Performance Analysis of DES and Triple DES Algorithm

Shraddha P Tankasali[1], Sunita Shirahatti[2], Thejaswini P[3]

[1]Student, Department of Electronics & Communication, JSS Academy of Technical Education, Bengaluru, India
[2]Professor, Department of Electronics & Communication, JSS Academy of Technical Education, Bengaluru, India
[3]Professor, Department of Electronics & Communication, JSS Academy of Technical Education, Bengaluru, India

---***---

Abstract - *Today's world is dominated by wireless systems and data security is also one of the weighty importances in wireless applications. To increase the performance of data security systems, both compression and encryption of data needs to be utilized. The order of application of compression and encryption/decryption techniques affect the amount of memory usage, time taken and power performance. The main intention of this work is of analyzing the performance of Encryption / decryption algorithms on text data. In this paper, the Implementation of FPGA of DES and Triple DES Encryption / Decryption algorithm is done in Xilinx 14.7 and simulated using ISIM simulator. In DES, the time delay taken to encrypt a text data is 30.6ns and power consumed is 0.224W and in Triple DES, the time delay taken to encrypt a text data is 70.632 ns and power consumed is 0.434W.*

Key Words: **Data Encryption Standard (DES), Encryption, Triple DES.**

1. INTRODUCTION

A cryptographic system is a technique for hiding data with the goal that very few individuals can realize it. The plaintext will be the original data. The secured data is named cipher text. Cryptography, at its most principal level, requires two stages: encryption and decryption. Changing the plaintext to cipher text is a technique entitled as Encryption. Whereas Decryption is a methodology that changes over cipher text into a plaintext. There are two kinds of cryptographic algorithms you have to understand, symmetric algorithm also known as "private key" and asymmetric algorithm also known as "open key". Symmetric algorithm, for the encryption process and decryption process it utilize a similar key, while asymmetric algorithm is going to utilize an alternate key for both, and the encryption key cannot derive the key for decryption. Cryptography is the study of ensuring data by changing it into a secure format.

1.1 Encryption

Encryption algorithms and components utilized in broadcast communications incorporate Triple DES, RSA, Advanced Encryption Standard and Data Encryption Standard. Each Encryption algorithm has an objective to make the decryption process as troublesome as conceivable produced cipher text by not using the key. For that kind of algorithm, as much as the key is drawn out so much is the troublesome to decrypt a bit of code text by not having the key. It is hard to decide the quality of an encryption algorithm.

1.2 Decryption

The recipient of decryption gets an ephemeral or window where a secret phrase can be arrived to get to the encrypted data. For decryption, the systems ponders and alterations over the jumbled data and alters it into words and images that are excellently reasonable by a reader as well as by a systems. This stint could be utilized to portray a technique for decryption the data manually or decryption the data utilizing the correct ciphers or keys. Data may be encrypted to make it rigid for someone to take the data. A few organizations similarly encrypt data for general protection of organization data and proprietary revolutions.

2. RELATED WORK

The past and future of the DES during the mid of 1970s, regarding the proposed standard, the forces primary to the expansion of the standard for the period of the early 1970s and the increasing receipt and usage of the standard in the 1980s, and some latest progresses that could disturb the upcoming of the standard is discussed in [1]. The most significant involvement of the DES is that it has directed us to other security contemplations, outside the algorithm that is to be done in order to have secured computer systems and links.

The study to approach a successful implementation of DES algorithm by means of High Level Language (HLL) is described in [2]. The hardware platform used here is Spartan 3e XC3S1600E Field Programmable Gate Array (FPGA). For DES Implementation, an HLL tool is used which is called Xilinx System Generator. An environment provided by System Generator is analogous to Simulink where it is mainly used to design the system pictorially as a substitute of scripting code of thousands lines. Its throughput is of 1.24GHz and the frequency it functions is 310.174 MHz; it makes use of 120 BRAMs and 1344 slices. Conversion of data block of 64 bit to cipher text of 64 bit is done in DES by making use a key of size 56 bit. This algorithm is having 16 rounds where the reverse of this method is equivalent to it is recurred that decrypts 64 bit of cipher text back to plain text of 64-bit utilizing the identical key.

The complete theoretical analysis and introduction of DES Algorithm is provided in [3].To take the algorithm to next level it offers a variety of designs for encryption key and s-box. To enhance the security the algorithm is structured and actualized to an improved DES algorithm as that of which hardware language VHDL is utilized. By multiplying the encryption key length the design makes sure that there is no access in the password system, can rest linear cryptanalysis. The implementation of DES on JBits is explained in a Virtex FPGA. For the run-time creation, JBits offers a Java-based

Application Programming Interface (API) and variation of the conjuration bit stream is given in [4]. The outcome becomes the throughput of over 10 Gbps when pooled with a speed competent outline. The DES design uses 0.18 micron with 1.8 volt and 6 layer metal process which will be transferred to Virtex-E. Maximum clock speed is going to develop up to 200 MHz (12.8 Gbits/sec).

Blowfish is referred as Feistel network, and also a symmetric key cryptographic algorithm, done along iterating a simple encryption function for sixteen times, which is explained in [5]. The size of the block should be of 64 bits, whereas the key be able to be kept of any size up to 448 bits. Blowfish algorithm involves two stages with key expansion and data encryption.
This project has carried out the encryption with blowfish algorithm using FPGA platform which is designed to be coded in VHDL also simulation by using VHDL simulator. This blowfish algorithm is extra protected because of the flexibility of the key compared to any other prevailing algorithms. Variable key length makes it difficult to collapse the algorithm for the reason that the generation of key is very difficult.

The project shows the proposed Enhanced key to expand the level of security as given in [6]. Thus, the proposed framework is divided into three more framework to make key generation more grounded which approaches direct keys era that key are client produced, so the second framework is done by making use of LFSR because it is a great generator of key stream and the third that is carried by means of taking chaotic encryption and the fourth stays 2's supplement. Control unit proposed to control the Encryption of 16 round of DES and DES calculation becomes the second part of this project and decoding process too. To execute the substitution boxes (S-boxes) a multiplexer-based engineering is made use. Hence, the proposed framework is carried out in the outline of VHDL language also joined in the Xilinx Virtex-xc6vlx75t-3ff484 FPGA device.

The project describes about the issues of using smaller key size in DES which makes it easy to translate the cipher-text to its corresponding plain-text done by the method called brute-force at a reasonable cost, explained in [7]. The objective of these projects is to recommend an alternative method to DES so as to obtain higher security by growing the key size obtaining next level execution efficiency and modernising the technique of iteration. After comparing the DES algorithm and Advanced DES entitled as triple DES algorithm (i.e., 3DES), the outcomes have verified that the proposed algorithm overtakes both the previous algorithms.

The VLSI implementations of the triple-DES block cipher, with three different kinds of hardware implementations are projected in [8]. First and the second implementations are built on the basis of pipeline technique, whereas the third implementation make use of successive iterations to transfer the data. Meanwhile, ROM blocks and Look up Tables (LUTs) were used to implement TDES S-boxes that provides meaningful information about the design throughput and covered area. On the other side, the ROM approach gave the enhanced performance than that of LUT one but also the LUTs were used in the circumstances where ROM blocks were unavailable.

This paper explains the DES and Triple-DES implementation of FPGA by giving us the advanced security against power analysis outbreaks given in [9]. The suggested designs utilizes the technique of Boolean masking that protects the implementations of smart card from being attacked. The result proves that to implement a masked DES recent reconfigurable devices do deal good opportunities. Thus, the use of large amount of embedded memories that are available in the Xilinx Virtex-II pro-reg FPGAs will be capable of storing masked and pre-computed substitution tables. The proposed design requires only 45% more logic than the unprotected DES designs when compared and it can also be obtained that 128kbits of memory is needed to that which yields the throughput of about 1Gbit/sec.

This paper efforts to reconsiders the security which is an encryption technique which is most used regardless of the presently being de-standardized by NIST that was offered by two-key triple DES, as shown in [10]. The paper gives an idea about the attack enhancements that implies the vastly used estimates that the 2 keys TDES delivers 80 bits of security which are not further be viewed as conservative, with this it also challenges that until the key is regularly altered the scheme is secure. The project concludes by saying that, for the 2 key 3DES the margin of safety is slim, and efforts are to be pursued with some urgency, to replace atleast with its three-key variant with preferably more modern cipher as that of AES.

3. DES and Triple DES Algorithm

3.1 The Data Encryption Standard Algorithm (DES)

DES algorithm, an algorithm recognized as symmetric block and also an iterated block cipher algorithm that is known by XOR, replacement in addition with permutation processes. These operations are iterated for 16 number of internal rounds which are successive and the ideologies of this algorithm is of Feistel Cipher structure. Round function F goes under the steps of XOR, expansion/permutation and replacement operations. And the plain text of 64 bits is separated into two halves of 32-bits, L_0 (left) and R_0 (right). Both the halves go over 16 rounds inward handling and afterwards intersect to create the 64-bit cipher text. For every round, inputs will be L_{i-1} and R_{i-1} that obtained from last round. Then, for individual round function F, obliges an exceptional sub-key K_i of 48-bit produced by input key K of 64-bit by the process of generating round key. So, the formulae for each round can be shown as below

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F\left(R_{i-1}, K_i\right)$$

By utilizing permutation with development initially the R input is stretched from 32 bits to 48-bits. Round key K_i is used to XOR the output. Then the output of 48-bit is given to the substitution table (i.e., S-Box) which delivers an output of 32-bit that is agreed and permuted to the DES algorithm. To begin the process of key generation, a 64 –bit information key is permuted to 56-bit output by changes made by major permutation decision. The above outcome is reflected as per dual C0 and D0 of 28-bits information. At every round, both C_{i-1} and D_{i-1} are left as well as circularly moved once or twice that seal in as an input to the upcoming round. Then the moved information is at that time given to another permutation decision that creates an output of 48 bits that fills as input to the function – when RK as compulsory.

3.2 Architecture for DES Algorithm

Figure 1 shows the high level view on design of DES Algorithm. A similar arrangement of h/w building blocks are used in Encryption/Decryption tasks. DES encryption/decryption has three standard parts of the figuring plan and they are: Regulator, the encryption/decryption engine and Key Generation. Key Generation block takes 64-bit input key and for every 16 individual rounds it produces 16 number of 48 bits round key. In the next Section the process of generating round key is explained briefly.

Then the controller is used to produce different control signals to control the key generation process. The definite plan aimed at the controller is specified below in the subsection B from Methodology section.

From the subsection C of Methodology we learn about the substitution box (S-Box). At this point, the information way of the architecture comprises of many of registers, multiplexers, and replacement and permutation/expansion tasks. A basic data routing is one of the major factor that is required in permutation/ expansion straightforward activity which is a bit-transposition activity. The substitution activity entails eight diverse substitution boxes. Subsection C explains about the actualization of an S-Box, by multiplexer based structure.

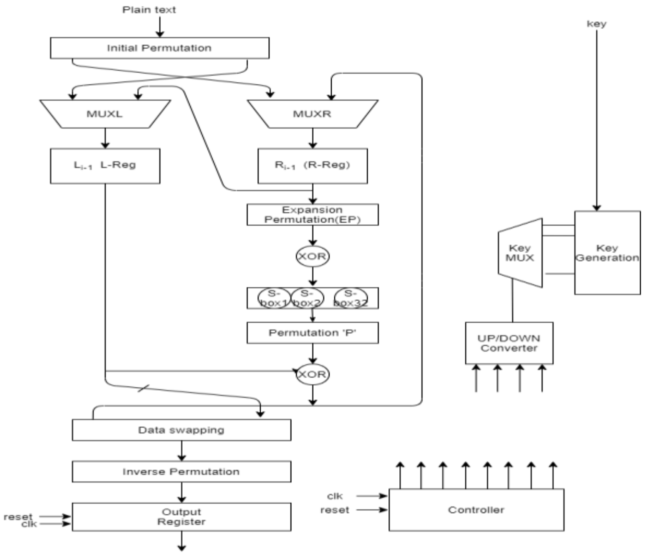


Fig 1. VLSI architecture for DES Encryption/Decryption Computation

3.3 The Triple DES Algorithm

Triple DES algorithm is exceptional identification of client with electronic acknowledgement method. From different cryptographic techniques, DES is demonstrated as the safer and quick algorithm. It utilizes 64 bit cipher and in this way, no possible method of breaking DES after inquiry of 2^{55} steps. By utilizing DES, computational power expands step by step and along these lines triple DES is the best algorithm to defeat it. The block diagram of 3DES is as shown in Figure 2. 3DES is used to encrypt the plain text by using DES thrice and every time one distinctive key that is utilized is meant for encryption. 3DES practices thrice, 64 bits key for instance 192 bit key however utilizes 168 bits also for parity checker 24 bits are utilized. 128 pieces key is utilized in size in which k1 which is of 64 bits and size of k2 will be of 64 bits as well as set k3 equivalent to k1.

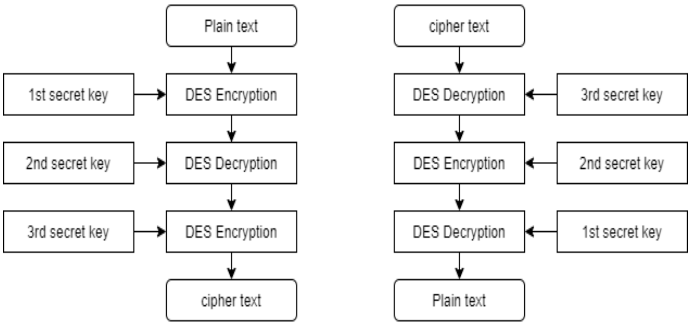


Fig. 2 Block Diagram of Encryption/Decryption

4. METHODOLOGY

The steps for the building blocks of the DES architecture are as follows

4.1 Generation of Round Keys

According to the DES algorithm requirements, the design appeared in above shown Figure.2 entails round key happening in every rounds. We can get the purpose of the process of generating the round key as it has appeared in Figure 3. For every specific rounds, exceptional round keys of 48 bits are created by this process.

All the sixteen rounds play a vital role in creating the 16 round keys in DES Algorithm. The process of generating round keys starts with input key of 64-bit that is directed towards the block of permutation decision-1 (permutation-1). When input key is permuted by stage 1 block into 48-bit information that are given to 2 blocks (C and D) of 28-bit then both the 28-bit inputs are left shifted circularly by a couple of bits, which relies on the quantity of round according to this DES key generation algorithm. Encryption/decryption activity is overseen with controller that is clarified beneath.

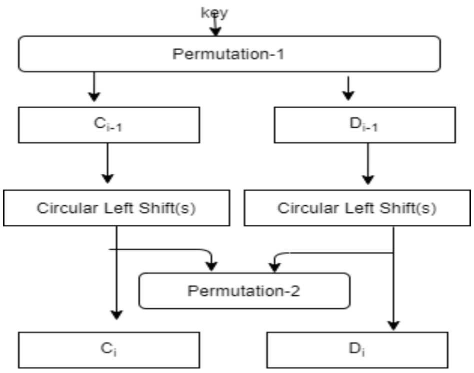


Fig 3. Round Key Generation Scheme

4.2 Architecture for an S-Box

There are set of 8 substitution boxes (S-boxes) in Substitution process. Every substitution box has 6-bits input and output of 4 bits. S-box can be designed by using 5 multiplexers (MUXs). By using this methodology, the architecture is built as appeared in Figure 4. To execute the S-Box, five MUXs are used. The initial 4 MUXs are of 4 bits i.e., from MUX [S00] to MUX [S11], 16 down 1 MUX. 4 rows of S-box are generated from those MUXs. The chain of 4 MUXs are driven by equivalent select lines and by using these the content of various distinct rows are chosen. According to S-box choosing rule, select lines from MUXs show up the 4 bits from the center of the contribution to the S box. RHS MUX is of 4 bit i.e., 4 down 0. 2-bit binary number is structured by the 1st bit and the last bit, S-Box_IN[5] and S-Box_IN[0] respectively. The multiplexer uses these 2 bits as select lines. The output is elected among the 4 outputs from the remaining 4 MUXs by utilizing the multiplexer that makes the output signal of 4 bit that is SBOX_Out. The structure of the S-Box is exceptionally basic and ordinary. The architecture meant for the S-Box is ordinary along with that it is having exceptionally basic directing associations. Designing a lot of 8 S-Boxes, the S-Box is going to be used multiple times with the relating replacement esteems that are given by DES algorithm.

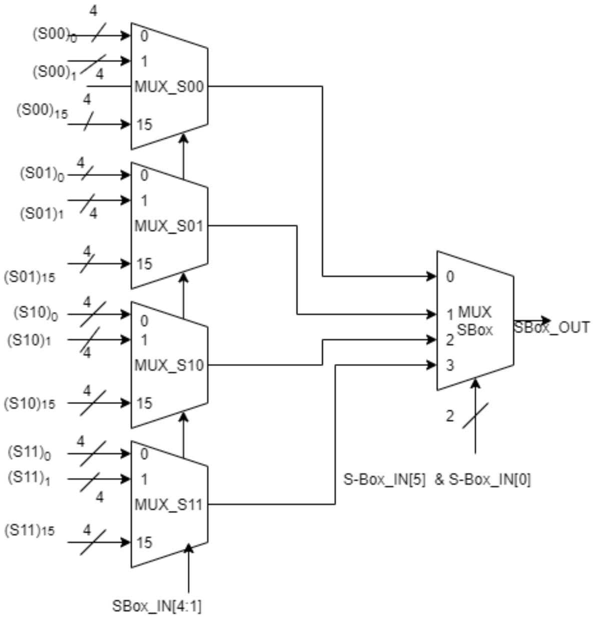


Fig. 4. Realization of S-box using DES Algorithm

4.3 The Encryption/Decryption Operation

The structure mechanism is for the 2 encryptions similarly with respect to decryption that depends on 'EN_DE', the info signal. At one point when 'EN_DE' signal will be at logic '1', then regulator demonstrations in an encryption express that it is going to cause EN_Encrypt to the logic High to and it achieves Encryption. At the point where the sign 'EN_DE' signal will be at logic Low it goes about as Decryption.

As showed that select line for MuxL is indicated by making use of the Sel_L_Mux signal and to determine the input MuxR, the signal Sel_R_Mux is used. Initially, all the select lines out of idle state, will be at logic 0. Then to determine the initial stage of permuted inputs the select lines are taken and all of them are routed to L_Reg with R_Reg enlists independently. For a signal 'E_XOR_K', the architecture have need of 48-bits XOR gate. One of the signals from input signal of the particular gate starts from the activity called expansion permutation activity (E). Thereafter, among 16, 48-bits round keys, new sign is one of it and the XOR gate's output is given to the Substitution Boxes (S-Boxes). The outputs of 32-bit of 8 S-Boxes is at that point permutated (P). The permuted output is once again XORed with that of the remaining underlying permutated 32 bits that was picked by MuxL. Then the activity of the output is put away in the R-Reg register. Iteration of previously shown operations are done for sixteen number of times with that regulator showed in Fig. 4. Delivers distinctive control signals and that are controlled. After satisfaction of impressive number of rounds, enlisted output will be open after next 19 clock cycles. Output created is cipher text or a plaintext will depend on the signal 'EN_DE' that indicates operation of encryption or decryption.

4.4 Triple DES Encryption/Decryption

Encryption:
Cipher_Text = En_{k3} (De_{k2} (En_{k1} (Plaintext)))

Decryption:
Plain_text = De$_{k1}$ (En$_{k2}$ (De$_{k3}$ (Ciphertext)))

The steps for triple DES is carried out as Encryption, Decryption, and Encryption with 3 unique keys, which implies 3DES utilizations three 64 piece keys like k1, k2, k3 absolute of 168 bits.
Initially, original text is encrypted by key k1 then decrypted by K2 and afterward by k3. Potential outcomes of doing this are;

1. The three keys are independent mutually i.e., k1= k2= k3= k1 at the point where total key space is 3x56 = 168 bits
2. Merely two keys are conjointly free and 3rd key is identical by 1st key which means k1= k2 and k3= k1. So 2x56 = 112 bits can be key space.
3. All 3 keys are equivalent by mutual, k1 = k2= k3 that is correspondent to DES algorithm.

   Once the accomplishment of these phases is over, average time and the encryption level will be improved by that of standard DES.

5. Results and Discussions

The simulation and synthesis of DES and Tripple DES algorithms are done using Xillinx 14.7 and ISIM simulator. The simulation results of DES and Triple DES Encryption, Decryption and synthesis is as shown in Figure 5, Figure 6, Figure 7, Figure 8, Figure 9 and Figure 10 for the given plain text , key and Cipher text.

Plain text:
Two things are infinite: the universe and human stupidity; and I'm not sure about the universe.
The Plain text in ASCII code is:
54776f207468696e_6773206172652069_6e66696e6974653a_2074686520756e69_766572736520616e_642068756d616e20_7374757069646974_793b20616e642049_276d206e6f742073_7572652061626f75_742074686520756e_006976657273652e

Key:
Einstein
The Key in ASCII code is**:** 45696e737465696e

Cipher text:
e0511fc675907715_877c452afe9f0917_c830990ccd36710d_82a6073d087afce3_78bcca435a5cb52a_775c5958f523cf6d_57ec2bc9ebea4fc5_d56ce715127ca5a7_4a0260c152043986_6dbb7f0d3148121e_56d7064bb67531ce_35033841794211a8

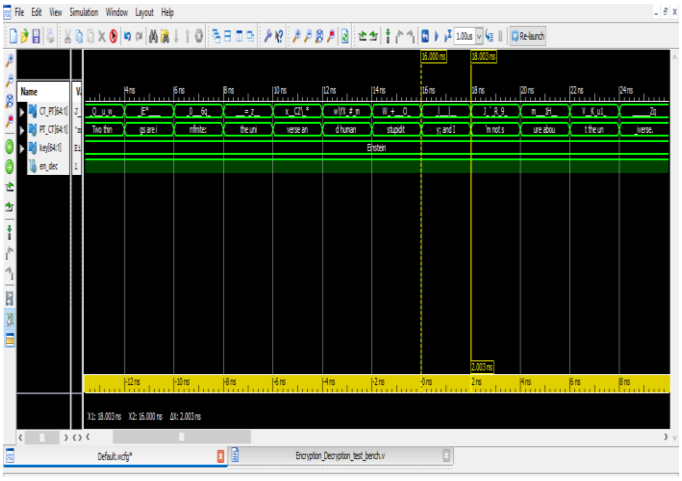

File Edit View Simulation Window Layout Help
Name
CT_PT[64:1]
PT_CT[64:1]
key[64:1]
en_dec
Einstein
Default.wcfg*
Encryption_Decryption_test_bench.v

Fig. 5. Simulation results of Encryption.

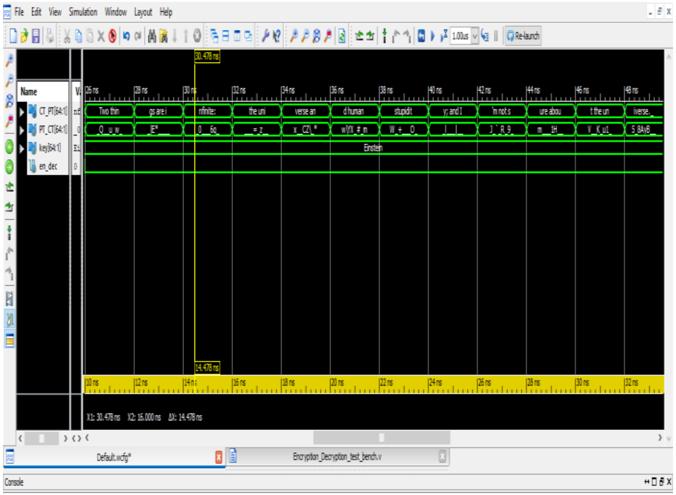
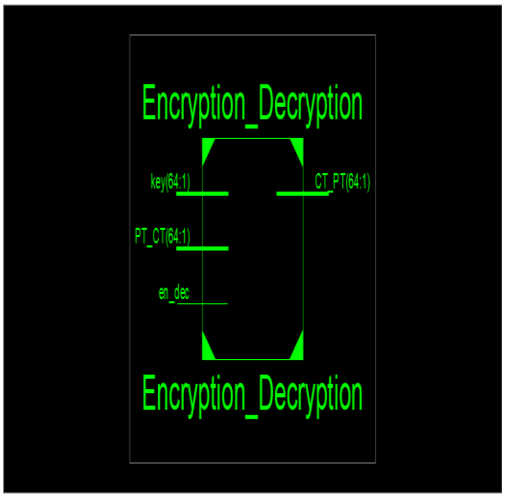

File Edit View Simulation Window Layout Help
Name
CT_PT[64:1]
PT_CT[64:1]
key[64:1]
en_dec
Einstein
Default.wcfg*
Encryption_Decryption_test_bench.v
Console

Fig. 6. Simulation results of Decryption.



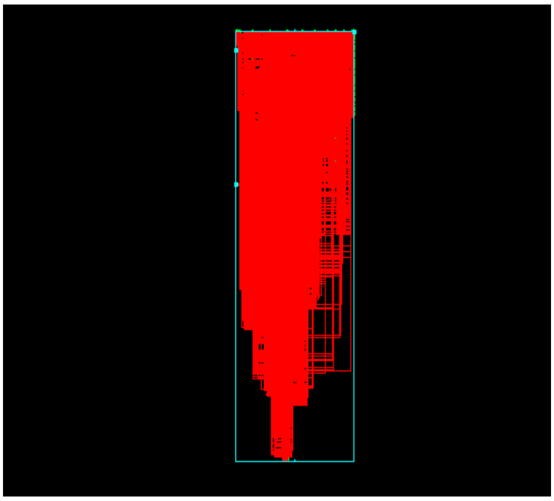


Fig. 7. Synthesis result

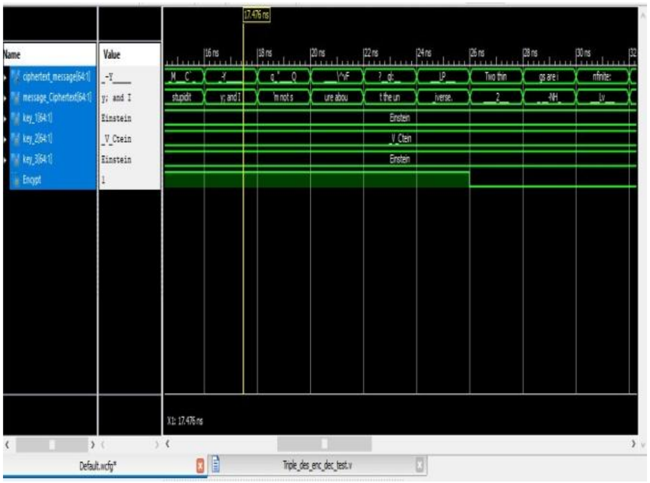


Fig. 8. Simulation result of 3DES Encryption

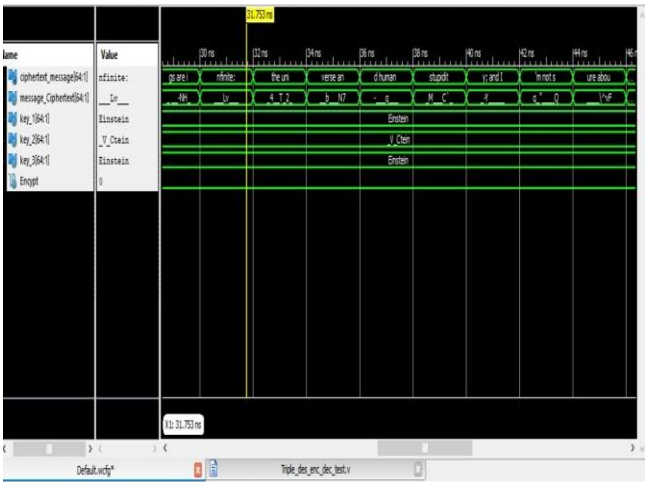


Fig. 9. Simulation result 3DES Decryption

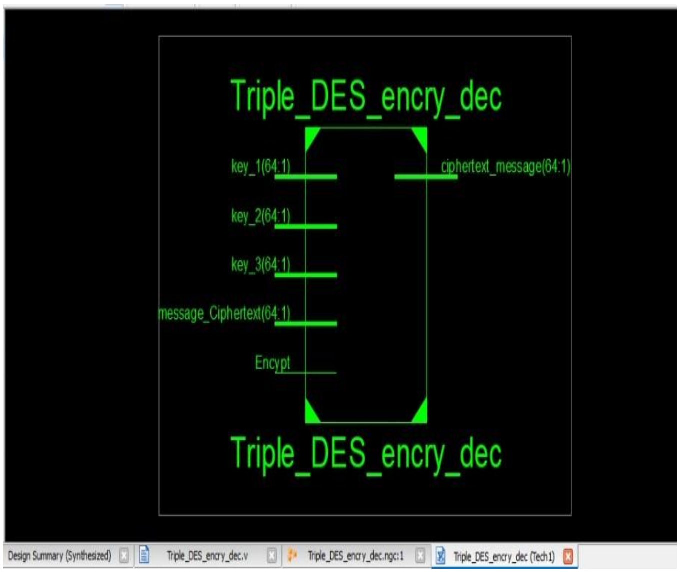


Fig. 10. Synthesis Output

The table 1 shows the performance of DES and Triple DES algorithm in terms of area, power and delay.

Table 1. Performance of DES and 3DES Algorithm

Analysis	Delay in Nano sec	Power in watts	Area (no. of LUTs)
DES	30.603	0.224	1970
3DES	70.632	0.434	4352

6. Conclusion

Nowadays it is evident that, to obtain most security and to increase the performance of data security systems, efficient encryption techniques are to be used. These encryption/decryption techniques affect the amount of memory usage, time taken and power performance. The main intention of this work is to analyze the performance of DES and Triple DES Encryption / Decryption algorithms on text data. The FPGA implementation of DES and Triple DES Encryption / Decryption algorithm is done in Xilinx 14.7 and simulated using ISIM simulator. In DES, the time delay taken to encrypt a text data is 30.6ns and power consumed is 0.224W and in Triple DES, the time delay taken to encrypt a text data is 70.632 ns and power consumed is 0.434W.

REFERENCES

[1] Smid, M. E., and D. K. Branstad. "The Data Encryption Standard Past and future in Contemporary Cryptology": The Science of Information Integrity," GJ Simmons, Ed." (1991): 43-64.

[2] Khan, Fozia Hanif, Rehan Shams, Asif Hasan, and NawaidHasan. "Implementation of Data Encryption Standard (DES) on FPGA." Journal of Information Communication Technologies and Robotic Applications (2018): 47-59.

[3] Fu, Li, and Ming Pan. "A simplified FPGA implementation based on an Improved DES algorithm." In 2009 Third

International Conference on Genetic and Evolutionary Computing, pp. 227-230. IEEE, 2009.

[4] Cameron Patterson, High Performance DES. "Encryption in Virtex (tm) FPGAs Using Jbits (tm)." In Proceedings of the 2000 IEEE Symposium on Field-Programmable Custom Computing Machines, p. 113. (2000).

[5] Arya, S. "An Implementation of Blowfish Algorithm Using FPGA." International Journal of Engineering Research and Technology 2, no. 8 (2013).

[6] Punam Milind Chabukswar, Manoj Kumar P., Balaramudu "An efficient implementation of enhanced key generation technique in data encryption standard (DES) algorithm using VHDL" International Conference on Computing Methodologies and Communication (ICCMC) (2017)

[7] Zhou Yingbing, Li Yongzhen. "The design and implementation of a symmetric encryption algorithm based on DES": IEEE 5th International Conference on Software Engineering and Service Science (2014)

[8] P. Kitsos, S. Goudevenos, O. Koufopavlou. "VLSI implementations of the triple-DES block cipher": 10th IEEE International Conference on Electronics, Circuits and Systems, 2003. ICECS 2003. Proceedings of the 2003

[9] F.-x. Standaert, G. Rouvroy, J.-j. Quisquater. "FPGA Implementations of the DES and Triple-DES Masked Against Power Analysis Attacks": International Conference on Field Programmable Logic and Applications (2006)

[10] Chris J. Mitchell. "On the Security of 2-Key Triple DES": IEEE Transactions on Information Theory (Volume: 62 , Issue: 11 , Nov. 2016)