International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May2019 www.irjet.net p-ISSN: 2395-0072

Design and Implementation of 256-bits Cryptography Algorithm used in the Data Security with Resistance to Brute-Force and Timing Attacks Written in VHDL code using Xilinx ISE 9.2i Software

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 create a virtual model for a new cryptography algorithm which is implemented using the modified version of the Data Encryption Standard (DES) and Hamming(448,256) code techniques. The original version of DES operates on 64-bits data with 56-bits cipher key to produce 64-bits encrypted data. Whereas the proposed work deals with the encryption of 256-bits original data using 224-bits cipher key to produce 256-bits middletext and this 256-bits middletext is given to the Hamming(448,256) code encryption block to generate 448-bits desired encrypted data. The 256-bits original data has been recovered by decrypting 448-bits encrypted data using the reverse order operations with respect to the encryption process. As the key length is 224-bits 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, Middletext, Brute-force, Timing attack.

1. INTRODUCTION

Cryptography is the process of hiding the content of the message by the process of encryption with or without the use of chip code. In this technique, the original message is converted into a message of unreadable format so that the attacker cannot access the original message easily. In the proposed work, the 256-bits original data is converted into 448-bits encoded data using modified DES and the Hamming(448,256) code encryption techniques. The proposed algorithm is different from the existing algorithm in terms of number of data bits and design styles with logic in addition to the achievement of robustness and newness of the algorithm.

1.1 Diagrammatic Representation of the proposed work

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

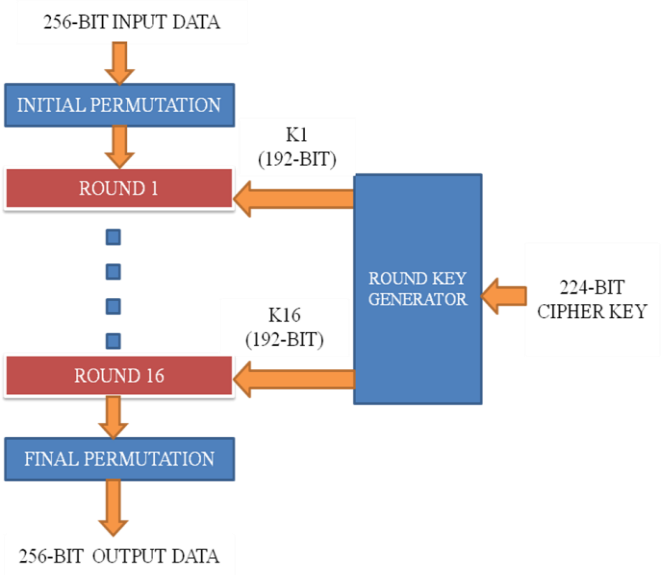

Fig 1: 256-bits Modified DES Encryption Process

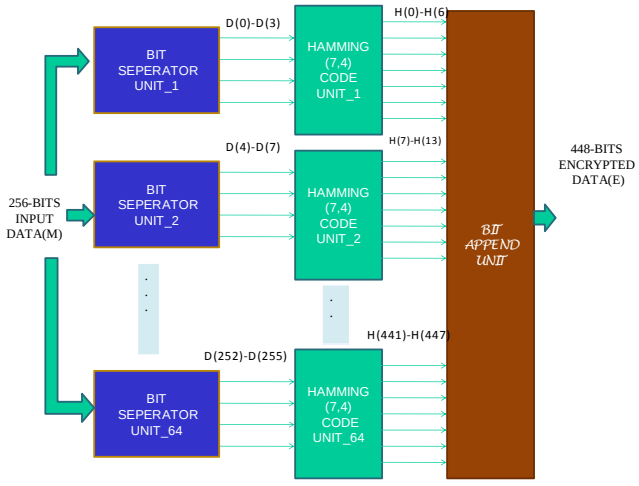

Fig 2: Hamming (448,256) code Encryption Process

2. LOGIC USED IN THE PROPOSED DESIGN

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

2.1 MODIFIED DES 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 HAMMING ENCIPHERMENT ALGORITHM:

Step 1: First, 256-bits data is divided into 64 nos. of data each consisting of 4-bits.

Step 2: The Hamming (7,4) code encoding technique is applied to 4-bits data of all the 64 blocks. For each 4-bits data, the encoding unit generates 7-bits encoded data. The logic for implementing the Hamming code technique is given as follows:

Suppose, the 4-bit data (P) to be encoded is P3P2P1P0 and the 7-bits Hamming code (H) generated from each Hamming encoding unit is H6H5H4H3H2H1H0.

Here, the value for each bit of H is given as follows:

H6 = P3 xor P2 xor P0

H5 = P3 xor P1 xor P0

H4 = P2 xor P1 xor P0

H3 = P3

H2 = P2

H1 = P1

H0 = P0

Step 3

After that, the 7-bits Hamming codes corresponding to each 4-bits data are appended to form the desired 448-bits encoded data.

2.4 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 simulation results have been obtained.

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

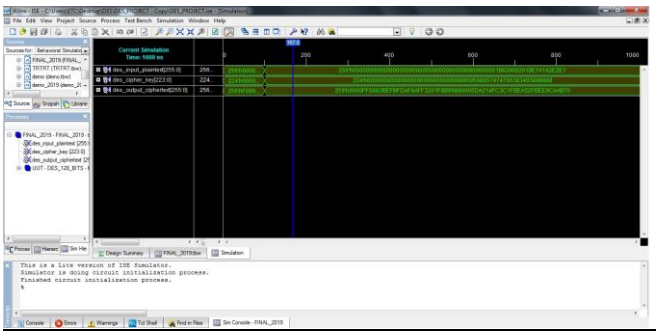

Fig 3: Simulation result of the 256-bits modified DES encryption process

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

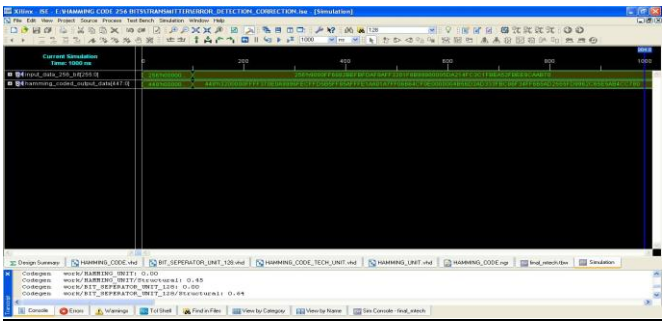

Fig 4: Simulation result of the Hamming (448,256) code encryption process

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

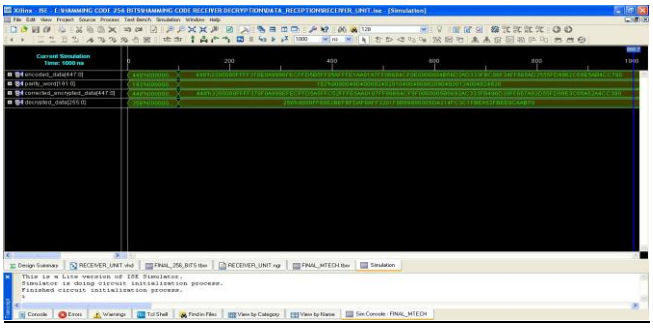

Fig 5: Simulation result of the Hamming (448,256) code decryption process

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

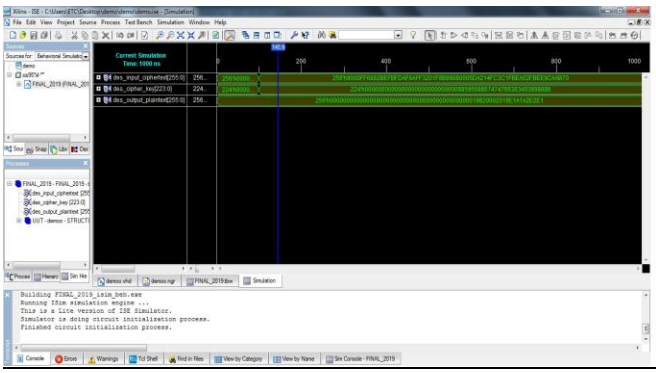

Fig 6: Simulation result of the 256-bits modified DES decryption process

4. CONCLUSION

It is concluded that the proposed 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 VHDL code of the proposed design is compiled and simulated using Xilinx ISE 9.2i software. The maximum combinational path delay required to convert 256-bits plaintext into 448-bits ciphertext is 19.231ns.

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.

.