Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 4, April 2017, pg.353 – 355

SECURITY ENHANCEMENT USING TRIPLE DES ALGORITHM

Akhil Arya
Computer Science Department, IIMT College of Engineering, Greater Noida, UP, India
Email: theakhilarya@gmail.com

Abstract: Data is the fuel that drives everyone from an individual to a global company to do anything. And in the age of digitalization when we are trying to gravitate ourselves from pen and paper to mouse and keyboard. This is essential to make sure that the data remains secure. Triple DES Algorithm is one of the ways to achieve the satisfaction that our data is secured from any preying eyes. The algorithm uniquely defines the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form.

Keywords: Digitalization, Triple DES Algorithm, Secure, Cipher, Mathematical steps

I. INTRODUCTION

Today when substantial amount of data is flowing all around us. It becomes significant to ensure that the data remains secure from any unauthorized user. To deliver such a reliability we used Triple DES Algorithm to develop such a system which stores data in cipher form. The sender can encrypt the message using their own key and send it to the receiver. On the receiver's end, the message will arrive in encrypted form. So as to decrypt the message, receiver will have to enter the exact key used to encrypt the message in order to read the message. This will ensure that no one other than two parties who have keys will be able to read the message.

II. LITERATURE SURVEY

Data Encryption Standard (DES) was the developed in 1974 by an IBM candidate based on earlier algorithm, Horst Feistel's Lucifer cipher. This algorithm was developed for US government's computer security needs. Later, many attacks were recorded that confronted several weaknesses of DES Algorithm. Brute force attack became major reason for the failure of DES algorithm as there was a fixed key size of 56bits (+ 8 parity bits). So with the advanced computational power it became possible to know the actual key. As an enhancement of DES Algorithm, the Triple DES Algorithm was proposed. Triple DES applies DES algorithm three times to each data block. 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.[1]

III. Proposed System

Since now we know that DES is lacking strength for many applications, mainly due to the 56-bit key size being too small. Triple DES Algorithm effectively responds to this issue of smaller key size. Triple DES algorithm uses three times of key size originally introduced in DES algorithm. The process includes three set of keys each of 64 bit which results in 3 X 64 = 192 bits. There are three main steps involved in encrypting the data. Firstly, the data is encrypted using the first key, then the output of previous step is decrypted using the second key and then finally the output of the second step is again encrypted with the third key. As similar to DES algorithm, 8 bits from every set of key (64 bits) are used as parity bits. This procedure helps in encrypting data in many complicated layers with a longer key size.

IV. Algorithm

Triple DES Algorithm is same as DES Algorithm except we apply it three time. So in order to understand Triple DES, we need to understand how DES Algorithm is used to encrypt data and generating key. DES performs an initial permutation on the 64 bits block of data. Then it splits it into two parts named L and R, each 32 bit sub-blocks. Then the encryption of block of message takes place in 16 rounds. From the input key, sixteen 48 bit keys are generated, one for each round. The right half is expanded from 32 to 48 bits. The result is combined with the sub-key for that round using the XOR operation. Using the S-boxes the 48 resulting bits are then transformed again to 32 bits, which are subsequently permutated again using yet another fixed table. This by now thoroughly shuffled right half is now combined with the left half using the XOR operation. In the next round, this combination is used as the new left half. This process is conducted for all 16 rounds. The function f in following figure makes all mapping in all rounds.[2]

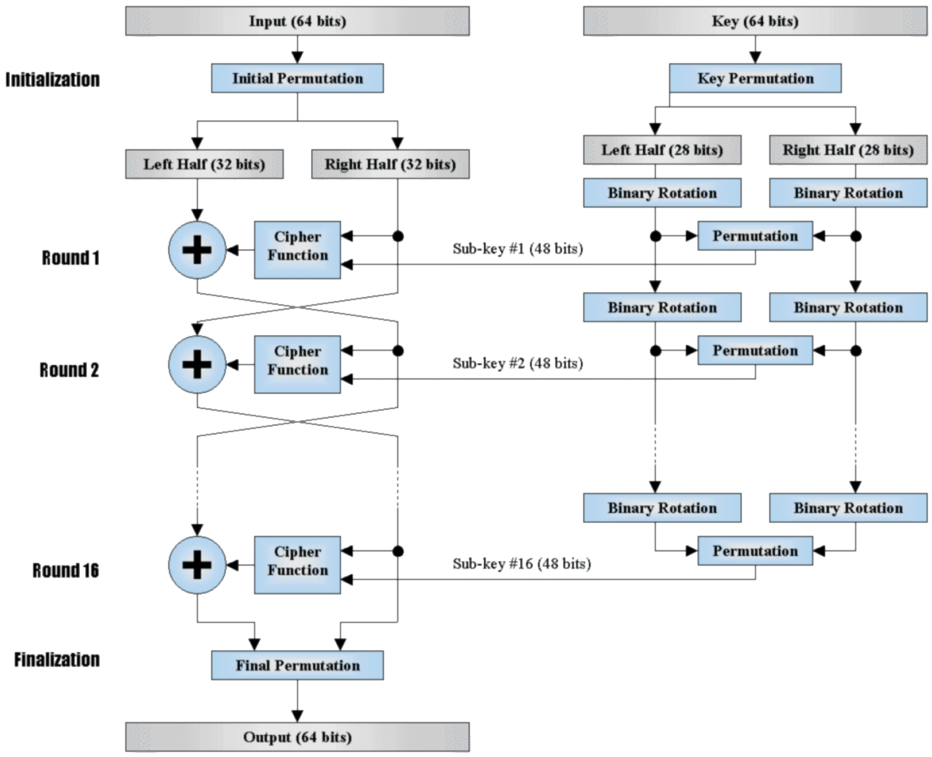

Figure 1. Implementation of DES Algorithm and key generation[3]

This completes the process of DES Algorithm. To increase the key size and the complexity of the encryption process, Triple DES encrypts any data three times and uses different keys for each step. We use three sets of 64 bits and 8 bits from each set is used as parity bits. So we are left with effective 56 bits which gives us 3 X 56 = 168 bits.[4]

The process of encryption is as follows –

1. Encrypt the data using DES Algorithm with the help of first key.
2. Now, decrypt the output generated from the first step using DES Algorithm with the help of second key.
3. Finally, encrypt the output of second step using DES Algorithm with the help of third key.

The decryption process of any cipher text that was encrypted using Triple DES Algorithm is the reverse of the encryption process i.e.,

1. Decrypt the cipher text using DES Algorithm with the help of third key.
2. Now, encrypt the output generated from the first step using the DES Algorithm with the help of second key.
3. Finally, decrypt the output of the second step using DES Algorithm with the help of first key.

The process of encrypt – decrypt – encrypt help complexing things and securing the data. The three keys can also be same or two of them can be same. But it is recommended to use all the three keys different.

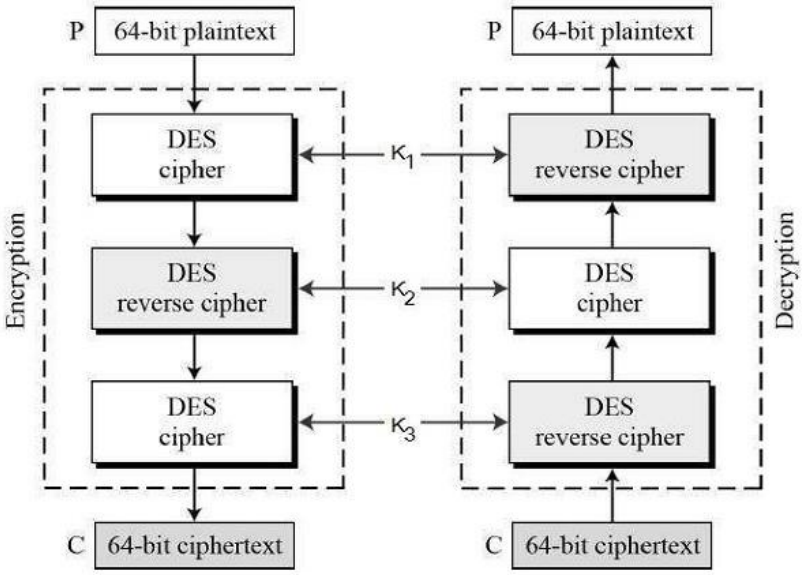

Figure 2. Implementation of Triple DES Algorithm[5]

V. Conclusion

The main purpose of this project was to ensure that the sensible data of every individual should remain secure from any kind of attack. I believe that Triple DES Algorithm has proven itself to be more secure than DES Algorithm for securing our data. With its significant key size, it is very effective against brute force attack. So it is recommended to use Triple DES Algorithm as encryption algorithm.

References

[1] Simar Preet Singh, and Raman Maini, International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp.125-127.

[2] Data Encryption Standard, Tutorials Point, https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm

[3] Development and Analysis of Block Ciphers and the DES system, http://homepage.usask.ca/~dtr467/400/

[4] Triple DES, Tutorials Point, https://www.tutorialspoint.com/cryptography/triple_des.htm

[5] Triple DES, Tutorials Point, https://www.tutorialspoint.com/cryptography/triple_des.htm

