International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 9 Issue 9 ǁ 2021 ǁ PP. 82-85

File System Protection UsingEncryption Method

Sushant Srivastav, Bhavya Harchandani, Srivathsan Nayak
Vellore InstituteofTechnology, Vellore

Abstract:*Storage systems are increasingly vulnerable to cyber-attacks. Cryptographic document frameworks reduce the risk of information disclosure by utilizing encryption and integrity security strategies, ensuring end-to-end security for their customers. The value of data stored on digital platforms is rapidly increasing. Furthermore, most information systems are networked and contain a large number of resources such as data, software applications, and business logics, all of which are vulnerable to attacks. This project describes a generic cryptographic file system design and its implementation in a distributed storage-area network (SAN) file system. Many cryptographic algorithms are available to provide security to such information systems. The most well-known and widely used cryptographic scheme is the* ***Data Encryption Standard****, which is a symmetric key block cipher algorithm. DES was a popular cryptosystem for encrypting sensitive data transmissions.* ***Simplified DES(SDES)*** *was created solely for educational purposes, to assist students in learning about modern cryptanalytic techniques.*

Keywords: *Data Encryption Standard (DES), Simplified DES (SDES), Encryption, Decryption, Cryptography, Operating System*

Date of Submission: 13-09-2021 Date of acceptance: 28-09-2021

I. Introduction

Data encryption is the process of converting data from a readable **(plaintext)** format to an unreadable, encoded format **(ciphertext).** Data that has been encrypted can only be read or processed after it has been decrypted with a decryption key or password. The decryption key should only be accessible to the sender and recipient of the data. The **Data Encryption Standard (DES)** is the most widely used cryptosystem for information protection around the world. **DES** is a Feistel Cipher implementation. It employs a 16-round Feistel structure. The **DES algorithm** is a 64-bit block cipher with a key of 56 bits. Although the key length is 64 bits, DES has an effective key length of 56 bits because the encryption algorithm does not use 8 of the 64 bits of the key (function as check bits only). **SDES** has similar properties and structure to DES but has been simplified to make encryption and decryption much easier to perform by hand with pencil and paper. Some argue that learning **SDES** provides insight into DES and other block ciphers, as well as various cryptanalytic attacks against them.

II. Objective

1. Understanding the importance of data security and integrity in the design of a distributed operating system.
2. Types of cryptographic modules that are used to store and authorize users in different operating system data.
   For the **Windows** platform, use DES to implement a file encryption technique.
3. Comparing the time and space characteristics of decrypted and encrypted files

III. System Requirements

Recommended **RAM** Size: 4 GB.
Recommended **Hard Drive** Space: 20 GB
OS: Windows 8.1 or higher.
Recommended **Processor** Type: Intel Core i3 or higher.

IV. Scope

The scope of this project is to provide a platform to our users for securing their texts by encrypting them and storing them in files which can be decrypted any time they want. First of all, users fulfill the

agreement form of this program, then user insert a text message or include text message file. Encryption key as an input as a result, this program will encrypt and decrypt this text message and save it in a file.

V. Analysis of SDES Algorithm

KEY GENERATOR

An input key (encryption key) is taken from the user, and this key is then converted into 10-bit binary key. After that, this 10-bit binary key is divided into 5-5 bits. Then we proceed with LS-1(LEFT [1 bit]) of these 5-5 bits. Then these bits are merged and arranged according to the following rule:

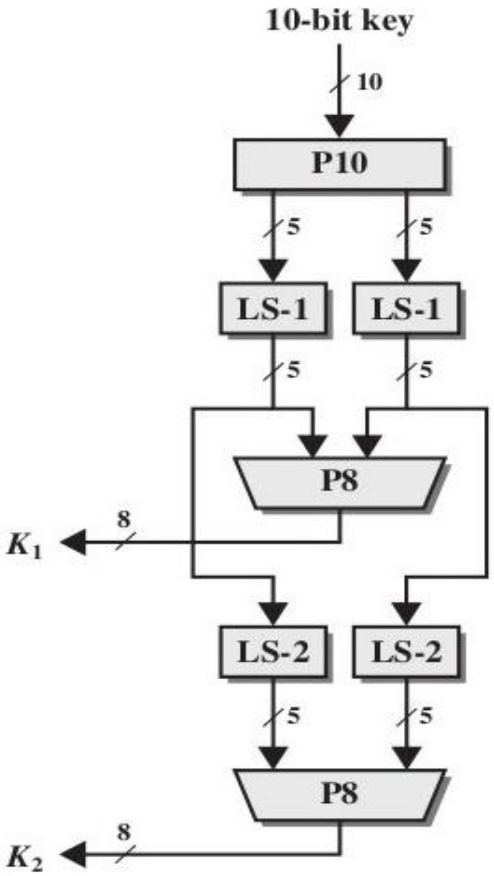
Through this we will get a key (K1) of 8 bit.

6	3	7	4	8	5	10	9

Now, from these 5-5 bits of (LS-1), along with the generating the key (K1) , LS-2(left shift [2bit]) is performed with the help of above rule (P8), we have merged(LS-2), and we get the key(key2).

ENCRYPTION DETAIL

For encryption, let us take any alphabet or integer from the user and convert it into an 8 bit (IP BINARY), then divide these 8-bit binary into 4- 4 bit binary as left 4 bit and right 4-bit IP. The right 4-bit binary is then converted into 8 bits binary and arranged according to the rule:



Flow Chart for Key Generation

F/P

4	1	2	3	2	3	4	1

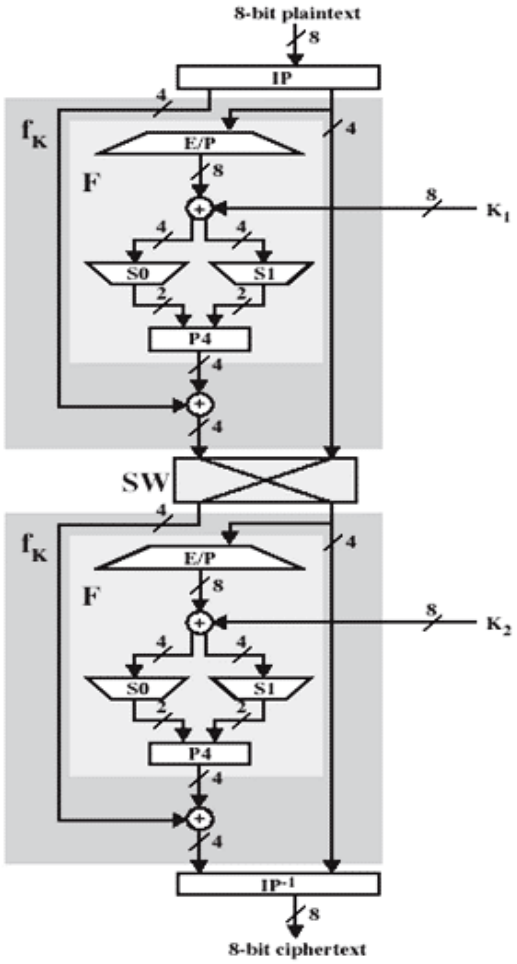
Now, this will be added with key 1 which was generated earlier. Then these 8 bits are divided into 4- 4 bits. From the first 4 bits we get S0 and from the remaining 4 bits we get S1.

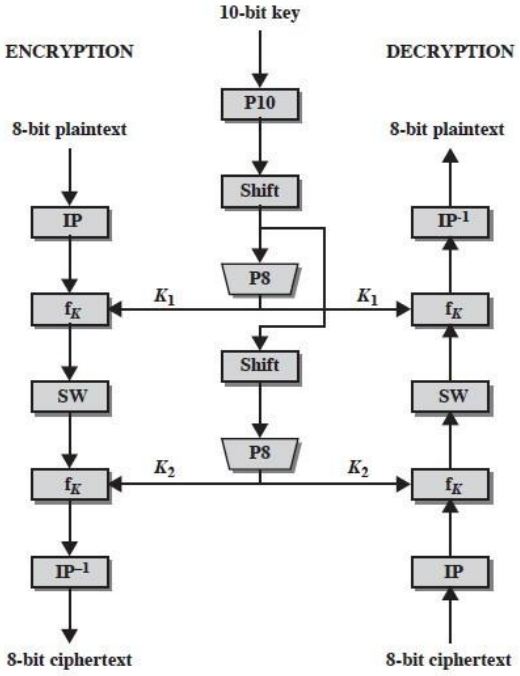
$$S0 = \begin{array}{c|cccc} P_{0,0}P_{0,3} \backslash P_{0,1}P_{0,2} & 0 & 1 & 2 & 3 \\ 0 & 1 & 0 & 3 & 2 \\ 1 & 3 & 2 & 1 & 0 \\ 2 & 0 & 2 & 1 & 3 \\ 3 & 3 & 1 & 3 & 2 \end{array} \qquad S1 = \begin{array}{c|cccc} P_{1,0}P_{1,3} \backslash P_{1,1}P_{1,2} & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 1 & 3 \\ 2 & 3 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 3 \end{array}$$

After getting S0 and S1, we will get 2-2 bit binary and arrange them according to Rule P4.

Now, this left 4 bit is added with the arranged 2-2 bit binary. This method is repeated by using a switch function. Here we use key 2 instead of key 1. Therefore, we can encrypt the user's message.

STRUCTURE OF ENCRYPTION AND DECRYPTION





VI. Future Work

The project implemented will help us understand the in-depth features of the **Data Encryption Standard**. However, we will ensure the following changes in the near future:

1. Learning about other improved cryptographic systems as the older encryption standards cannot be used forever due to developing cryptanalytic attacks.
2. Implementation of the latest cryptographic systems on different elements such as file systems in order to test the cryptographic scheme used.
3. Discovering a more efficient approach to encrypt and decrypt file systems.

VII. Conclusion

During the course of this project, we have understood the vital nature of data security and cryptography, and its role in creating a safer environment for the file systems. The **Simplified Data Encryption Standard** (SDES) cryptographic scheme has been used in such a way that it is easier to learn about the principals involved in cryptography. This knowledge can be used and applied in our further works involving cryptography.

Bibliography

[1]. https://ieeexplore.ieee.org/document/563518 - "The improved data encryption standard (DES) algorithm"
[2]. https://iopscience.iop.org/article/10.1088/1742-6596/1363/1/012078/meta - "Designing the Application of Security Text Messages into Audio Files Using Data Encryption Standard (DES) Algorithms Using the End of File (EOF) Method."
[3]. https://www.researchgate.net/publication/330077146_Performance_analysis_of_AES_DES_and_Blowfish_cryptographic_algorithms_on_small_and_large_data_files - "Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files"
[4]. https://www.researchgate.net/publication/297613039_Research_and_Implementation_of_File_Encryption_and_Decryption - "Research and Implementation of File Encryption and Decryption"
[5]. https://www.researchgate.net/publication/282526872_Cryptanalysis_of_Simplified_Data_Encryption_Standard_Using_Genetic_Algorithm - "Cryptanalysis of Simplified Data Encryption Standard Using Genetic Algorithm."
[6]. https://www.irjet.net/archives/V3/i7/IRJET-V3I7322.pdf - "Color Image Encryption and Decryption using DES Algorithm."
[7]. https://www.irjet.net/archives/V4/i3/IRJET-V4I3489.pdf - "DES - Data Encryption Standard"
[8]. https://ieeexplore.ieee.org/document/6421347 - "Design and Implementation of Algorithm for DES Cryptanalysis"
[9]. https://en.wikipedia.org/wiki/Data_Encryption_Standard
[10]. https://www.geeksforgeeks.org/simplified-data-encryption-standard-key-generation/