Implementation and Analysis of Triple Data Encryption Algorithm

Shivani Vogiral, Sanat Bhandarkar, Shashwat Mishra
Dept. of Computer Science and Engineering
PES University, Bangalore

***Abstract*—The world today is witnessing a tremendous increase in the number of security breaches, unauthorized information accesses, modifications and destruction. The importance of securing data in organizations has thus increased manifold. Cryptographic tools like encryption and decryption can be used to strengthen security parameters such as Confidentiality, Integrity, Authentication and Availability. In Cryptography, Encryption is the practice and study of techniques for secure communication. The intended information or message, referred to as plaintext, is encrypted using an encryption algorithm known as a cipher, generating ciphertext that can be read only on correct decryption. An authorized recipient can easily decrypt the message with the key provided by the originator, which is given to recipients but not to unauthorized users. Encryption is the process of transforming plaintext into ciphertext, where ciphertext is the output of the encryption. Decryption is the reverse of encryption, in that it transforms ciphertext into plaintext. This project deals with the implementation of the Triple Data Encryption(DES) Algorithm, and a comparative study and analysis of Triple DES with respect to traditional DES.**

***Index Terms*—encryption, decryption, key, cipher text, plain text, blocks**

I. Introduction

Data Security is a major issue for businesses and organizations today, and ensuring that the data is secure and protected is vital to business operations. According to recent studies, data loss is one of the biggest cyber security challenges faced by medium to large scale businesses. Data loss can damage organizations in multiple ways, with an estimated loss of USD200 for every record breached, which translates to an estimated USD6.8 million on the whole. Measures to ensure protection and security of data have therefore advanced considerably over the last 50 to 60 years to keep up with the demand. Encryption of data is one of the most potent ways to ensure prevention of unauthorized access and modification. Various encryption algorithms are in use today, but one of the most popular among these is the Triple Data Encryption Standard(Triple DES or 3DES) algorithm, which is an extension of the Data Encryption Standard algorithm.

II. Data Encryption Standard

Data Encrytion Standard is a symmetric-key algorithm which was developed in the early 1970s at IBM. DES is a Fiesel-type Substitution-Permutation Network (SPN) cipher, which was the result of the effort to produce an encryption standard for the United States of America. It uses a 56-bit key, which at the time was sufficiently adequate, however with the advent of increased computational power, these keys can be cracked using mere brute force attacks in a matter of days, making this algorithm virtually obselete. A 16 cycle Fiestiel system is used, with the 56-bit key permuted into 16 48-bit subkeys, one for each round. The structure is shown in the figure below. Decryption is the exact reverse of encryption,

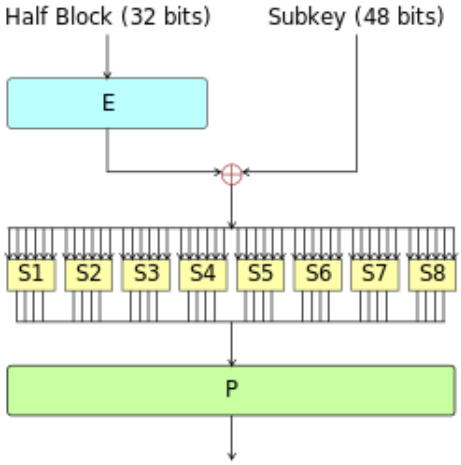

Fig. 1: Feistel Structure

wherein the order of subkeys applied is simply reversed. A block is divided into two subblocks L and R, each having 32 bits. The hash function specified by the S-boxes takes a 32 bit data block and one of the 48-bit subkeys as input and produces a 32-bit output. Sometimes 64-bit keys are said to be used, but 8 bits out of these 64 are used for parity checking, effectively reducing the key size to 56 bits. The working of DES can be observed in the figure below. With rapid advances

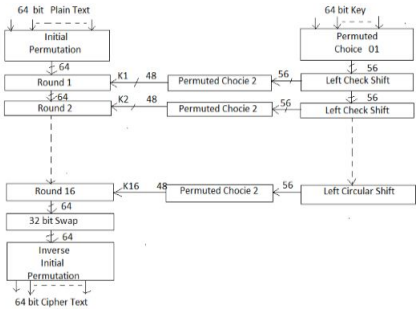

Fig. 2: Working of DES

in computational power, combined with the natural parallelism of Fiestiel's ciphers and the relatively small key size, DES can be broken in a matter of days today, making it almost completely obselete.

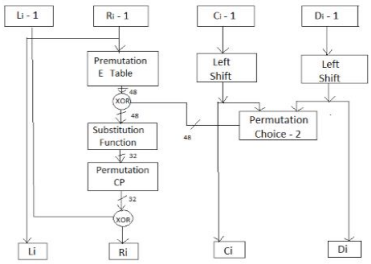

Fig. 3: Single Round Function in DES

III. Triple Data Encryption Algorithm

Triple DES, officially the Triple Data Encryption Algorithm(Triple DEA) is a symmetric-key block cipher which applies the DES cipher algorithm three times to each data block. It has been referred to as 3DES from the time RFC first promulgated the idea in 1998. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm. It uses a key bundle that comprises three DES keys, Key 1, Key 2 and Key 3, each can be of 56, 112 or 186 bits. Following is a block diagram of the Triple DES algorithm :

Encryption in Triple DES is implemented in three stages,

1) DES encrypts the plain text with Key 1
2) DES decrypts the result of stage 1 with Key 2
3) DES encrypts the result of stage 2 with Key 3 to produce the cipher text

Decryption is the reverse of encryption and is also implemented in three stages,

1) DES decrypts the cipher text with Key 3
2) DES encrypts the result of stage 1 with Key 2
3) DES decrypts the result of stage 2 with Key 1 to produce the plain text

Each triple encryption encrypts one block of 64 bits of data. In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying option 2, and provides backward compatibility with DES with keying option 3.

IV. Comparative Study

The analysis of the encryption algorithms - DES and 3DES has been done based on the following evaluation metrics:

1) Encryption Time
2) Decryption Time
3) Performance against Brute force attacks

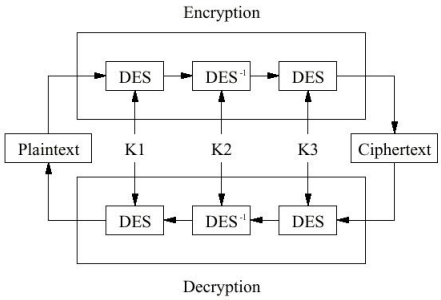

Fig. 4: Triple DES

Any cryptographic system has two important aspects: the cryptographic algorithm and the key. We have mentioned earlier that the Triple DES algorithm uses a key bundle and applies the DES algorithm thrice. From the results of the implementation it has been observed that the time required by Triple DES for encrypting the plain text and decrypting the cipher text is longer compared to the tradition DES algorithm with one key for encryption and decryption.

DES was always considered a strong encryption method, but the strength is relative. The strength of an encryption algorithm is measured by how resilient it is against attacks. From the outset, it was known that DES was susceptible to brute force attacks and was in fact cracked in 1997. It is observed that the bigger the key, the more difficult it is to attack the cryptosystem.

Although Triple DES runs slower than DES, it is proved to be more secure against brute force attacks. There are multiple keying options to choose from, but the one which is the strongest is making all 3 keys independent of each other. There are 168 independent key bits, and the number of steps that a meet-in-the-middle would require for breaking the encryption is 2^{112}.

V. Results

Following are the results of the evaluation metrics - Encryption Time and Decryption Time:

TABLE I: Comparison of Triple DES and DES

Input and Algorithm	Encryption Time	Decryption Time
Plain Text a45d6a0f2c80dd4		
Cipher Text 2b510a3183af2d3b		
Triple DES	0.000171 secs	0.000178 secs
DES	0.000047 secs	0.000050 secs
Plain Text 2da55a2043fcf6c7		
Cipher Text d4cb0a600f32c53e		
Triple DES	0.000156 secs	0.000179 secs
DES	0.000046 secs	0.000048 secs
Plain Text 523aeb98a44083d0		
Cipher Text be7db2990bed76f1		
Triple DES	0.000175 secs	0.000153 secs
DES	0.000046 secs	0.000045 secs
Plain Text d5cfc14e4e3b08f3		
Cipher Text f51366d9ac03ed86		
Triple DES	0.000175 secs	0.000164 secs
DES	0.000046 secs	0.000055 secs

VI. Conclusion

DES was a big step forward in the data security domain, and despite its inherent limitations, people did not want to discard it due to the large computational and financial power required to develop a new cryptographic algorithm. The pragmatic approach then was to improve on the already existing algorithm to try to work around the limitations. 3DES simply extended the key size by applying DES three times, thus solving the problem temporarily. However, even 3DES is susceptible to brute force and man in the middle attacks, and can be broken in reasonable time today. This led to the development of Advanced Encryption Standard(AES), to overcome the drawbacks of 3DES. AES is being used very frequently today,and as of now, no successful cryptanalysis attacks against AES have been discovered.