Simplified Data Encryption Standard (S-DES)

Implementing Secure Data Transmission Using S-DES

Sagar Ramani - 21BEC102
Dhyan Rathod - 21BEC105

Course Code :- 2ECDE60

Department of Electronics and communication engineering
Nirma University,Ahmedabad,Gujarat,382421
India
24-3-2024

Simplified Data Encryption Standard (S-DES)

Sagar Ramani, Dhyan Rathod
Nirma University, Ahmedabad, India

***Abstract*—With the rapid advancement of communication devices, internet-connected networks have become ubiquitous in various human activities globally. Ensuring the security of information has emerged as a paramount concern for all users and clients reliant on network systems. Cryptography has been instrumental in addressing these challenges by enhancing the confidentiality, integrity, and authentication of data communication within networks. The Data Encryption Standard (DES) stands as one of the most widely recognized cryptographic techniques.**

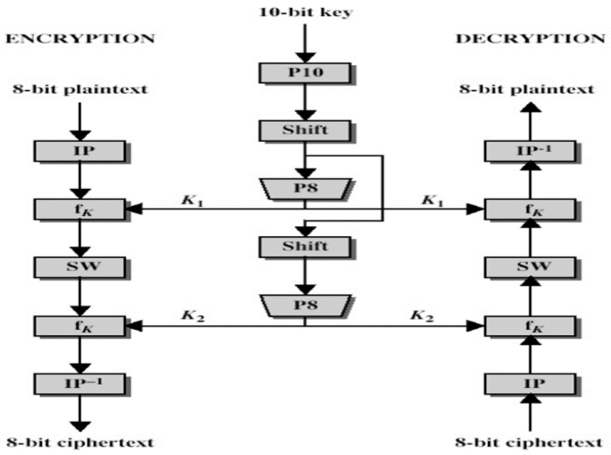
In the realm of research and academia, the choice of hardware implementation tools holds significant importance for efficiently designing and constructing prototypes of proposed models. Consequently, this paper centers on the simulation aspects of a Simplified Data Encryption Standard (S-DES) model. The emphasis lies on minimizing FPGA resource utilization, particularly in terms of Configurable Logic Blocks (CLB). By reducing complexity and logic element usage in the design, the aim is to enhance system throughput while mitigating latency.

Implemented within the Quartus II software environment using VHDL, S-DES encompasses symmetric encryption, decryption, and key generation blocks. Successfully synthesized, compiled, and deployed on an Altera Cyclone IV 4CX150 FPGA device, the S-DES demonstrates notable efficiency. Remarkably, the implementation for two rounds necessitated only 32 CLBs, surpassing existing literature on the subject.

I. Introduction

In contemporary applications such as financial transactions and online meetings, ensuring the confidentiality of information is paramount. Cryptography, with its roots in Ancient Greek, meaning "hidden," serves as the cornerstone of secure information exchange. It achieves this by transforming messages into ciphertext, thereby guaranteeing authentication even across insecure channels. Among cryptographic standards, the Data Encryption Standard (DES) stands out. Initially developed by IBM in 1970 and later endorsed by the National Institute of Standards and Technology (NIST) in 1977, DES continues to play a crucial role in safeguarding sensitive data. Despite the introduction of more advanced standards like the Advanced Encryption Standard (AES) in 2001, DES remains relevant in various applications. Its implementation can be realized through software or hardware, with Field Programmable Gate Arrays (FPGAs) offering a compelling hardware solution. FPGAs, programmable via Hardware Description Languages like VHDL, provide an optimal balance between security, simplicity, and cost-effectiveness. This paper aims to design a simplified data encryption system using VHDL targeting Altera Cyclone IV 4CX150 FPGAs. To achieve this, we undertake a comprehensive review of relevant literature, delve into FPGA fundamentals and their applications, elucidate the methodology underlying our proposed system, present experimental results, and conclude with insights and future directions.

II.



III. Simplified Data Encryption Standard (S-DES)

Edward Schaefer introduced the Simplified Data Encryption Standard (S-DES) at Santa Clara University. S-DES is a symmetric encryption algorithm derived from the Data Encryption Standard (DES) technique, based on Feistel's approach [13]. The purpose of S-DES was to simplify the principles of DES for educational activities, so it is not suitable for application purposes where high security is required.

A. Encryption Process

The S-DES algorithm takes an 8-bit block of plaintext and a 10-bit key as input, which are processed into digital binary. The plaintext and key are transformed into an 8-bit ciphertext block. The encryption process involves the following steps:

1) Initial Permutation (IP): Rearrange the positions of input bits to randomize the plaintext data bits and increase message security.
2) Complex Function Block (fk): Perform XOR, permutation, and substitution operations based on subkeys provided by the key generation block.
3) Swap Stage (SW): Switch the two halves of the data.
4) Complex Function Block for the Second Round: Repeat the fk operation for the second round.
5) Inverse of Initial Permutation (IP-1): Reverse the initial permutation to generate the final ciphertext.

B. Architecture of f-Function (fk)

The fk function in S-DES is a complex configuration consisting of expansion-permutation, XOR, substitution functions (S-boxes), and permutation operations. The operations in the fk function involve expansion, XOR with subkeys, substitution using S-boxes, and permutation.

C. Key Generation

The key generation process in S-DES is crucial for the encryption algorithm. It involves permuting and shifting the initial 10-bit key to generate two 8-bit subkeys (Key1 and Key2). The key generation circuit is shown in Figure 6.

D. Decryption

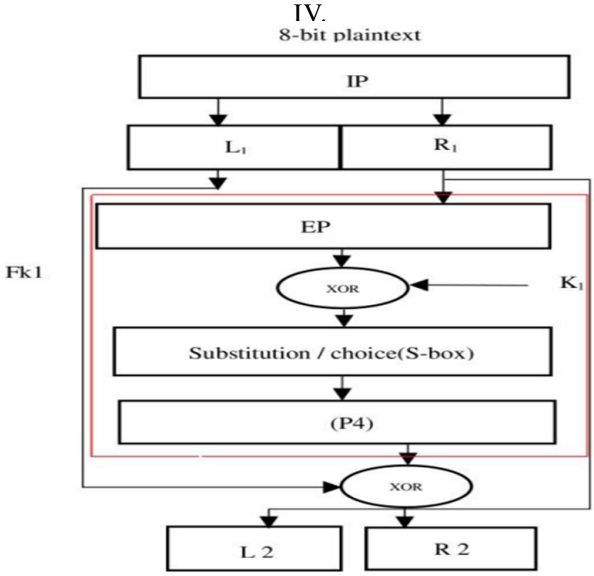
The decryption process in S-DES is similar to encryption but with the reverse order of subkeys. The ciphertext is decrypted using the same steps as encryption, but with the subkeys used in reverse order.

E. ASCII Conversion

If the plaintext is in a different format, such as alphabet or symbols, it must first be converted into decimal or hexadecimal format using the ASCII Code table, and then transformed into binary format.

F.

IV.



A. Final Permutation (FP)

After the Feistel rounds are completed, the Right and Left halves are combined and passed through a final permutation table to produce the ciphertext block.

V. Implementation in Verilog HDL

The Simplified Data Encryption Standard (S-DES) can be implemented in Verilog Hardware Description Language (HDL) using modules for key generation, initial permutation, Feistel rounds, and final permutation. These modules can be connected sequentially to form the complete S-DES encryption and decryption process. The Verilog code for these modules can be synthesized and implemented on a Field-Programmable Gate Array (FPGA) or Application-Specific Integrated Circuit (ASIC) to create a hardware implementation of the S-DES algorithm.

A. Key Generation Module

The key generation module generates the subkeys used in the Feistel rounds. It takes the initial 10-bit key as input and produces two 8-bit subkeys, Key1 and Key2.

B. Initial Permutation Module

The initial permutation module rearranges the positions of the input bits to randomize the plaintext data bits. It uses a fixed permutation table to perform this operation.

C. Feistel Rounds Module

The Feistel rounds module is the core of the S-DES algorithm. It consists of several rounds of a complex function block (fk). Each round involves XOR, permutation, and substitution operations based on the subkeys generated by the key generation module.

D. Final Permutation Module

The final permutation module reverses the initial permutation to generate the final ciphertext. It uses a fixed permutation table similar to the initial permutation module.

By connecting these modules in the correct sequence, the complete S-DES encryption and decryption process can be implemented in Verilog HDL. This implementation can then be synthesized and implemented on an FPGA or ASIC to create a hardware-accelerated version of the S-DES algorithm.

VI. Application in Secure Data Transmission

The Simplified Data Encryption Standard (S-DES) can be applied in scenarios requiring secure data transmission, especially in embedded systems and small devices with limited resources. Encrypting data using S-DES before transmission helps protect sensitive information from unauthorized access. However, due to its limited key size and number of encryption rounds, S-DES is not suitable for high-security applications where more robust encryption algorithms like AES are preferred.

In embedded systems, S-DES can be used to encrypt data transmitted over communication channels such as UART (Universal Asynchronous Receiver-Transmitter) or SPI (Serial Peripheral Interface). Small devices like IoT (Internet of Things) devices can also benefit from S-DES encryption to secure data transmitted over wireless networks.

While S-DES provides a basic level of security, it may not be sufficient for applications requiring stronger encryption. For

such applications, more advanced encryption algorithms like AES (Advanced Encryption Standard) with larger key sizes and more complex encryption processes are recommended. Nonetheless, S-DES remains a useful tool in scenarios where simplicity and efficiency are more important than high security.

VII. Conclusion

The Simplified Data Encryption Standard (S-DES) is a straightforward encryption algorithm that offers a foundational understanding of cryptographic principles, making it valuable for educational purposes. However, its limited key size and number of rounds make it unsuitable for high-security applications where stronger encryption is necessary.

Despite its limitations, S-DES serves as an excellent starting point for those new to cryptography, providing insights into how encryption algorithms work and how they can be implemented in hardware using Verilog HDL.

Future research efforts could focus on optimizing the S-DES algorithm to enhance its performance and security. This could involve exploring modifications to the key generation process, the number of rounds, or the substitution boxes to improve the algorithm's resistance to attacks.

Overall, while S-DES may not be suitable for modern high-security applications, it remains a valuable tool for learning and understanding the foundational concepts of encryption, laying the groundwork for more advanced studies in cryptography.

VIII. Refrance

@onlinegeeksforgeeks, author = "GeeksforGeeks", title = "Simplified Data Encryption Standard (S-DES) Key Generation", year = "n.d.", url = "https://www.geeksforgeeks.org/simplified-data-encryption-standard-key-generation/",

@onlinesdes-fpga, author = "0xCC00FFEE", title = "SDES-FPGA", year = "n.d.", url = "https://github.com/0xCC00FFEE/SDES-FPGA",

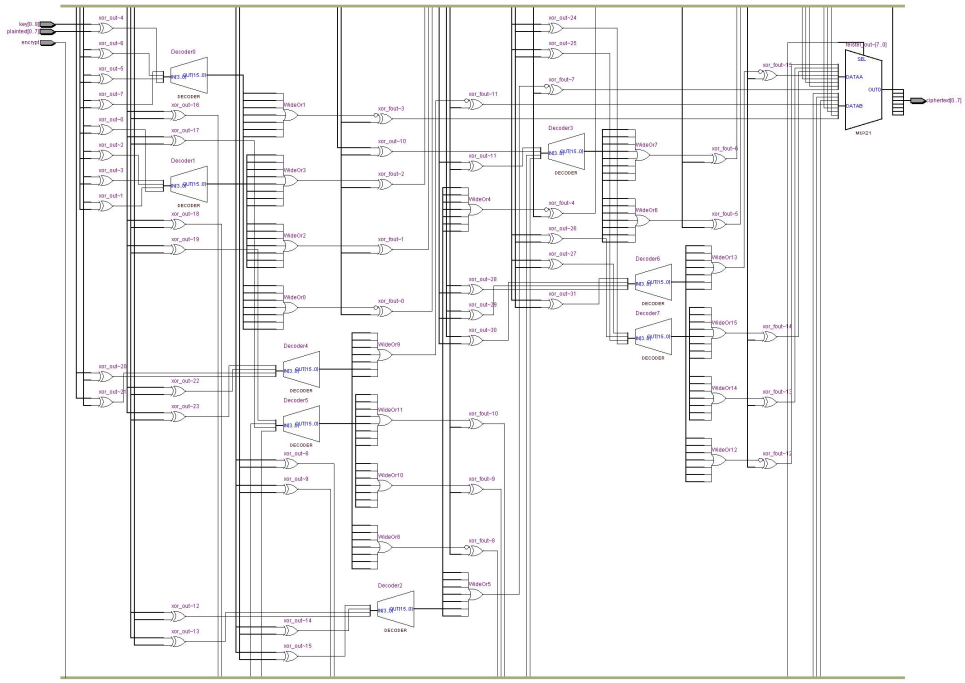


Fig. 1: Simulation Output

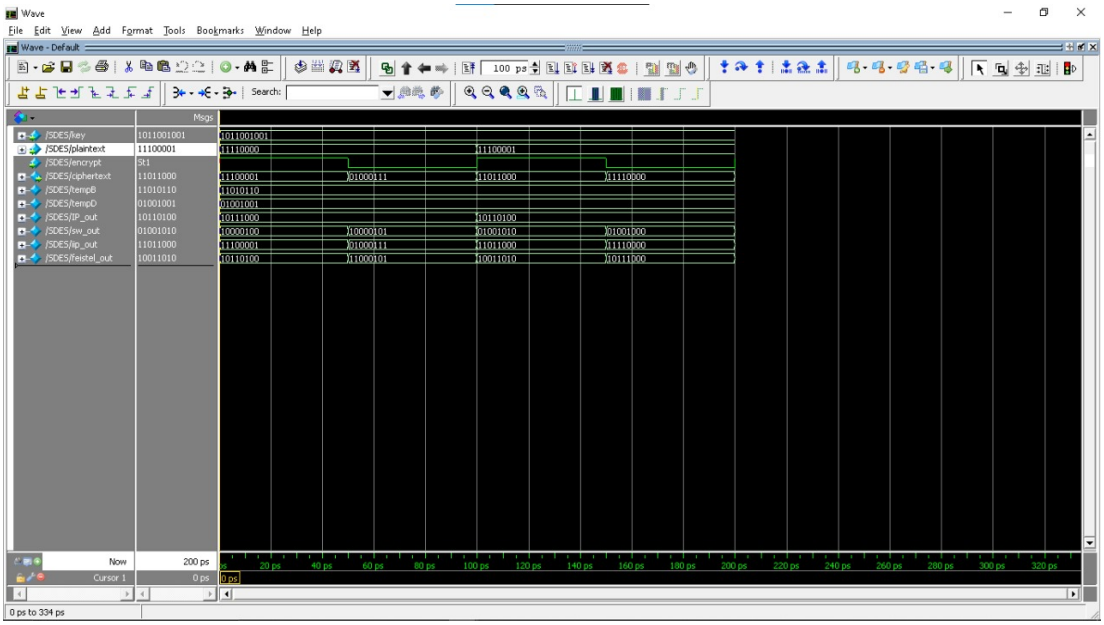


Fig. 2: Simulation Output