Implementation of Data encryption & decryption using DES Algorithm

***Deepak Guled*[1*], *Nagaraj Angadi*[2], *Soumya Gali*[3], *Vidya M*[4], *Deepti Raj*[5]**

[1-4]*Student, Department of Telecommunication, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India*

[5]*Assistant Professor, Department of Telecommunication, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India*

***Email:** deepakguled@gmail.com

DOI: http://doi.org/10.5281/zenodo.2624422

Abstract

Security is one of the most important fields to be considered for data secrecy & confidentiality many small scale applications like health-monitoring and biometric data-based recognition system need low or short-term security. Data encryption standard (DES) is one of the lightweight cryptographic algorithms to be considered for such applications. DES is itself simpler & effective algorithm for data encryption & decryption. A single architecture is used to perform encryption & decryption operation. As per the need same architecture performs both encryption & decryption operation. A multiplexer-based architecture is used known as substitution boxes (S-Box). The architecture used here is modelled Verilog HDL language and synthesized in the Xilinx device. To further enhance the security concept of dynamic key generation is implemented.

Keywords: *DES, Encryption, Decryption, Verilog, Cipher text, ModelSIM, Xilinx*

INTRODUCTION

Data security has been a topic of major interest since decades. With the development of communication systems, the techniques of data exchange have been revolutionized hence the need of data integrity and authenticity has also elevated. Different cryptographic algorithm has been designed for it. A cryptographic algorithm is a system that can convert data from its original readable form into a scrambled one in such a way that the original data can’t be accessed by fraudster.

Nowadays the information security is the most important aspect of digital data communications. Since these data become of more importance and secrecy of data like banking data, military data, sensitive information like medical records, and multimedia contents such as image, audio, or video is very much necessary. Thus, it is required to use an adequate algorithm for data security which stops data leakage to unauthorized person. On the other hand, the pace of the technology and the developments in the field of computational processing speed in our lives is becoming faster and faster. These developments facilitate the threats and attacks on the data to reveal its secrecy increasingly and burden the huge challenge of accomplishing the task of securing the communications.

Data Encryption Standard (DES) is a standard cryptographic algorithm, developed by IBM and adopted as a Federal Information Processing Standard. DES has been used by many applications that require data confidentialities. DES algorithm is a symmetric block cipher and it provides adequate level of security with low hardware cost. Though, the 56-bit key somewhat compromises the security level, yet, brute-forcing this key requires several months along with several computing engines. Although DES has evolved into the advanced encryption standard (AES), nonetheless, many applications continue to rely on DES for cryptography and information security. Therefore, the designers and implementers continue to support for efficient architecture for the DES in many short-term security applications. Thus, there is always a need of optimized, high-performance hardware implementation of DES and other lightweight ciphers. Based on the above discussion, a light weight DES implementation has been discussed here.

The architecture also uses a single substitution box, which are used eight times. The implemented design has been used for resource-limited applications that include, radio frequency identification (RFID) tags, wireless sensor nodes applications, etc. In this implementation, sixteen rounds of the DES algorithm have been fully unrolled. The proposed architecture is a simple and efficient VLSI architecture for computation of DES algorithm. The proposed architecture uses nearly nineteen clock cycles to encrypt a plaintext into cipher text. The decryption process is identical to encryption operation and it completes the decryption process in nearly nineteen clock cycles. The key generation process is realized in a combinational data path and it provides all the required sixteen round keys to the encryption/decryption block in the first cycle of the clock. By this, it makes the decryption block to start the decryption process by using the last round key, which is mandatory as per the DES decryption algorithm. To implement an S-Box, five multiplexers (MUXs) are used. Out of the five MUXs, four MUXs are of 4-bit, 16-to-1 MUXs and one 4-bit, 4-to-1 MUX. To make the design work in pipelined mode the inputs and outputs are registered. To further enhance the security the concept of dynamic key generation is implemented.

Previous work done

J. G. Pandey, Heena Nehra [1] "An Efficient VLSI Architecture for Data Encryption Standard and its FPGA Implementation". This paper deals with the security of small-scale applications like health-monitoring and biometric data-based recognition system which requires short term security. The proposed architecture is an efficient design of DES algorithm-based encryption/decryption engine. As per the requirements of encryption/decryption operation, the same set of architecture can be used to perform both encryption as well as the decryption. The substitution operation (S-Box) needed in the DES algorithm has been implemented by multiplexer-based architecture. The proposed architecture is very regular and it requires very low amount of hardware resources, therefore it can be efficiently utilized in lightweight cryptography applications. The architecture is modeled in the VHDL language and it has been synthesized for Xilinx. In another implementation, a JBits programming language-based implementation of the DES algorithm for Xilinx Virtex field programmable gate array (FPGA) has been described.

Ho Won ki [2] "Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System". In this paper the author describes about a special-purpose microprocessor designed to enhance the execution of cryptographic algorithms. This processor is used for many security applications such as embedded systems, network routers, etc. The processor consists of a reduced instruction set computer and coprocessor blocks. These blocks are dedicated to the AES, SEED, DES & RSA crypto algorithm. The dedicated coprocessor block helps in fast execution of different operations. Similarly, 32-bit reduced instruction set computer preforms execution of different crypto algorithms like Hash and other application programs. The processor has been designed and developed using a fixed programable gate array, and have been fabricated on a VLSI chip using 0.5 µm CMOS technology. The performance of this chip is studied using on time data security board.

Sarita Kumari [3] “A research Paper on Cryptography Encryption and Compression Techniques”. This paper gives a brief idea on different encryption and decryption technique associated with Symmetric & Asymmetric Key Cryptography algorithms. Along with this it also provides ideas on different compression technique that is used for transmission. Basically, compression is a technique which reduces the size of data which in turn saves space. Cryptography enables us to confidentially transmit the data such that no data is altered. Data is a type of stored information it can be digital or physical. Security means providing protection to assets. Data security means security of data privacy in order to prevent unauthorized access to computers, personal databases etc. Cryptography protects users by acting as a proxy or firewall allowing only the legitimate users access the data & blocking fake users from access the data. Cryptography is a famous way of sending confidential data in a secret way.

Chaitra B, Kiran Kumar V.G, Shatharama Rai C [4] “A Survey on Various Lightweight Cryptographic Algorithms”. In this paper the author’s have performed a brief study on various lightweight symmetric block ciphers such as DES, PRESENT, TEA and HUMMINGBIRD & AES. Lightweight cryptography is very well suited for resources limited devices such as RFID tags, smart cards & wireless sensor networks. Many real time applications that are transmitted quickly are voice, video, images and text but not limited to highly sensitive information like transaction of credit card, banking and confidential security numbers/data which have limited resources & require security. Thus, protection of data for such application is required with high security to avoid unauthorized access to Wireless networks. This can be done by a using cryptography techniques, there are 2 cryptography techniques available & they are symmetrical & asymmetrical techniques. This paper provides effective comparison between different Lightweight symmetric cryptography.

H. Fathima, K.S.R. Matriculation & K.S.R. Kalvi nagar [5] “Comparative Study of Symmetric Key Algorithms-Des, AES and Blowfish”. The author’s in this paper presents an analysis in the field of cryptographic algorithms, focusing on the private key ciphers which are used for bulk data and link encryption. This paper’s main aim is to study different kinds of cryptographic algorithms that are used today and provide difference between them as comparative study in form of literature survey. The study further represents performance of each encryption algorithm and analyze security issues of each algorithm. Cryptography is a technique which provides secure path between source & destination by hiding the data from unauthorized persons i.e. by converting information from a readable state to scramble state. In order to stop unwanted persons being from reading the information, sender controls/holds the ability to decrypt the information. There are 3 different types of cryptography used to secure the information. A detailed study of various symmetric key encryption algorithms such as DES, & AES is provided in this paper.

CONCLUSION

Previous work focuses on the concept of general DES algorithm which uses 56 bits key for encryption & decryption which may lead to brute force attack (i. e trying all the 2^56 keys to decrypt the data) but the work presented here uses the concept of dynamic key generation to enhance the security of the algorithm. Further pipelining is included to make the execution of algorithm faster.

ACKNOLEDGEMENT

We would like to express our gratitude to our project guide Mrs. Deepti Raj, Assistant Professor, DSCE, Bangalore for her constant support throughout this endeavor.

REFERNCES

1. J.G.Pandey & H.Nehra presented "An Efficient architecture for data encryption & decryption"(2016).
2. HoWon Kim published "Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System in May 2017
3. Sarita Kumari presented "A research Paper on Cryptography Encryption and Compression Techniques" in April 2017
4. Chaitra B, Kiran Kumar V.G & Shatharama Rai C presented the paper "A Survey on Various Lightweight Cryptographic Algorithms on FPGA" in Jan.-Feb. 2017.
5. K.S.R. Kalvi Nagar proposed "Comparative Study of Symmetric Key Algorithms-Des, AES and Blowfish" in Dec 2016.
6. Irfan Ahmed proposed "A Low Cost FPGA based Cryptosystem Design for High Throughput Area Ratio" in Nov 2016.
7. E. Biham and A. Shamir, Differential Cryptanalysis of the Data Encryption Standard. Springer Science & Business Media, 2012.
8. W. Stallings, Cryptography and Network Security Principles and Practice, 5th ed Prentice Hall. 2011
9. G. Leander, C. Paar, A. Poschmann, and K. Schramm, "New Lightweight DES Variants," in Fast Software Encryption, 2010
10. T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography implementations," IEEE Design & Test of Computers, vol. 24, no. 6, pp. 522-533.@2007

Cite this article as:
Deepak Guled, Nagaraj Angadi, Soumya Gali, Vidya M, & Deepti Raj. (2019). Implementation of Data encryption & decryption using DES Algorithm. Analog and Digital Devices, 4(1), 24–27. http://doi.org/10.5281/zenodo.2624422