International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 10, October 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

Implementation of Three Fish Cipher Algorithm to Achieve Secured Communication

Vadthyavath Vijaya[1*], Ramavath Anusuria[2]

[1*]*Department of Electronic Communication Engineering, Sreyas Institute of Engineering and Technology, Hyderabad, Telangana, (India)*

[2]*Asst. Professor, Department of Electronic Communication Engineering, TKRCET, Telangana, (India).*

ABSTRACT

The prime requirement of everyone is to see the secure communication in our life. Now a day's the security has became utmost aspect of life. Password can be used like, numbers, letters and biometrics with cryptography technique. In this report various encryption and description algorithms were studied, description standard data is used for data security and implementation of Three-Fish Cipher algorithm with minimum number of overheads and then compile, simulate and test with the help of Xilinx ISE software and compare the proposed work with test bench.

Key Index: Secure communication, Three-Fish Cipher algorithm, Xilinx ISE software.

INTRODUCTION

Data Encryption Standard is the most well-known cryptographic mechanism [1]. In the history came in 1976 when Diffie and Hellman published a transaction [2]. It begins with the work of Feistel at IBM in the early 1970s. Ruth M. Davis [3] provides a hardware-implementable algorithm for enciphering data, which has been adopted as a Federal standard to provide a high level of cryptographic protection against various attacks. Whitfleld Diffie et. al [4] describes cryptographic technology, which examines the forces driving public development of cryptography. Ingrid Verbauwhede [5] described Security and Performance Optimization of a New DES Data Encryption Chip. James E. Katz [6] provides Social Aspects of Telecommunications Security Policy for privacy and of society for security. H. Bonnenbergt [7] described the VLSI implementation of a new block cipher. K.H. Mundt [8] presented superscript ASIC get 100Mbits/ s encryption speed on silicon applying 1 micron design rules. C. Boyd [9] provides the modern data encryption in which proposed standard for digital signatures based on RSA were introduced. R. Zimmermann et. al. [10] provides a 177 Mb/s VLSI implementation of the International Data Encryption Algorithm. Stefan Wolter [11] provides the implementation of the IDEA architecture that includes a concurrent self-test based on a mod3 residue code self-checking system. Seung-Jo Han [12] describes the improved DES algorithm in which a 96-bit data block is divided into three 32-bit sub-blocks. Hassina Guendouz et. al. [13] describes rapid prototype of a fast data encryption standard with integrity processing for cryptographic applications. K. Wong [14] performed transform domain analysis of DES algorithm by using tool. M.P. Leong [15] described a bit-serial implementation of the International Data Encryption Algorithm (IDEA). R. G. Sixel et. al. [16] describes a high level language implementation of the DES and bit-slice architecture. Teo Pock Chueng [17] provides implementation of pipelined DES using Alter

CPLD. Yeong-kang lai et. al. [18] represented the VLSI architecture design and implementation for two fish block cipher Toby Schaffer et. al. [19] describes an integrated design of Advanced Encryption Standard (AES). Cameron Patterson [20] provides high performance DES encryption using Vertex FPGA. Jbits. Pui-Lam Siu et. al. [21] presented about the A Fault Attack on pairing based Cryptography Current fault attacks against public key cryptography focus on traditional schemes.

SECURED COMMUNICATIONS

Secured communication against network is increasing significantly with time. Our communication media should also be secure and confidential. Cryptanalysis is the study used to describe the methods of code-breaking or cracking the code without using the security information, usually used by hackers. For this purpose, the following things can be done by the sender/receiver.

- One can transmit the message secretly, so that it can be saved from hackers.
- The sender ensures that the message arrives to the desired destination.
- The receiver ensures that the received message is in its original form and coming from the authenticate person.

The confidentiality of information that cryptography can provide is useful not only for the legitimate purposes of preventing information crimes e.g. the theft of trade secrets or unauthorized disclosure of sensitive medical records but also for illegitimate purposes e.g., shielding from law enforcement officials a conversation between two terrorists planning to bomb a building. In order to achieve the same one can use two techniques, (i) one can use invisible ink for writing the message or can send the message through the confidential person, and (ii) use of scientific approach called "Cryptography". The fundamental and classical task of cryptography is to provide confidentiality by encryption methods. It is used in applications present in technologically advanced societies; it includes the security of ATM cards, computer passwords, and electronic commerce.

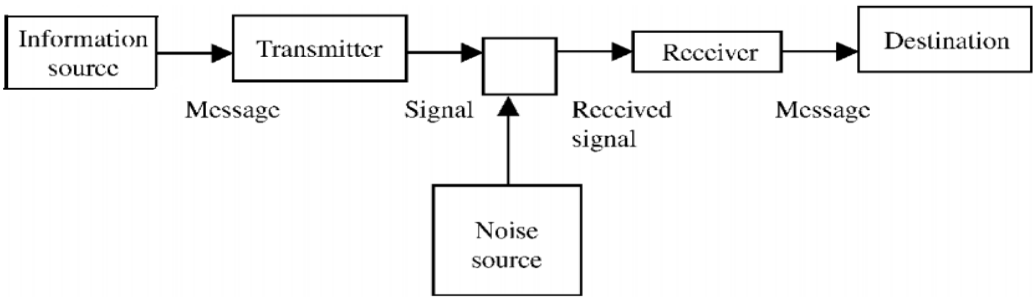

Fig.1. Schematic Model diagram of Secured Communication

But the most recognized form of cryptography is its use encipher and decipher information, thus keeping its contents guarded against unauthorized disclosure. There are two classes of key-based encryption algorithms: symmetric and asymmetric algorithms. Symmetric algorithms use the same key for encryption and decryption, whereas asymmetric algorithms use different keys for encryption and decryption. Ideally it is infeasible to compute the decryption key from the encryption key.

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 10, October 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

CRYPTOGRAPHY

It is a technique used to avoid an unauthorized access of data. It helps to provide accountability fairness and accuracy and also provide confidentiality. Broadly, four different kinds of people contributed their efforts in this technique and are: (i) Military, (ii) The Diplomatic Corps, (iii) Diarists, and (iv) Communications System.

Cryptography involves two basic operations and is named as encryption and key management. Information/data can be encrypted using a cryptographic algorithm by various keys. The security of cryptographic system is not only dependent on the encryption algorithm; it also depends upon the keys used for the encryption. These keys area always kept secured from the hacker and are known as secret key. Key plays an important role in encryption process, which is a main part of cryptography. Due to channel impairments sometimes the transmitted data and/or key may get corrupted. If it is slightly changed or corrupted, the data will not be recovered; therefore, key needs to be transported over the secured channel. The frequency of use of a cryptographic key always has a direct correlation to how often the key should be changed. Encryption algorithms can be hacked by utilizing supercomputer which provides fast speed and allows the hacker to use more permutations and combinations in a specified time. Modern era depends upon wireless communication and almost all the electronic funds are being carried out online. In order to protect the same and maintain the privacy of the users; cryptography is the best solution due to their better response even in the presence of advisory. For better security, either more number of keys is used or the length of the existing keys is increased. In both the approaches the overheads are increased, therefore, the best idea is to use sub-keys. Sub-keys are used only for such nodes which are attacked by the hacker.

The sub keys are always derived from the main key which helps in reducing the overheads. The basic cryptographic model has been shown in figure 1.1. It involves encryption and decryption section; initially, the data has been encrypted by the help of key and further transmitted over the web. Finally, it has been received and the encrypted data is decrypted with the help of same or different key. The key is any value and/or word and is used in both the sections for encryption and decryption purpose.

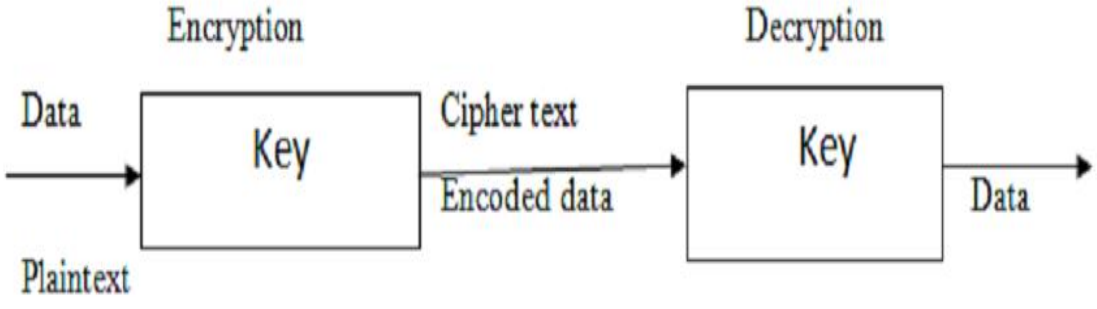

Fig.2. Schematic diagram of Basic Cryptographic Model

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 10, October 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

RESULTS AND CONCLUSION

Following are simulated results of three fish block cipher algorithm implemented in virtex-5 kit with the help of Xilinx ISE 12.1.

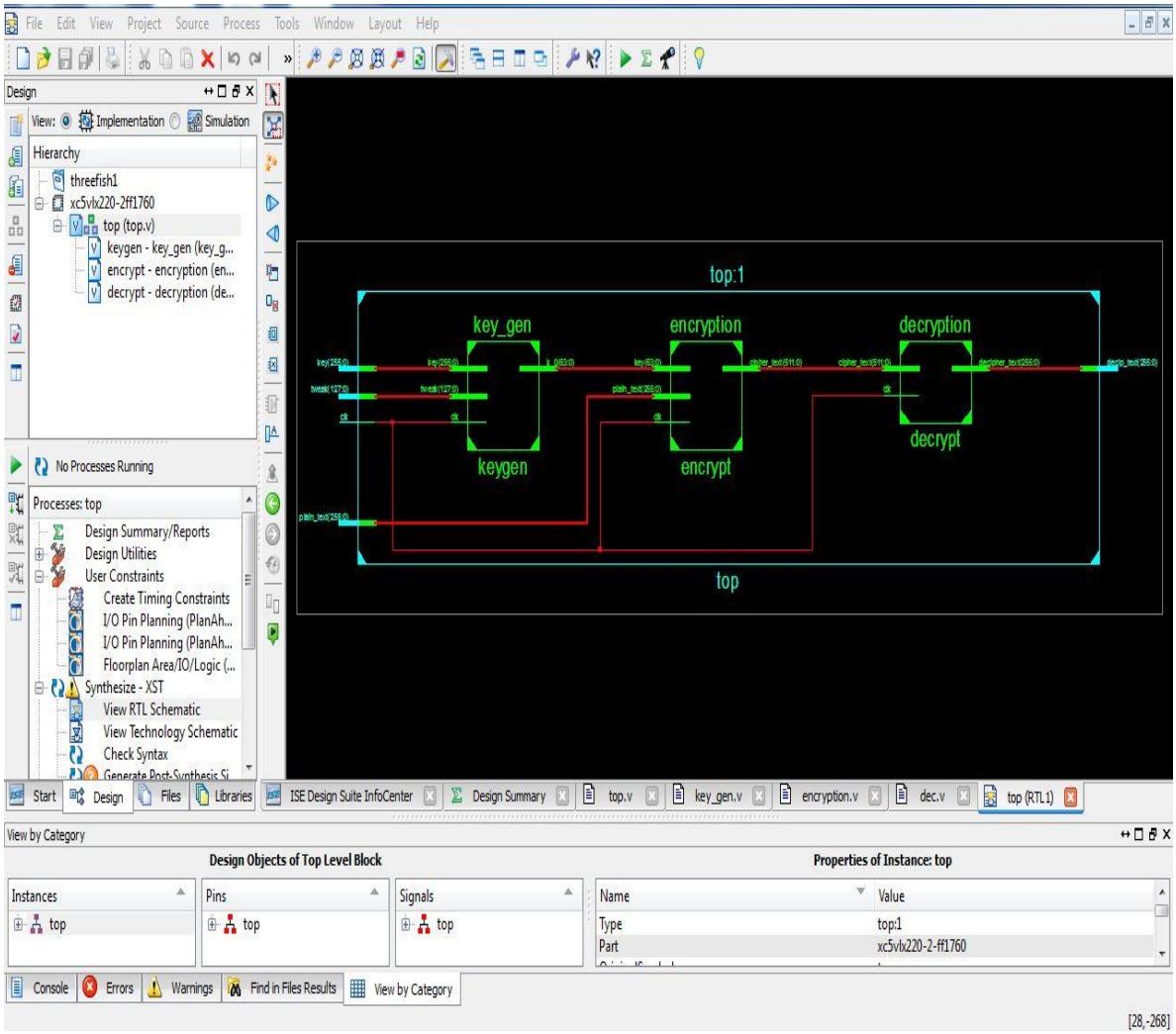

Fig.3. Block Diagram of Three Fish Cipher In Xilinx

The figure shows block diagram of encryption decryption and key scheduling blocks with plaintext as input, key K and tweaked input and cipher text as output from encryption block and deciphered text is obtained as output from decryption block.

Key scheduler tweaked input and plain text:

key = 256'h3663586286256862856826862927927979725766427497942492752237 32;

tweak = 128'h93448681648614681648618468126486;

plain_text =256'h9856734567834255664368568346568365468685636485686385683654863856;

Following shows ciphered text as output:

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 10, October 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

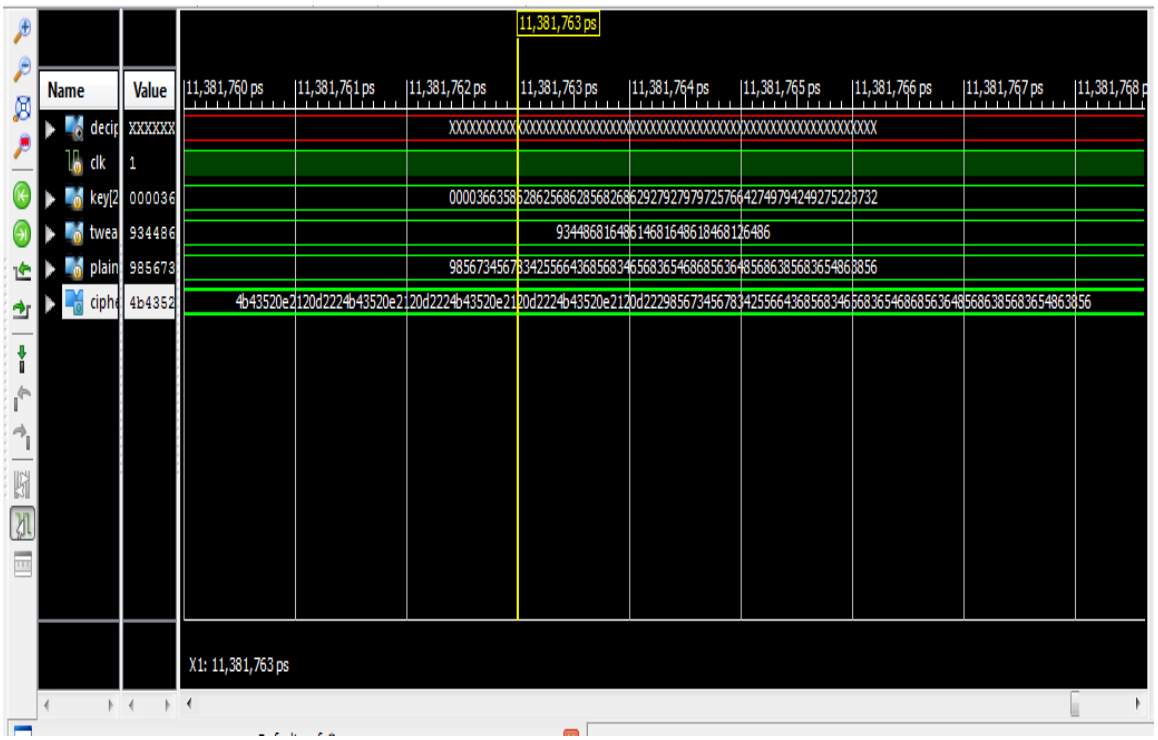

Fig.4 Ciphered Outputs

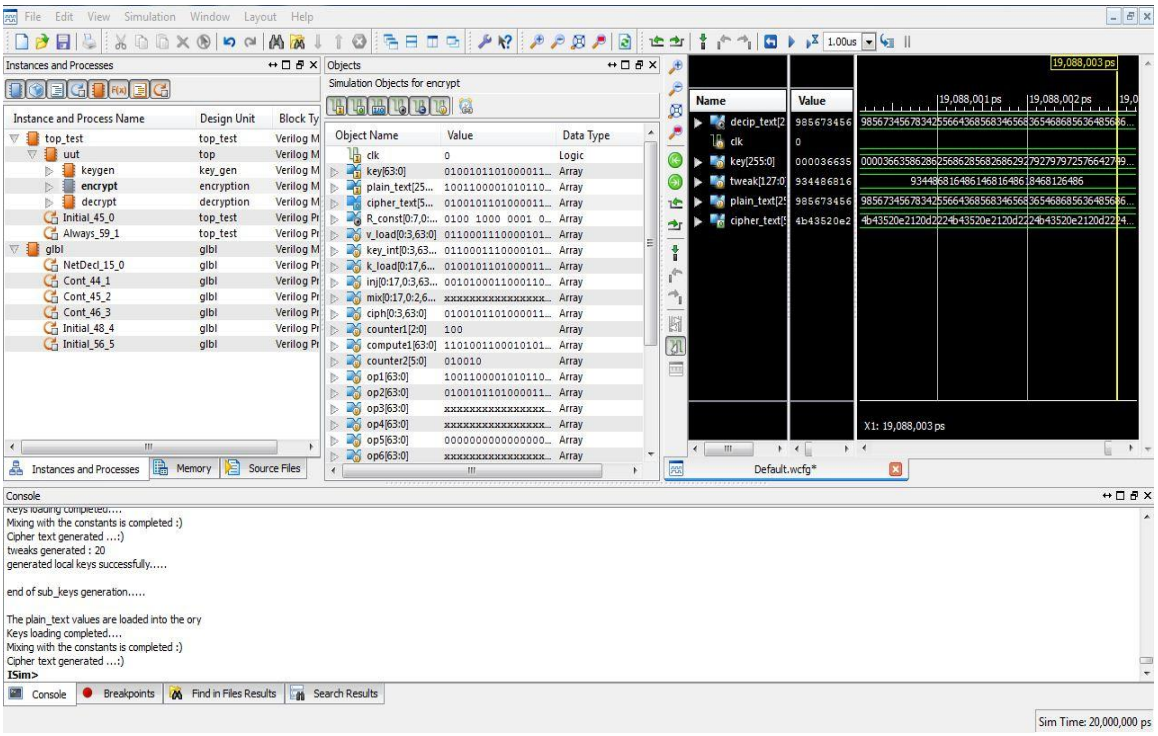

Fig.5. Deciphered Outputs

CONCLUSION

- The information security can easily be achieved by cryptography algorithm techniques a large number of encryption algorithm have been developed for securing confidential data from the cyberpunks. The aim of current Cryptography is to prevent data from hackers. The strength of the system is dependent on the length of the key. But to achieve this a large computational time is required, giving a large delay which can be harmful to us.
- The use of FPGAs can help us to improve this limitation because FPGAs can give enhanced speed. This is due to fact that the hardware implementation of most encryption algorithms can be done on FPGA. The proposed scheme for three fish cipher algorithm has been optimized on the time required to generate the keys or decode data. The algorithm and coding has been implemented on Xilinx ISE software with the help of Verilog HDL language. The synthesis has been done on Xilinx FPGA (Xilinx 12.1c) and the faster clock frequency has been observed in comparison with classical DES.
- It has been observed that it takes 19 nanoseconds for the input data of size 8 bytes while the technique by which the algorithm has been implemented in this thesis using Verilog HDL has reduced the time to 14.2 nanoseconds for 32bytes. The improvement has been observed to be 45.78% as compared to classical DES technique.

REFERENCES

[1] Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, Jesse Walker, "The Skein Hash Function Family (Version 1.3)", Oct 2010.

[2] D. Kahn: The Code breakers: the story of secret writing, MacMillan publishing,1996.W.Diffie and M. Hellman, "New Directions in Cryptography", IEEE Transaction on Information Theory, Vol. IT-22, 1976, pp. 644-654.

[3] Ruth M. Davis, "The Data Encryption Standard", Proceedings of Conference on Computer Security and the Data Encryption Standard, National Bureau of Standards, Gaithersburg, MD, 1977, NBS Special Publication 500-527, pp 5-9.

[4] Whitfleld Diffie, "Cryptographic Technology: Fifteen Year Forecast" Reprinted by permission AAAS, 1981 from Secure Communications and Asymmetric Crypto Systems. AAAS Selecte8 Symposia. Editor: C.J. Simmons. Vol. 69, West view Press, Boulder, Colorado, pp 38-57.

[5] Ingrid Verbauwhede, "Security and Performance Optimization of a New DES Data Encryption Chip", IEEE journal of Solid-State Circuits, Vol. 23, No. 3.1988, pp 647-656.

[6] James E. Katz, "Social Aspects of Telecommunications Security Policy", IEEE journal Technology and Society Magazine, 1990, pp 16-24.

[7] H. Bonnenbergt, "VLSI Implementation of a New Block Cipher", IEEE journal on Information Theory 1991, pp 510-513.

[8] K.H. Mundt, "SUPERCRYPT, ASIC Technology facilitates a new Device Family for Data Encryption", IEEE journal on cloud computing 1992, pp 356-359.

[9] C. Boyd. "Modern Data Encryption," Electronics & Communication Engineering Journal on data security and neural networks 1993, Vol. 5, pp 271-278.

[10] R. Zimmermann, "A 177 Mb/s VLSI Implementation of the International Data Encryption Algorithm", IEEE Journal of Solid-State Circuits. Vol. 29, No. 3, 1994, pp 303-307.

[11] Stefan Wolter "On the VLSI Implementation of the International Data encryption Algorithm IDEA", IEEE journal on computer system and data security 1995, pp 397-400.

[12] Seung-Jo Han, "The Improved Data Encryption Standard (DES) Algorithm" IEEE journal on information system 1996, Vol. 3, pp 1310-1314.

[13] Hassina Guendouz, "Rapid Prototype of a Fast Data Encryption Standard with Integrity Processing for Cryptographic Applications", IEEE transaction on data originations 1998,pp 434-437.

[14] K. Wong, "A Single-Chip FPGA Implementation of the Data Encryption Standard (DES) Algorithm" Global Telecommunications Conference, 1998. GLOBECOM 98, IEEE, Vol. 2, pp. 827-832.

[15] M.P. Leong, "A Bit-Serial Implementation of the International Data Encryption Algorithm IDEA", 2000 IEEE conference Symposium on Field-Programmable Custom Computing Machines, pp 122-131.

[16] R. G. Sixel, "A High Level Language Implementation of the Data Encryption Standard and a Bit-Slice Architecture", Roc 43rd IEEE Midwest Symposium on Circuits and Systems, Lansing MI, 2000, pp 266-269.

[17] Teo Pock Chueng, "Implementation of Pipelined Data Encryption Standard (DES) Using Altera CPLD", TENCON 2000 Proceedings, Vol. 3, IEEE 2000, pp 17-21.

[18] Yeong-Kang Lai, "A Novel VLSI Architecture for a Variable-Length Key, 64-Bit Blowfish Block Cipher", Signal Processing Systems, 1999 IEEE Workshop, pp 568-577.

[19] Toby Schaffer, "A Flip-Chip Implementation of the Data Encryption Standard (DES)", IEEE1997, pp 13-17.

[20] Cameron Patterson, "High Performance DES Encryption in Vertex FPGAs using Jbits", journal Symposium on FPGA 2000, pp 113-121.

[21] Cameron Patterson, "High Performance DES Encryption in Vertex FPGAs using Jbits", IEEE journal Symposium on FPGA 2000, pp 113-121.