International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr2019 www.irjet.net p-ISSN: 2395-0072

Design and implementation of 256-bit symmetric key cryptography algorithm used in the data security written in VHDL

Anwesha Das[1], Paresh Kumar Pasayat[2]

[1]PG student, Dept. of ETC Engineering, IGIT, Odisha, India
[2]Assistant Professor, Dept. of ETC Engineering, IGIT, Odisha, India

---

Abstract – *The proposed paper aims to provide the software implementation of a cryptography algorithm which is based on the modified version of the Data Encryption Standard (DES) algorithm. The original version of DES operates on 64-bit data with 56-bit cipher key to produce 64-bit encrypted data. Whereas the proposed work deals with the encryption of 256-bit original data using 224-bit cipher key to produce 256-bit cipher key. As the key length is 224-bit and the time required for the encryption is in the range of nanosecond (ns), the data security algorithm is resistant towards the brute-force attack and the timing attack respectively. The proposed work can be implemented in the banking sector, telecommunication sector and military sector etc.*

Key Words: DES, Cipher Key, Brute-force, Timing attack.

1. INTRODUCTION

Cryptography is the process of concealing the content of the message by the process of encryption. In this technique, the original message is converted into a message of unreadable format so that the attacker cannot access the original message. In the proposed work, the original message is taken as 256-bits binary data and the encryption algorithm is applied on this data using 224-bits cipher key to produce a binary data having 256-bits. The algorithm is based on the modified version of the Data Encryption Standard algorithm. The proposed algorithm is different from the existing DES algorithm in terms of no. of input bits, output bits and the cipher key bits in addition to the logic of each blocks used to design the model for the addition of robustness and newness to the algorithm.

1.1 Project Model

The project describes the flow chart for the proposed project work. Each number in the model signifies the no. of bit in the input and output of each unit. The diagrammatic representation of the proposed work is given as follows:

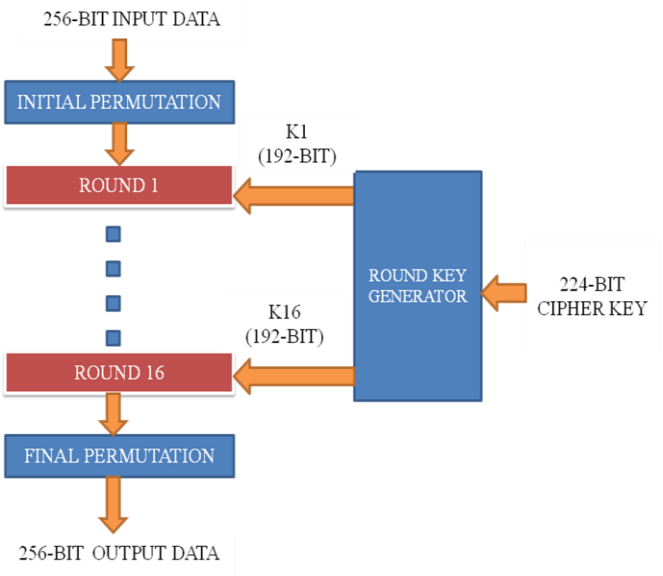

Fig 1: Project Model

2. LOGIC USED IN THE PROPOSED DESIGN

The logic used in the proposed design has been described in different steps as follow:

2.1 ENCIPHERMENT ALGORITHM:

Step 1: First, 256-bits Original data also known as plaintext is fed to the input of the initial permutation unit which transposes the data randomly to generate 256-bit output.

Step 2: The outputs of initial permutation unit is given to the first rounds which produces 256-bit output using a 192-bit round key generated from a round key generator with 224-bit cipher key as input.

Step 3: The outputs of first rounds is again given to the second round which produces 256-bits output using a 192-bit round key generated from a round key generator with 224-bit cipher key as input.

Step 4: Similarly, step 3 is repeated till the completion of 16-nos. of round.

Step 5: The output of round-16 is given to the final permutation which does the random transposition of the bits

to produce 256-bits output and this output is the desired 256-bits encrypted data.

2.2 ROUND KEY GENERATION ALGORITHM:

The sixteen nos. of 192-bits round keys are generated from a single 224-bits cipher key by performing the transposition and append operations on the cipher key.

2.3 DECIPHERMENT ALGORITHM:

The algorithm for the decryption process can be written in the reverse order of the encryption algorithm.

3. SIMULATION RESULT AND DISCUSSION

The VHDL code of the proposed work has been simulated using Xilinx ISE 9.2i software and the desired results have been obtained.

The simulation result of the encryption process is given as follows:

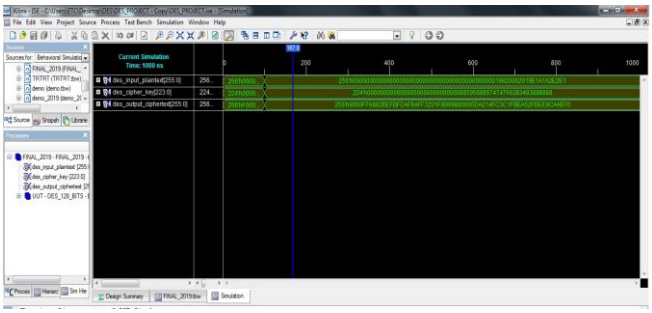

Fig 2: Simulation result of the encryption process

The simulation result of the decryption process is given as follows:

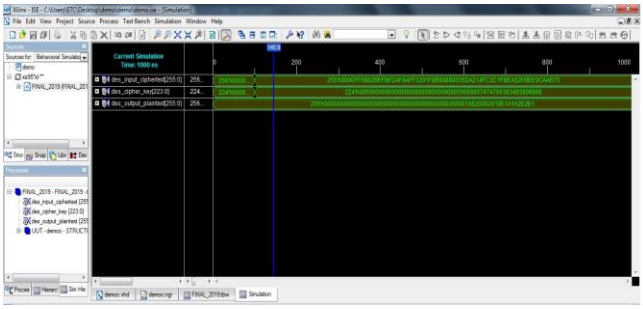

Fig 3: Simulation result of the decryption process

4. CONCLUSION

After doing the proposed work, it is concluded that the work is best suited in the field of data security to provide protection to the 256-bits original data from unauthorized access by the attackers available in the network. It is resistant to the brute-force attack, timing attack which makes the algorithm more robust. The combinational path delay required to convert 256-bits plaintext into 256-bits ciphertext is 10.763ns which obtained from the Xilinx software.

REFERENCES

[1] Dr. Sandeep Tayal, Dr. Nipin Gupta, Dr. Pankaj Gupta, Deepak Goyal, Monika Goyal, "A Review paper on Network Security and Cryptography", Advances in Computational Sciences and Technology, Volume 10, Number 5,pp. 763-770,2017.

[2] J. G. Pandey,Aanchal Gurawa, Heena Nehra,A. Karmakar, "An efficient VLSI architecture for data encryption standard and its FPGA implementation",VLSI SATA,IEEE International Conference,pp.1-5,2016.

[3] W.Stallings,"Cryptography and Network Security", 2nd Edition, Prentice Hall.

[4] Douglas L. Perry. "VHDL Programming by Examples", TMH.

[5] Soufiane Oukili,Seddik Bri,"FPGA implementation of Data Encryption Standard using time variable permutations", International Conference on Microelectronics (ICM),IEEE,pp.126-129,2015.

[6] Ramadhan J. Mstafa; Khaled M. Elleithy, "A highly secure video steganography using Hamming code (7, 4)", Systems, Applications and Technology Conference (LISAT), IEEE Conference,pp.1-6,2014.

[7] Ravikumar M.Raypure, Prof. Vinay Keswani, "Implementation For Data Hiding Using Visual Cryptography", IRJET, Volume: 04, Issue: 07, 2017.

.