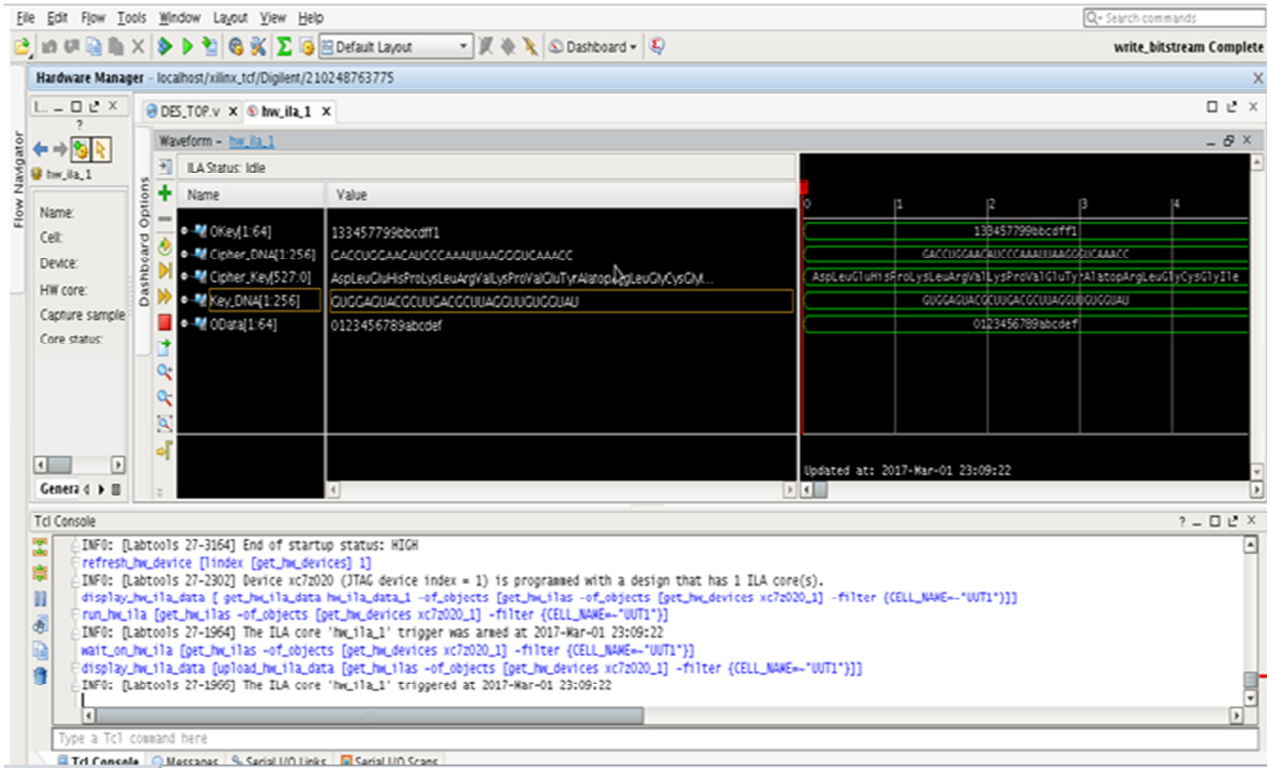


Fig 9: FPGA Implementation Of DES_DNA Encryption Output Using Chip Scope Pro Analysis.

Journal of Theoretical and Applied Information Technology
31st May 2017. Vol.95. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

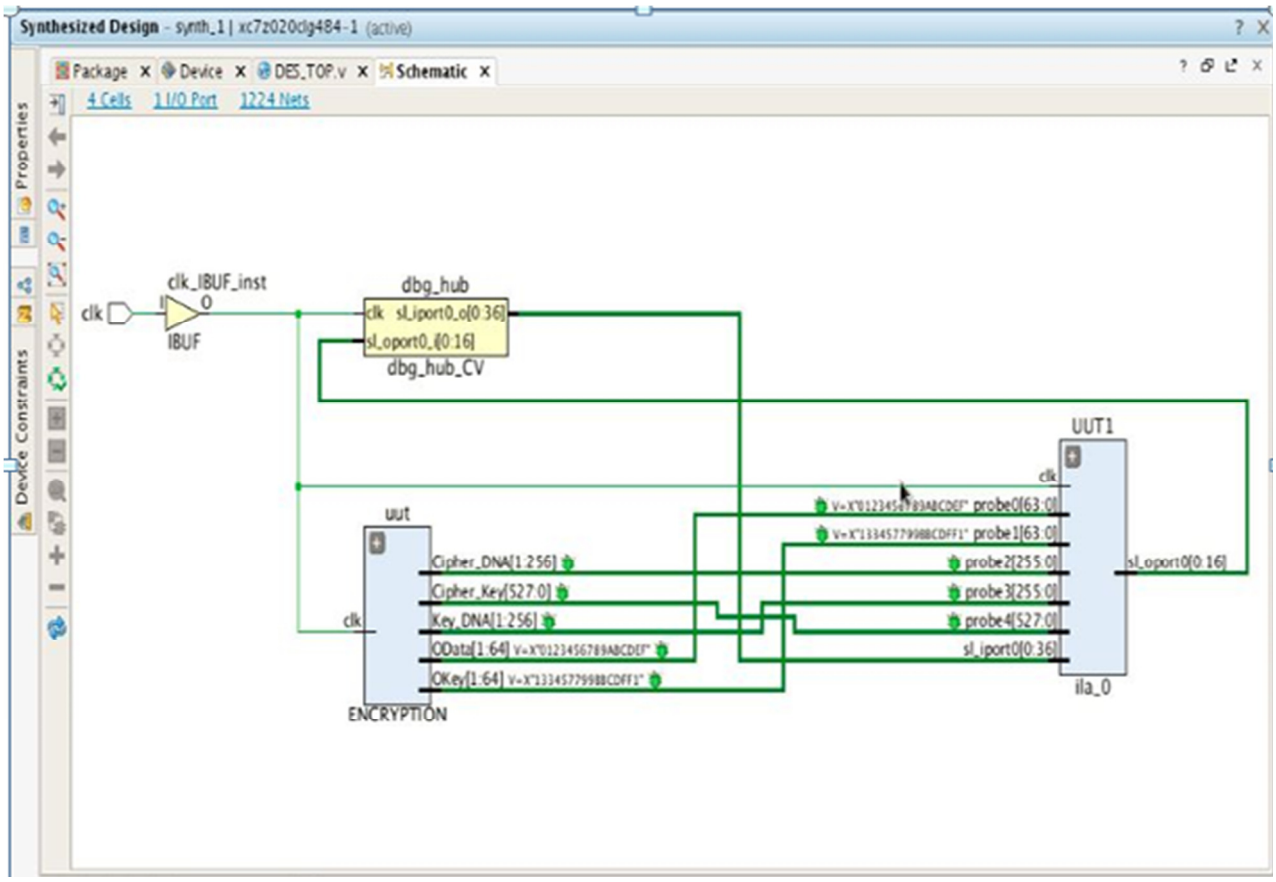


Fig 10: Synthesized Design Of DES Algorithm Using DNA Cryptography With Internal Logic Analyser (Ila).

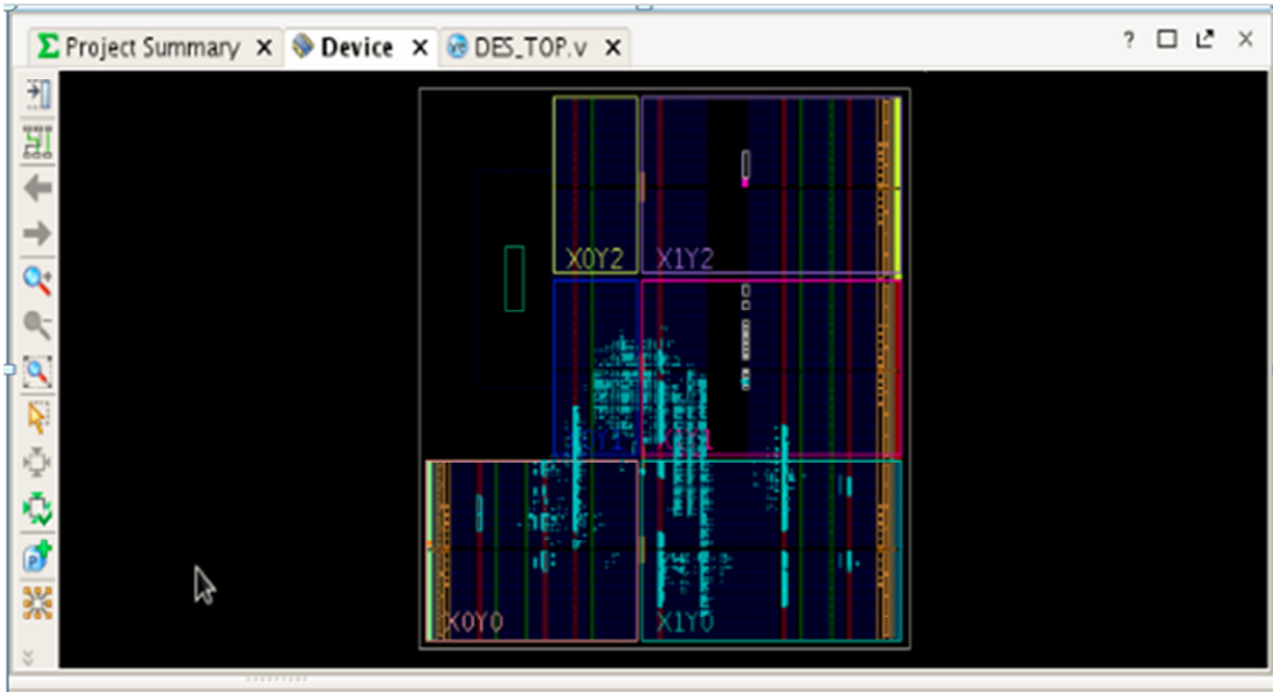
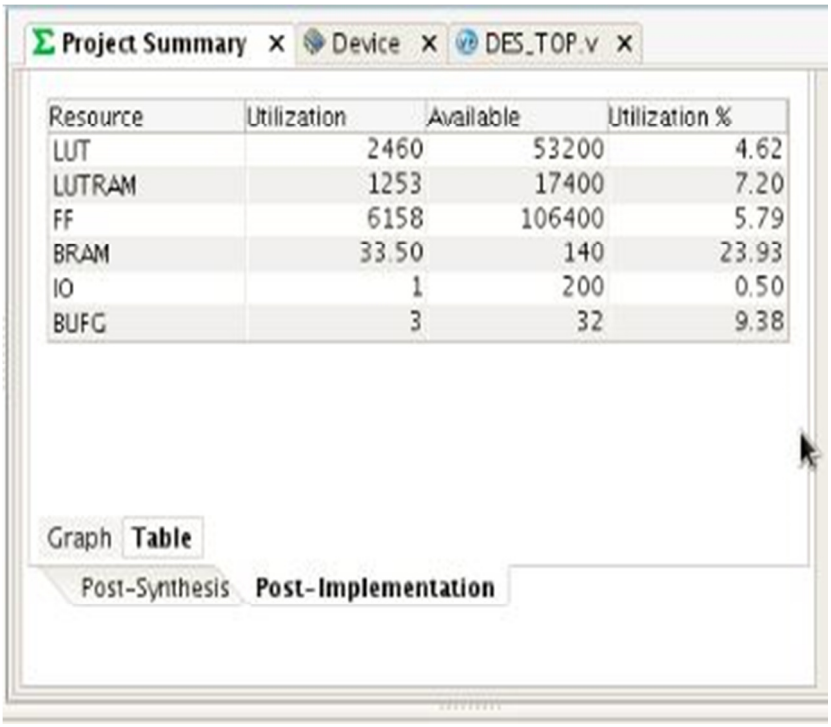


Fig 11: Place And Route Occupancy Of DES Algorithm Using DNA Cryptography.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



Resource	Utilization	Available	Utilization %
LUT	2460	53200	4.62
LUTRAM	1253	17400	7.20
FF	6158	106400	5.79
BRAM	33.50	140	23.93
IO	1	200	0.50
BUFG	3	32	9.38

Fig 12: Device Utilization Summary Of Des Algorithm Using Dna Cryptography.

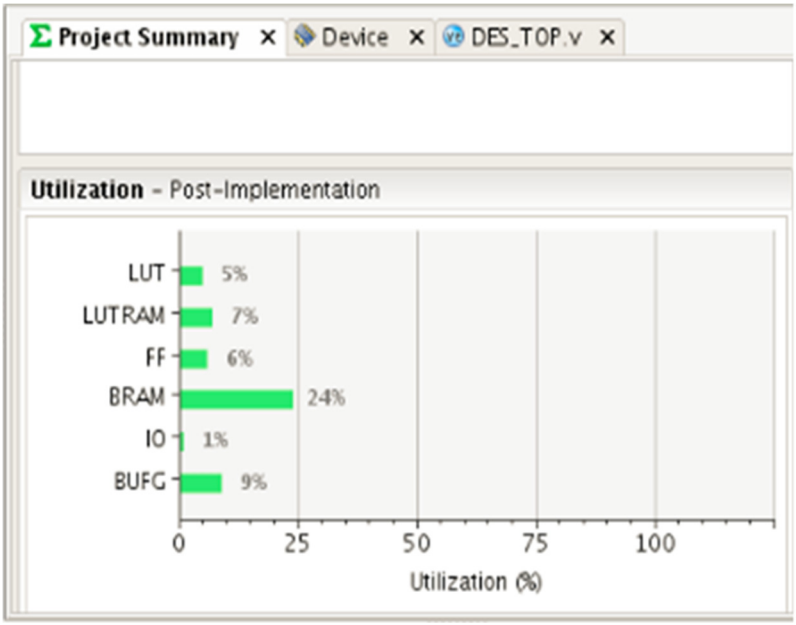


Fig 13: Percentage Of Device Utilization Summary Of DES Algorithm Using DNA Cryptography.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

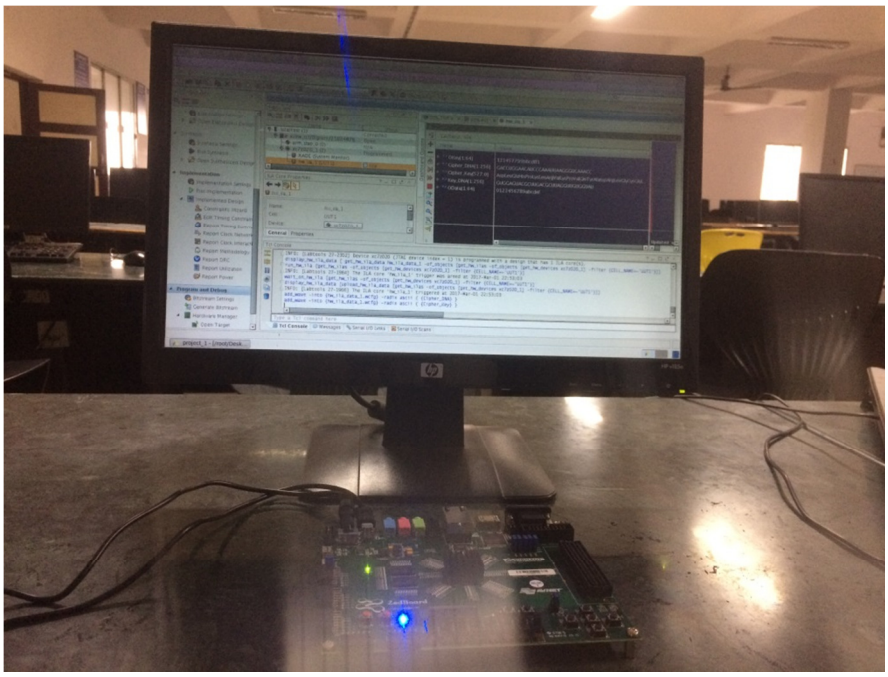


Fig 14: Physical View DES_DNA Algorithm On Zync FPGA Architecture.

Some of the Merits of the proposed work are high Performance rate, Parallel processing, Ability to hold large amounts of info in very small spaces. Regarding the limitations of the work that is carried out the designed cryptosystem is very complex while decrypting when protein form of message is converted into mRNA form since we have to choose the correct nucleotide triplet from the available nucleotide triplets which will be identical. However this increase in the complexity will enhance the security level of cryptosystem.

7. CONCLUSION

The objective of this paper is to deliver a stronger cryptosystem which uses biological conception and notations of DNA cryptography for DES process to perform the encryption and decryption. This paper explores the full procedure of implementing DES algorithm using DNA cryptography which provides higher security than the DES. The advantages of our proposed cryptosystem are it is more secure, reliable and robust. The variation of key using partial reconfiguration ability of system made our proposed method unique when compared with the traditional encryption techniques with DNA sequence. In spite of having handful number of advantages, this technique may lead to high computational complexity.

REFERENCES

[1] Sombir Singh, Sunil K.Maakar, Dr.Sudesh Kumar,"Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, June-2013.

[2] Gurpreet Singh, Supriya,"A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications, April-2013.

[3] Mandeep Singh Narula, Simarpreet Singh, "Implementation of Triple Data Encryption Standard using Verilog", IJARCSSE, Volume 4 Issue 1,January-2014.

[4] Karthik.S, Muruganandam.A, "Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System", International Journal of Scientific Engineering and Research (IJSER), Volume 2 Issue 11, November 2014.

[5] Nirmaljeet Kaur, Sukhman Sodhi, "Data Encryption Standard Algorithm (DES) for Secure Data Transmission", International Conference on Advances in Emerging Technology (ICAET), 2016

.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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

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

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

[9] 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.

[10] Sreeja C.S, Mohammed Misbahuddin, Mohammed Hashim N.P, "DNA for Information Security: A Survey on DNA Computing and a Pseudo DNA Method Based On Central Dogma of Molecular Biology", IEEE 2014.

[11] 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.

[12] I.Rama Satya Nageswara Rao, B.Murali Krishna, Syed Shameem, Habibullah Khan, G.L.Madhumati, "Wireless Secured Data Transmission using Cryptographic Techniques through FPGA", International Journal of Engineering and Technology (IJET), Vol 8, No 1, Feb-March 2016.

[13] U.Noorul Hussain, T. Chithralekha, A.Naveen Raj, G.Sathish, A.Dharani, "A Hybrid DNA Algorithm for DES using Central Dogma of Molecular Biology (CDMB)", International Journal of Computer Applications (0975 – 8887) Volume 42– No.20, March 2012.

[14] Solomon Raju Kota, Ashutosh Gupta, Shashikant Nayak, and Sreekanth Varma, "Module Based Implementation of Partial Reconfiguration Using VHDL on Xilinx FPGA ",International Journal of Recent Trends in Engineering, Vol 2, No. 7, November 2009.

[15] Wang Lie, Wu Feng-yan, "Dynamic partial reconfiguration in FPGAs",Third International Symposium on Intelligent Information Technology Application, 2009.

[16] Sheetal U. Bhandari, Shaila Subbaraman, Shashank Pujari, Rashmi Mahajan, "Internal dynamic partial reconfiguration for real time signal processing on FPGA", Indian Journal of Science and Technology Vol 3 No. 4, April 2010.