iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 Issue: VII Month of publication: July 2016

DOI:

Volume 4 Issue VII, July 2016
ISSN: 2321-9653

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Design and Implement Dynamic Key Generation to Enhance DES Algorithm.

Priyanka K. Babar[1], Vishal P. Bhope[2]
Electronics and Telecommunication Department, Pune University

Abstract— Cryptography is the process of transforming message to avoid an unauthorized access of data. Key is an important part in cryptography. For higher level of secure communication key plays an important role. For increasing the level of security in any communication this project proposed a Dynamic key generation unit. Dynamic key generation enhances the DES algorithm securities. As per the research done DES algorithm is weak due to its weak key generation, so that key generation can be reconfigured. Therefore to make key generation more effective and strong dynamic key generation unit is proposed here which is totally independent on DES algorithm. The system proposed here three ways to make key generation more stronger are user generated key, second one by using LFSR which is good key stream generator, third is by using chaotic encryption and fourth is 2's complement. This system also has good resistance against brute-force attack which makes system more effective. Another part is DES algorithm and control unit is also designed for controlling the round of DES for encryption and decryption.

Keywords— Cryptography, Dynamic Key Generator, LFSR, Chaotic encryption, 2's complement

I. INTRODUCTION

Cryptography is the process of secret writing means scrambling the data which is not in readable format. The need of cryptography is arises to protect the private information from unauthorized person. There are different goals of cryptography like confidentiality, authentication, integrity, non repudiation, access control etc. Data is encrypted by using various cryptographic algorithms [10]. Security of the data or system is depends on both cryptographic algorithm and key used for encryption/decryption. Cryptography is needed in various sectors like banks, military, railways, telecommunication etc. In electronic fund transfer like ATM cards, computer passwords, electronic passwords also require the security. Cryptography has wide area of scope because this technique has ability to provide security against various attacks. Cryptography mainly includes two parts i.e. encryption and decryption, encryption is the process of converting of plain text (readable) to cipher text (unreadable) and decryption is the process of converting cipher text (unreadable) to plain text(readable) as shown in figure 1.

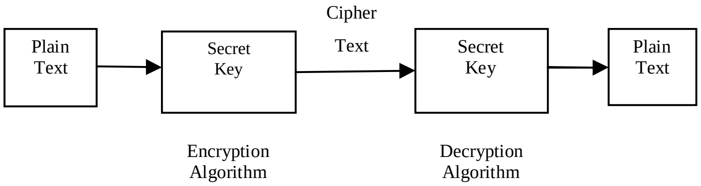


Fig.1 Block diagram of cryptography

There are two types of encryption algorithms based on the type of key used are:

A. *Symmetric*-use the same key for encryption and decryption.

B. *Asymmetric- use the different keys for encryption and decryption.*

There are different types of cryptographic algorithms based on the type of key used: AES, DES, TDES, RC2, RC6 are symmetric key algorithms and Diffie-Hellman, RSA, DSA are asymmetric key algorithms. The DES (Data Encryption Standard) algorithm is a block cipher operates on the 64-bit plain text which uses the same key for both encrypt and decrypt data blocks [12]. 64-bit key produces the 64-bit encrypted cipher text from 64-bit plain text and for decryption same process is done in reverse. The DES algorithm is weak due to its key generation therefore to enhance the DES algorithm we proposed a dynamic key generation due to that security level of DES algorithm is get increased at higher level and implementing it using FPGA. This proposed work is done mainly in two parts first one is DES algorithm and second one is dynamic key generation.

The rest of the paper is organized as follows. Section II includes literature survey. Section III includes system development. Section IV explains proposed system. Section V includes simulation results and Section VI includes conclusion.

II. LITERATURE SURVEY

Literature survey includes the various researches done by the various researchers for enhancing the cryptographic algorithm securities for secure data communication.

In paper" A Novel approach for data encryption standard algorithm" by the author prashanti.g, deepthi.s, sandhya rani.k[4]. Proposed a new method to enhance the DES algorithm by replacing the 8/32 S-Box by 6/4 S-Box and then followed by the AND and XOR operations before going to permutation. It also includes the new operation of modulo-2 operation during the 16 round instead of regular XOR operation. It also proposes the modified s-box operation to improve the security level in banking sector by replacing the XOR operation which improves the implementation. This improves the performance of the DES algorithm and security level also gets improved.

In paper "A reconfigurable block cryptographic processor based on VLIW architecture" by LI Wei, ZENG Xiaoyang , NAN Longmei , CHEN Tao , DAI Zibin [6] proposed a reconfigurable VLIW processor for block-cipher processing and for block-cipher proposes multi-cluster register file structure. For element operation of block ciphers it uses the reconfigurable units for multiple cryptographic processing units. Proposed system is not only able to do cryptographic operations but also used to do dynamic configurations for cryptographic processing unit. The comparison of various encryption algorithms and the analysis is the proposed design has highest throughput compared to other which enhances the performance and security level get increased.

In paper "Hardware Implementation of DES Using Pipelining concept with Time-Variable Key" of 22nd international conference on microelectronics [9] includes two implementations of high performance reconfigurable hardware of the DES algorithm by using pipelining concept and time variable key. Counter is used in first concept to change key with every clock cycle and in second pseudo random generator is used. Due to time variable key the security of the DES algorithms is enhanced due to which it is very difficult to hack the data by the hackers.

In paper "Area efficient universal cryptography processor for smart cards" of IEEE transactions on VLSI system [4] proposed a cryptography circuits for smart cards and portable electronic devices for secure data communication. This circuit is small in size, requires low power and provide high performance for several cryptographic algorithms. This paper presents a hardware implementation of three standard cryptography algorithms on a universal architecture.

In paper "Performance analysis of multiple keys used for data security" by Hitesh Mittal and Ajay Kakkar [11] includes the importance of dynamic key generation for secure data transmission and performance analysis of keys used in various cryptographic algorithms for data security as it is an essential component of an organization in order to keep the information safe from hackers, it helps to keep the privacy of the data.

III. SYSTEM DEVELOPMENT

A. DES algorithm description

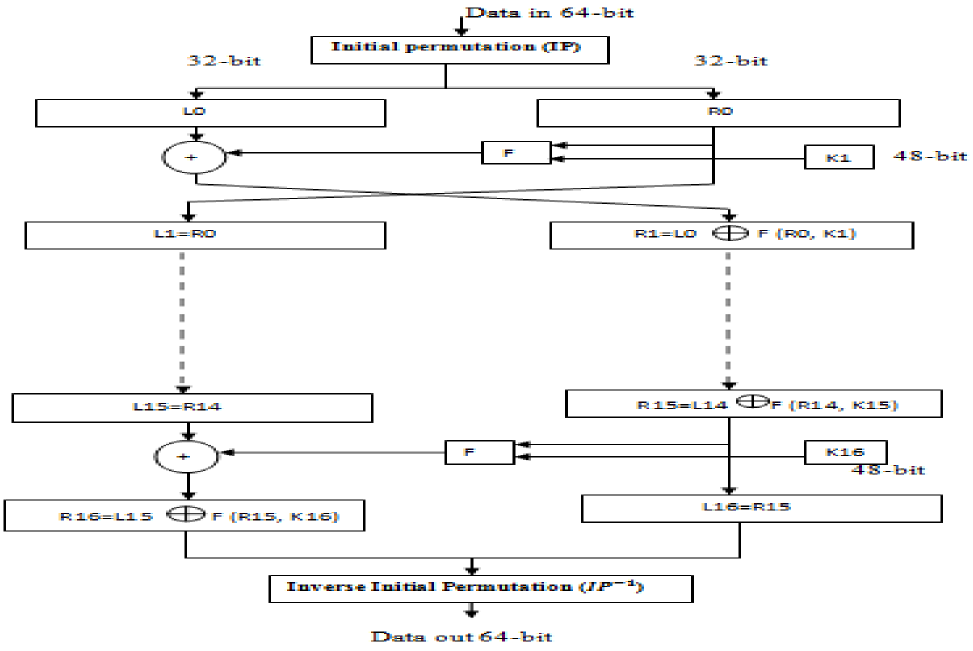


Fig. 2 DES algorithm description.

DES (Data Encryption Standard) algorithm is a block cipher algorithm which uses symmetric key cryptography. It uses 64-bit key for both encrypt and decrypt 64-bit plain text and cipher text respectively. DES algorithm description is as shown in figure 2 [3].It works on 64-bit plain text to produce 64-bit cipher text therefore 64-bit plain text is given as data input to perform initial permutation (IP) first then key dependent permutation and at last final permutation which is inverse initial permutation i.e.IP^{-1} DES algorithm performs 16-rounds of operation to produce 64-bit output data. The implementation of DES requires four basic operations mainly XOR, shift, LUT (Look up table) and permutation which are simple to implement in hardware. As shown in figure 3, 64-bit data input is initially get permuted by IP and then get splits into two equal parts right half (R0) and left half (L0), each is 32-bit in length. Right half in first round will be the left half of the next round and right half of next round is obtained by firstly expanding 32-bits to 48-bits by using expansion function in that we expand it by repeating some bits then this expanded 48-bit are XORed with 48-bit key and then results fed into eight 6-bit substitution boxes (S-boxes) which converts 48-bit input to 32-bit output i.e. 6-bit s-box gives 4-bit output to form 8 4-bit boxes and finally permutation is done on these 32-bits. In next stage this 32-bit permuted output is get XORed with first right half 32-bits to get next right half 32-bits [1].

Function F in the key dependent permutation is the most important function of the DES algorithm and its operation is as shown in figure 3.Different operations like expansion, substitution, permutation and also XOR operation with the 48-bit key are takes place.

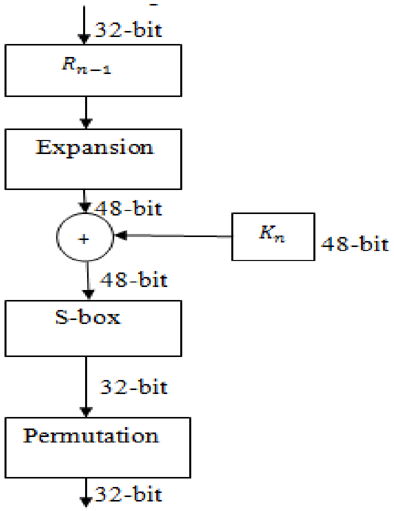


Fig. 3 DES function F details

B. *Linear feedback shift register*

LFSR is a good stream generator. A LFSR consist of shift register and a linear feedback function as shown in figure. In that shift register is a sequence of M flip flops B_M to B_{M-1} and each flip flop holds single bit. Flip flops are initialized to an M-bit word. B_M is a linear function of B_0,B_1,B_2,…..,B_{M-1}. LFSR is divided based on the type of inputs and outputs. Here LFSR is used to generate sequence of keys.

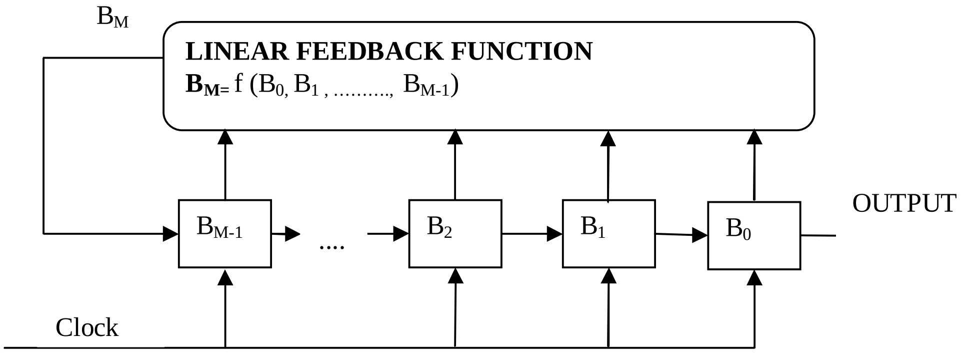


Fig. 4 Block diagram of linear feddback shift register

C. *Chaotic encryption*

In chaotic encryption 'chaos' means 'a state of disorder'. Here system uses one dimensional chaotic signal which is used to mask useful information and make it unrecognizable by attackers. To obtain high level of security chaotic encryption is used to encrypt digital data. Here specifically system uses piecewise linear one dimensional chaotic map (PWLCM) [13]. This system has more and more complex dynamics there fore it has wide applications in the field of communication. So the piecewise linear one dimensional chaotic map is used for dynamic key generation unit. It's equation is as follows:

$$x_{n+1} = \begin{cases} 1 + 2x_{n,} & \text{for } x_n < 0 \\ 1 + 2x_n, & \text{for } x_n \geq 0 \end{cases} \qquad \text{.......................... (1)}$$

Sequence is produced by logistic map. It is non-periodic and convergence under initial condition. Chaotic sequence is not pseudo-random, but truly stochastic, so strong key is get generated using these characteristics.

D. 2's complement

This can be also the another option used to generate more combinations of keys. It's equation is as follows:

$$\text{2's complement} = \text{1's complement} + 1 \qquad \text{.......................... (2)}$$

$$\text{1's complement} = (2\text{^}n) - N$$

IV. PROPOSED DESIGN

A. Dynamic key generation unit

According to kerckhoff's principle, the resistance of the cipher to attack is based on the secrecy of the key. According to this the guessing the key should be so difficult that there is no need to hide the encryption and decryption algorithms, but in DES algorithm, 56 bit key is the main weakness because there are now 2^{56} possible keys are available which are easily get crack by "brute force attacks". It involves trying all 2^{56} keys out of that 4 are weak, 12 are semi weak and 48 are possible weak keys. So to improve the performance of the DES algorithm and enhance security we have to increase number of possible ways of key generation. We proposed a dynamic key generation unit in DES to increase number of possible ways of key generation. In this dynamic key generation unit it includes two blocks i.e. key generated by user and LFSR. By using key generated by user there are 2^{56} possible keys are available but after shifting through LFSR there are more 2^{56} keys are get generated means finally there are total 2^{112} ways are available. For making more confusion in key generation it can be generated by any of the above method.

To increase number of ways of key generation more than 2^{56}, we proposed a dynamic key generation in DES. As shown in figure dynamic key generation unit consist of four blocks named direct key, LFSR, chaotic encryption and 2's complement. Here we are not going to give the original key input to the chaotic encryption block; chaotic encryption block generates the different combinations of keys automatically at each clock cycle.

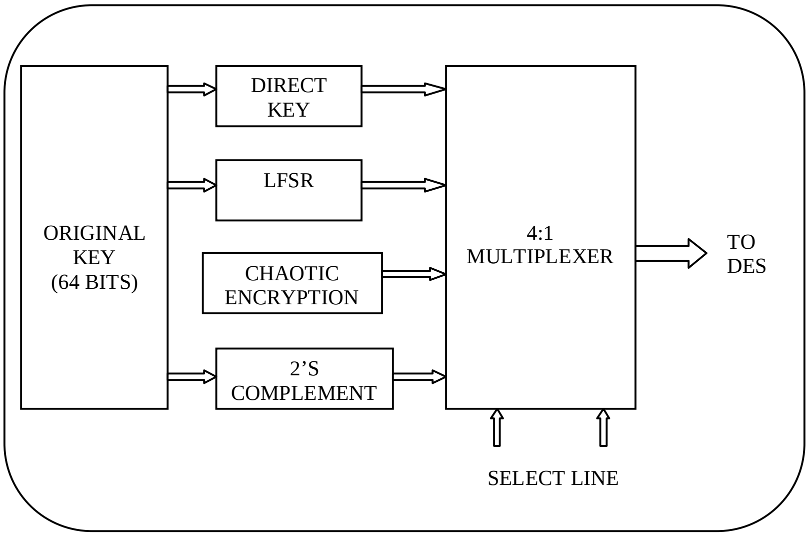


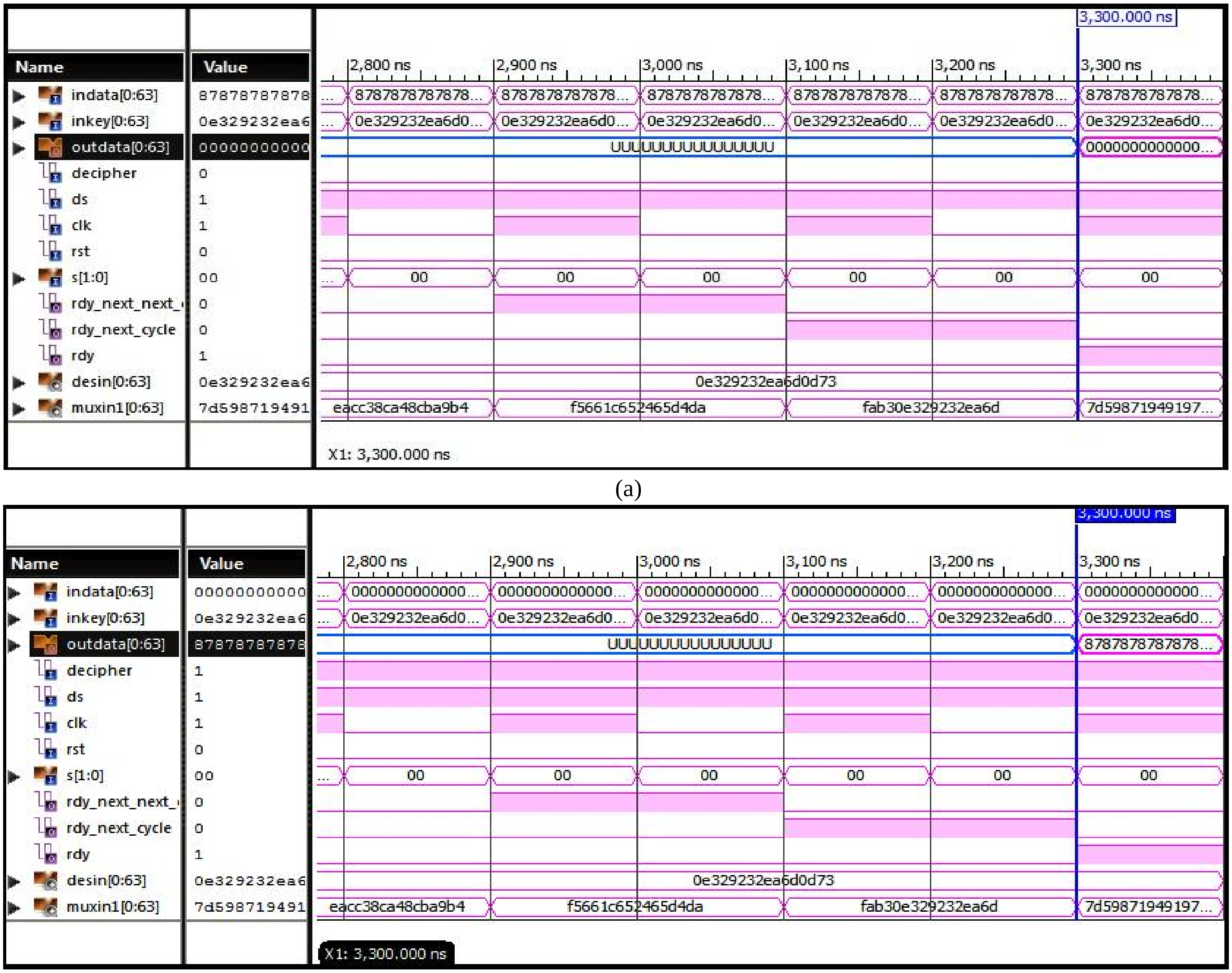
Fig. 5 Block diagram of Dynamic Key Generation Unit.

V. SIMULATION RESULTS

DES algorithm is implemented with VHDL and simulated in RTL level with Xilinx ISE 12.3 simulator and simulation results are as shown in figure. In simulation results both encryption and decryption results are shown when decipher is 0 then encryption takes place and when decipher is 1 decryption takes place. Encryption results are get after 16 clock cycles and this encryption result is decrypted using same key to get original data.

Simulation results contains encryption and decryption and it will be done by giving decipher signal when decipher 0 then encryption takes place and when decipher 1 then decryption takes place. As we are using multiplexer, mode selection is based on the select input given when select input S is “00” then direct key is get selected, for S “01” LFSR is get selected, for S “10” chaotic encryption is selected and for S “11” 2’s complement is get selected and we get the different simulation results for different modes as shown in figures below.

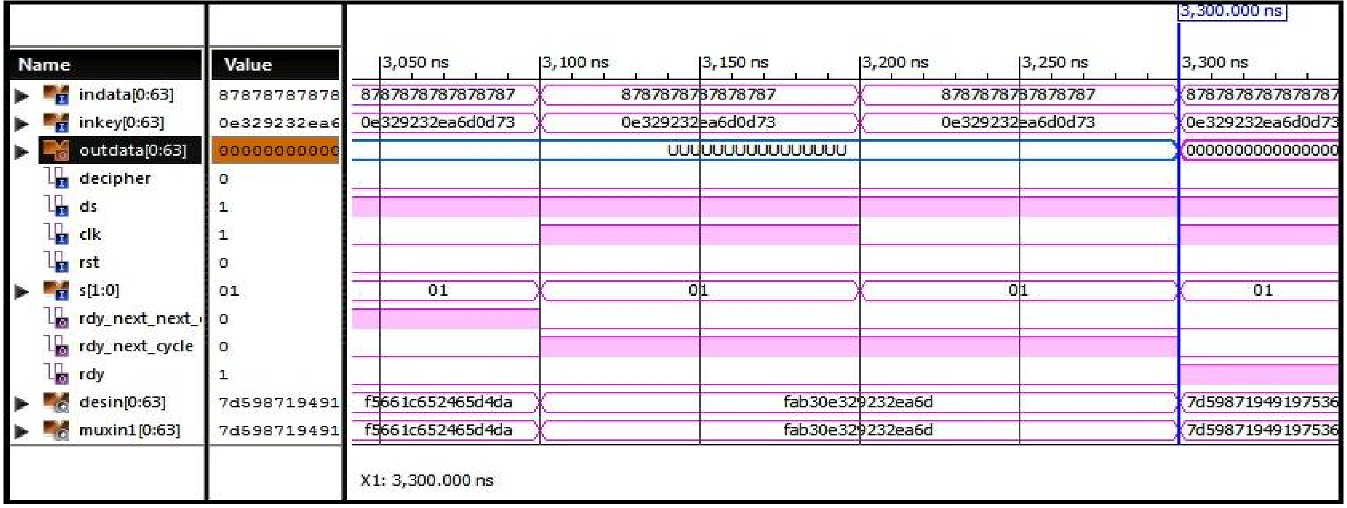
For encryption we used input value of 64-bit input value indata 8787878787878787 and 64-bit key inkey 0E329232EA6D0D73. For decryption we used input value as its encryption output value and same key. Simulation results for encryption and decryption are shown in figures below. In chaotic encryption we only get the encryption there is no decryption results are shown because we are not giving key to the chaotic encryption block. In each simulation result figure (a) indicates encryption and figure (b) indicates decryption.



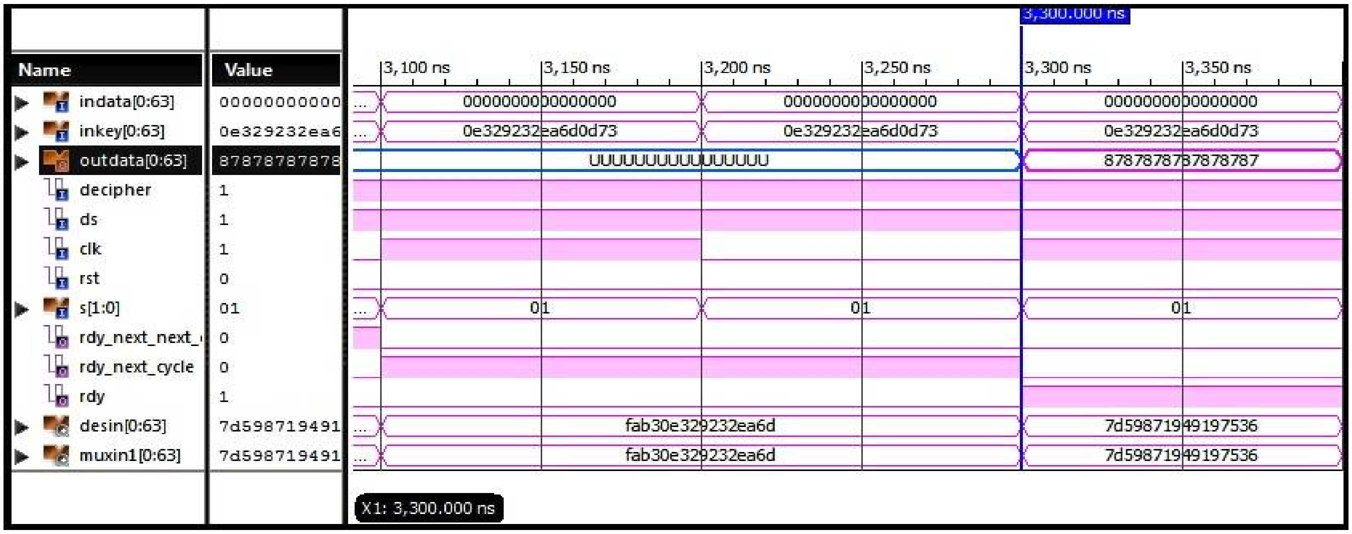
(a)

(b)

Fig. 6.1 Simulation results for direct key.

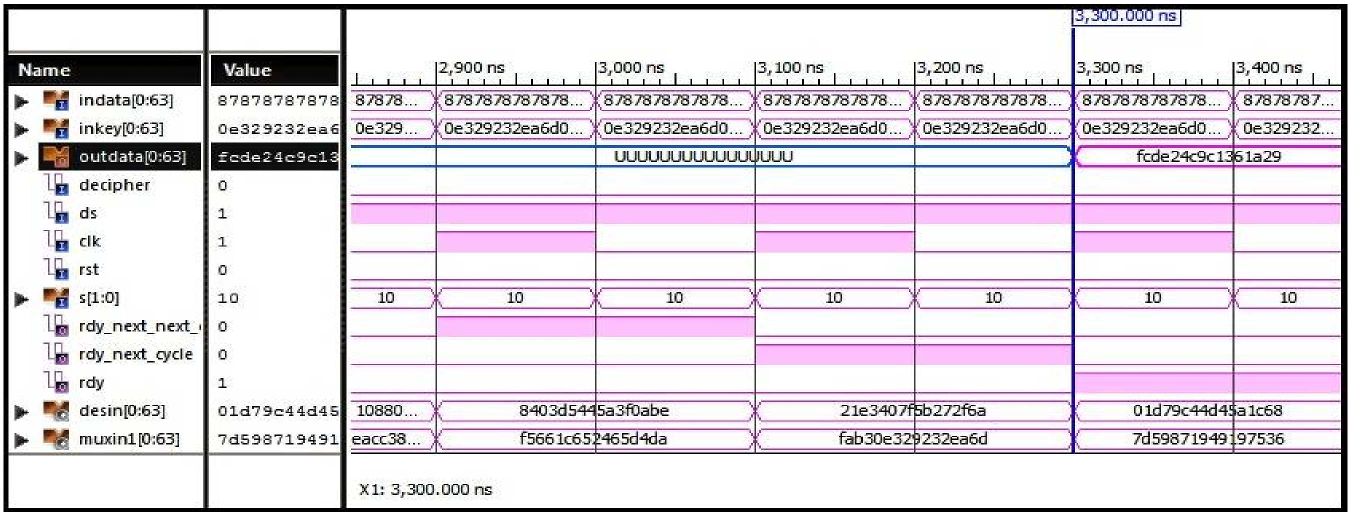


(a)



(b)

Fig. 6.2 Simulation results for key generated by LFSR.



(a)

Fig. 6.3 Simulation results for key generated by chaotic encryption

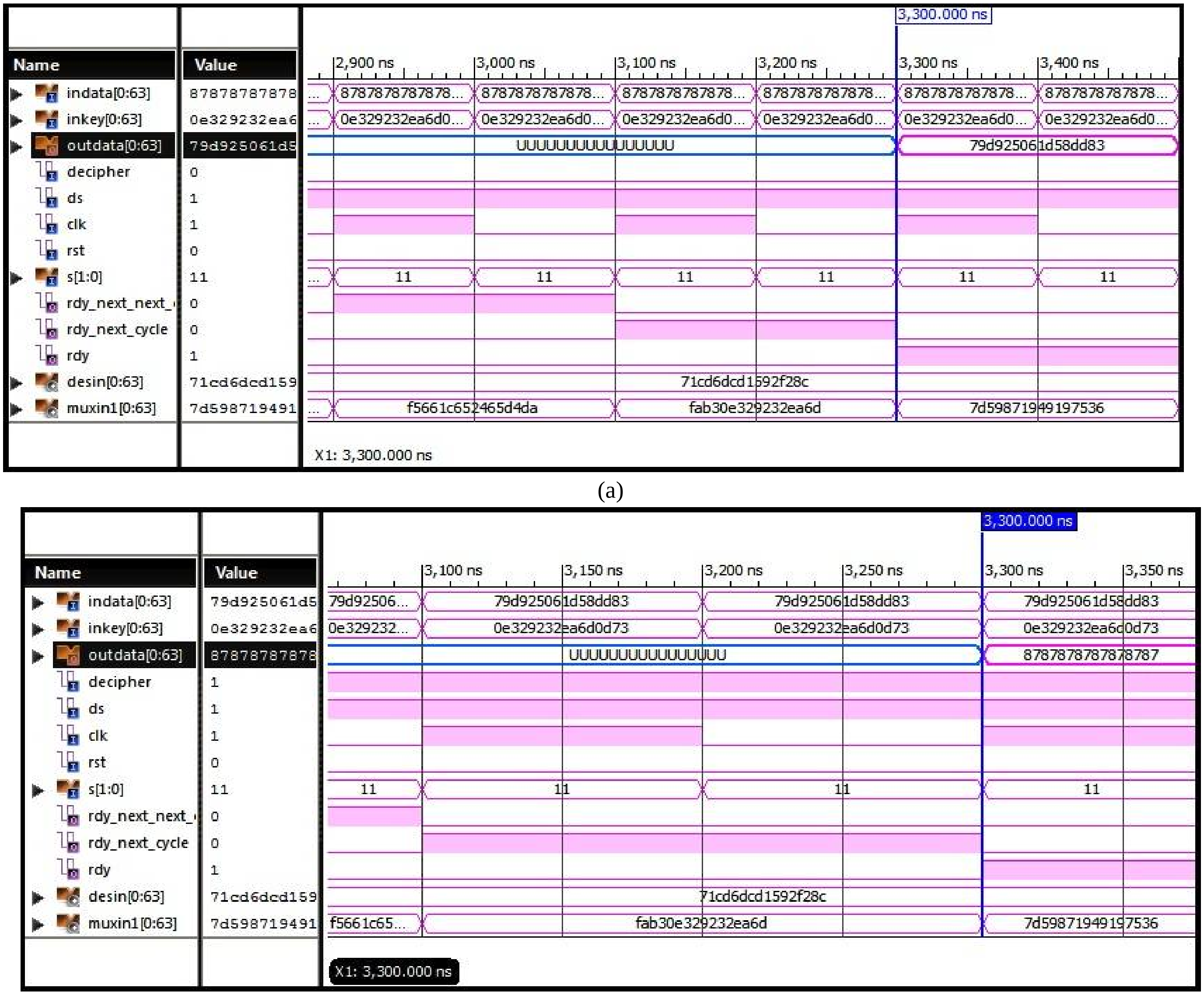


Fig. 6.4 Simulation results for key generated by 2's complement.

VI. CONCLUSIONS

The security of any type of algorithm is dependent on the secrecy of the key. To enhance the algorithm this paper proposed the dynamic key generation unit which is independent on DES algorithm. Due to the dynamic key generation unit secrecy of the key get increased. Simulation results are shown for both encryption and decryption.Using proposed design we can achieve high speed and reduced logic complexity which gives enhanced DES algorithm. According to this enhanced DES algorithm has broad application area in secure data communication and transmission.

REFERENCES

[1] Akhilesh Gautam, Prof. Preet Jain,"FPGA implementation of dynamic key generation to enhance DES algorithm securities", International journal of engineering research & technology (IJERT) ISSN: 2278-0181, Vol. 4, Issue 01, January-2015.

[2] Hitesh Mittal, Ajay Kakkar,"Performance analysis of multiple keys used for data security", International journal of computer applications (0975-8887), vol.95-No.14, June 2014.S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," IEEE Electron Device Lett., vol. 20, Nov. 1999.

[3] Akhilesh Gautam, Prof. Preet Jain,"Dynamic key generattion to enhance DES algorithm securities using FPGA" International journal of advanced research in

computer science and software engineering, Volume 4, Issue 12, December 2014.

[4] Prashanti. G, Deepthi. S,Sandhya Rani.K, ”A novel approach for data encryption standard algorithm”, International journal of engineering and advanced technology (IJEAT), June 2013, ISSN: 2249-8958, Volume-2, Issue-5

[5] Khemraj Deshmukh, Prof. Vishal Moyal,”Key reconfiguration in DES algorithm”, International journal of digital applications and contemporary research, Volume 1, Issue 6, January 2013.

[6] LI Wei, ZENG Xiaoyang, NAN Longmei, CHEN Tao, DAI Zibin,”A reconfigurable block cryptographic processor based on VLIW architecture”, IEEE transaction on security schemes and solutions.

[7] Zodpe H. D., Wani P. W., Mehta R. R.. "Design and implementation of algorithm for DES cryptanalysis", 12th IEEE International Conference on Hybrid Intelligent Systems (HIS), pp. 278-282, 2012.

[8] X. Shuang-jian, Y. Liang, X. Fang-fang. "The Principle of DES Algorithm and Realization on FPGA". Computer Technology and Development, vol. 21, no. 7, pp. 158-160,164, 2011.

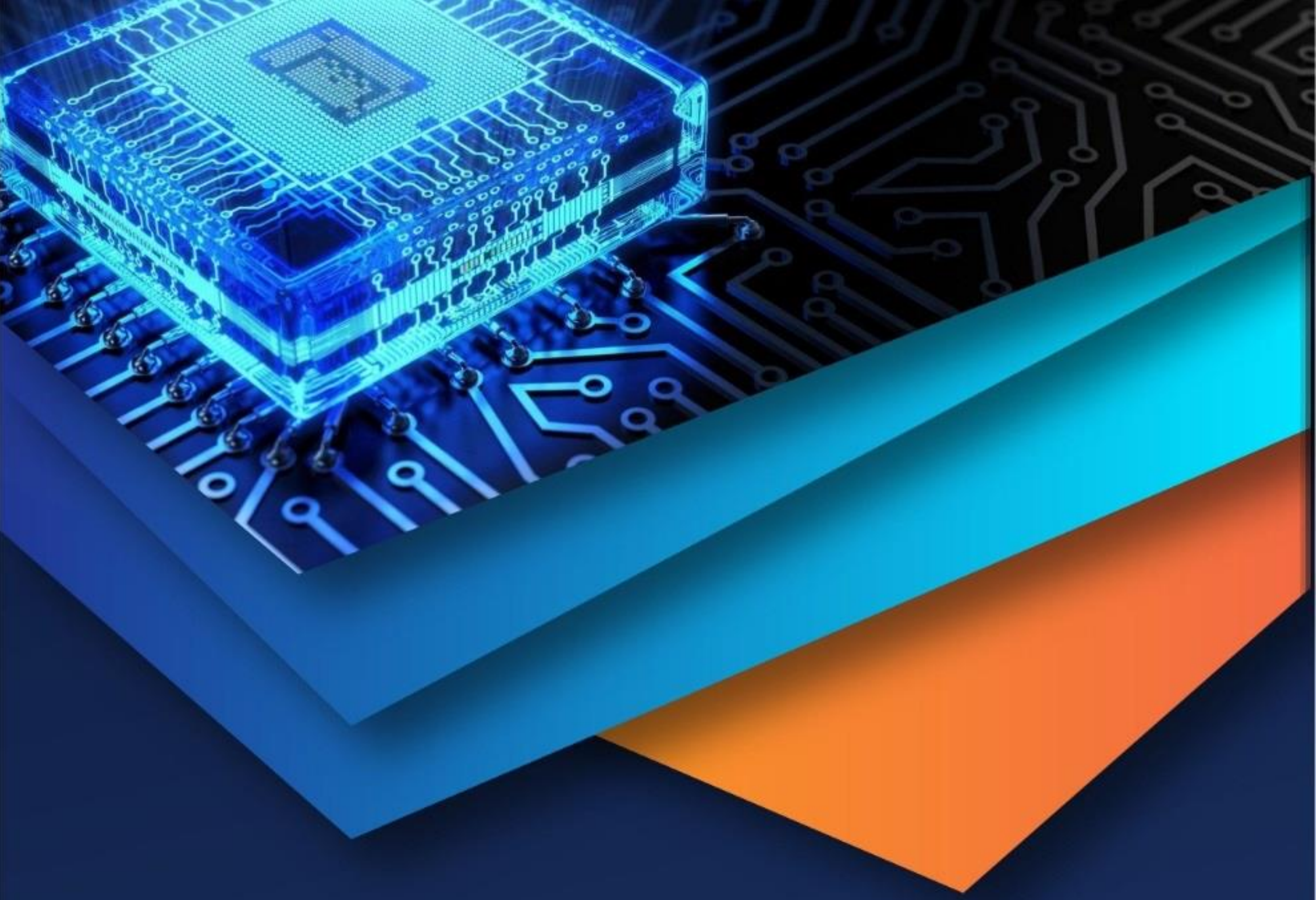
[9] Karim Moussa Ali Abd El-Latif, Hesham Fathi Ali Hamed, El-Sayed Abd El-Hameed,” Hardware implementation of DES using pipelining concept with time-variable key”, 22nd International Conference on Microelectronics (ICM 2010)

[10] Behrouz A. Forouzan, “Cryptography and Network Security”, Special Indian Edition., TMH: New Delhi, 2007.

[11] Yadollah Eslami, Ali Sheikholeslami, , P. Glenn Gulak, Shoichi Masui, and Kenji Mukaida,” An Area-Efficient Universal Cryptography Processor for Smart Cards”, IEEE transactions on very large scale integration (VLSI) systems, Vol. 14, No. 1, January 2006.

[12] William Stallings,” Cryptography and Network Security Principles and Practice”, publishing as Prentice Hall, 5th edition, ISBN 10,pp. 330-337,2006

[13] Toni stojanovski and Ljupco kocarev, senior member, IEEE , chaos-based random number generators—part I: analysis” IEEE transactions on circuits and systems—I: fundamental theory and applications, vol. 48, no. 3, march 2001



10.22214/IJRASET

45.98

IMPACT FACTOR:
7.129

IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY