A Synopsis on

Image Encryption using Triple DES Algorithm

Abstract:

In today’s world almost all digital services like internet communication, medical and military imaging systems, multimedia system needs a high level and Protected security. There is a need for security level in order to safely store and transmit digital images containing critical information. This is because of the faster growth in multimedia technology, internet and cell phones. Therefore there is a need for image encryption techniques in order to hide images from such attacks. In this system we use Triple DES (Data Encryption Standard) in order to hide image. Such Encryption technique helps to avoid Active and Passive Attacks.The triple DES algorithm is based on The DES algorithm itself its uses same method as that of the DES but the difference is that it uses 3 keys rather than just one. For the encryption process it initially encrypts the data using just one key and then decrypts the data using another different key and then finally encrypts the data again using another key. For the decryption process it is the reverse of the encryption process it initially decrypts the cipher data using one key, then encrypts the data using another key and then finally decrypts the data back to its original form using the another different key. This algorithm uniquely defines the mathematical steps required to transform the image into a cryptographic cipher and also to transforms the cipher image back to its original form.

Table of Contents :

1.INTRODUCTION

In this era of universal electronic connectivity, the possibility of data damage or stolen is very high that’s why it is need of the time is to secure data from the those group .The tremendous growth in computer systems and inter connection with networks have increased depends on company or individual based on information stored and communicated using this system. There is need to protect the data from disclosure and to protect systems from network based attacks.

Cryptography:

Cryptography is a technique which is intended to transform the data and can be used to provide various security related concepts such as confidentiality, data integrity, authentication, authorization and non-repudiation. Secure the information and other services is very important thing by using the security mechanism we have to protected from unintended or unauthorized access, change or destruction. Cryptography is the art of secret writing to hide information secret or keeping message secure. A secure network must have integrity, so that all of the information stored in always correct and protected without any redundant data.which are used to reduce network threats . Basically encryption/decryption are the fundamental function of cryptography, which is used to hide the information from the unauthorized users so that chances of threats also reduced. The aim of many cryptosystems is to make their data computationally infeasible to crack by intruders. It can provide integrity as it can be used to detect any changes which may have happened to the data, and it can provide accountability as it can be used to verify the origin of the data.In encryption simple message (the plaintext) converted into unreadable form called cipher text (scrambled message after encryption). While decryption the cipher text is converted into plain text(original form) Many encryption algorithms are widely available and used in information security.

2. EXISTING METHODS

DES(Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It is based on the IBM proposed algorithm called Lucifer. DES became a standard in 1974. Since that time, many attacks and methods recorded that exploit the weaknesses of DES, which made it an insecure block cipher. It has a key size of 56 bits.
Problem with DES is,it has only 2^{56} of combinations

Double DES which applies the algorithm twice to the plain text with a different key each time.

$$C=Enc(K_{2,}Enc(K_{1,}P))$$

$$P=Dec(K_{1,}Dec(K_{2,}C))$$

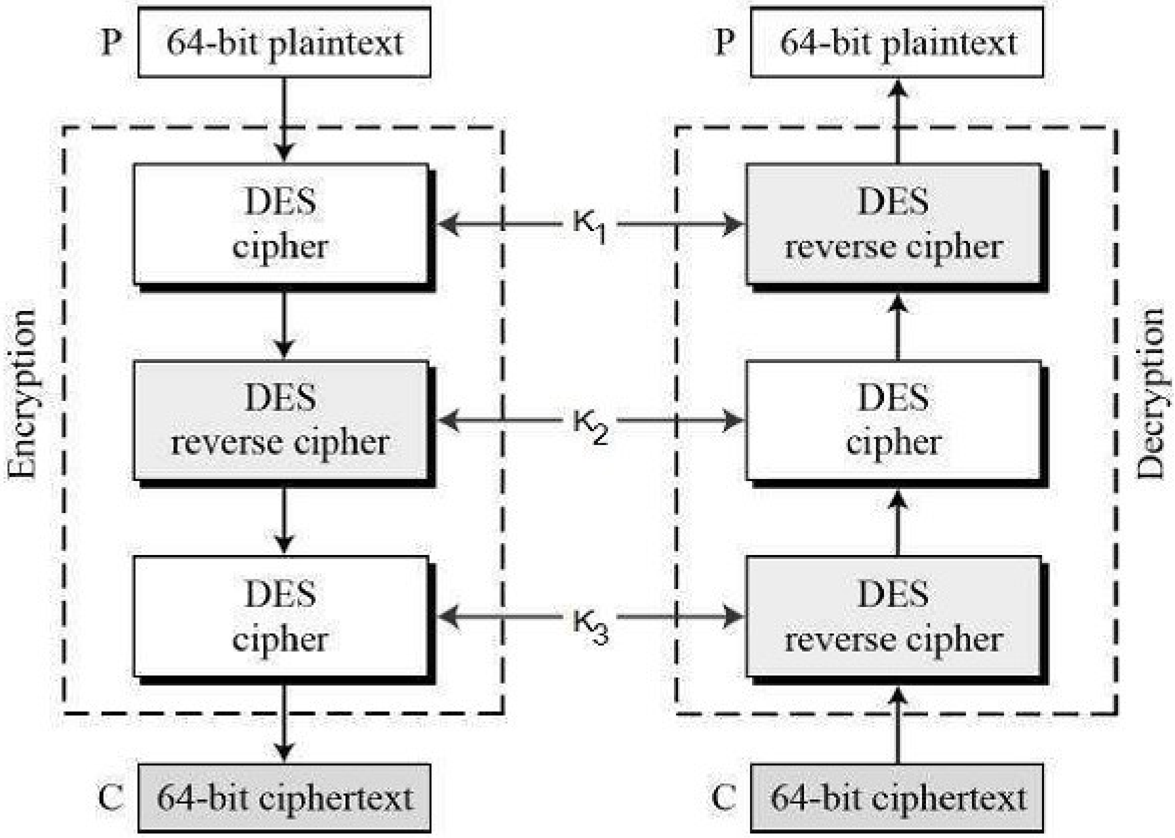
It has 2^{112} of combinations.Due to the MITM attack (Meet in the middele) it lowers the attack complexity of finding the key easyliy , attacker can find out keys in less time.It has $O(2^{56})$.

PROPOSED METHOD:

An enhancement of DES and Double DES, the 3DES (Triple DES) encryption standard was proposed. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level.

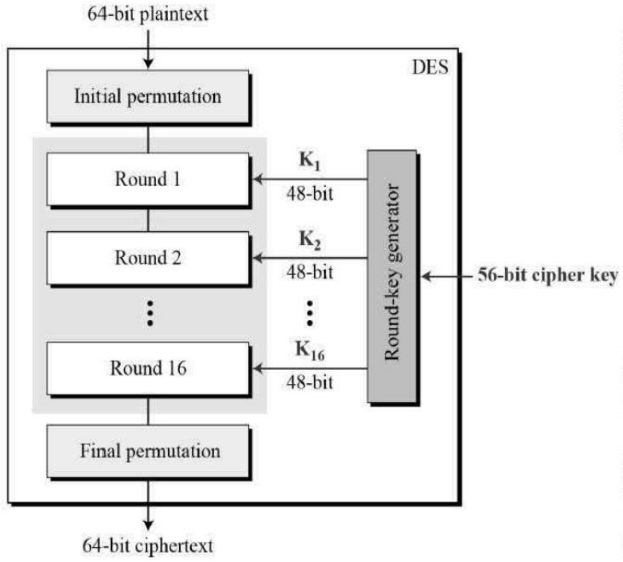
Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.

ARCHITECTURE OF Triple DES :



METHODOLOGY :

Data Encryption Standard The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).

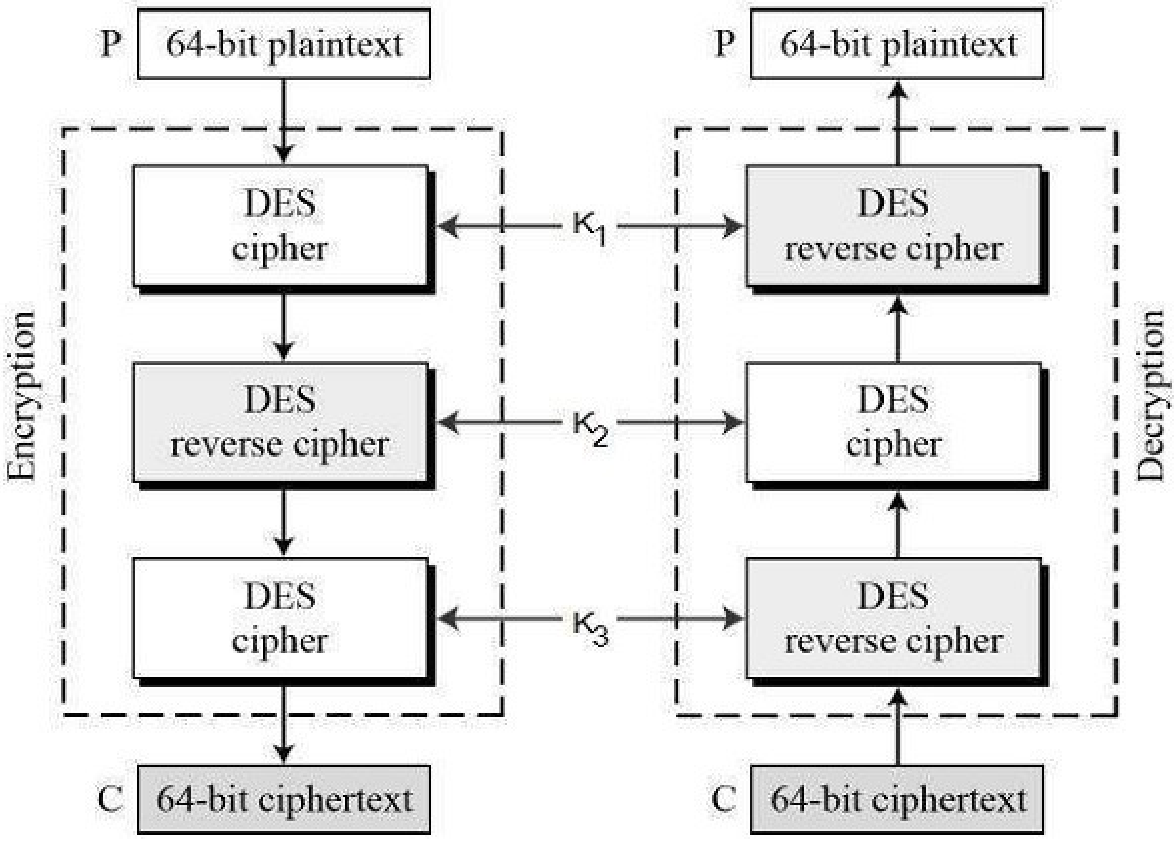


Triple-DES:

Triple-DES is a process in which we encrypt a nimage, text or video using 56 bit two keys or 128 bit keys. This kind of process may be secure but still has its flaws. To overcome this flaw we encrypted out file with three 56 bit keys instead of two keys. Hence making it more secure. In the previous referred case study there was only two keys were used for encryption process. Triple-DES process follows EDE(Encryption,Decryption,Encryption)model. EDE model states that every file or text must be encrypted twice and decrypted once in a sequential order to perform encryption process. First it encrypts using one secret key and then decrypts using a different secret key finally encrypts using same encrypt key. So the flaw was if the hacker got to know one secret key it’s very easy to apply brute force attack. Hence to overcome this flaw we are using three different keys for every EDE process. EDE uses 192 bit keys out of which only 168 bits are used for encryption process.

Still a very strong algorithm even though we don’t use the last eight bits. Which makes it more secure over a network.As the security weaknesses of DES became more apparent, 3DES was proposed as a way of extending its key size without having to build an entirely new algorithm. Rather than using a single key as in DES, 3DES runs the DES algorithm three times, with three 56- bit keys:

•Key one is used to **encrypt** the plaintext.
•Key two is used to **decrypt** the text that had been encrypted by key one.
•Key three is used to **encrypt** the text that was decrypted by key two.



IMPLEMENTATION :

Algorithm:

Step1: Choose Encryption || Decryption
Step2: Opening file name and image
Step3: Give password as Key
Step4:

$$\text{Cipher Text} = E_{K3}(D_{K2}(E_{K1}(\text{plain text})))$$

DES encrypts with K_1, DES decrypt with K_2, then DES encrypt with K_3.

$$\text{Plain Text} = D_{K1}(E_{K2}(D_{K3}(\text{ciphertext})))$$

DES decrypt with K_3, encrypt with K_2, then decrypt with K_1.

Conclusion :

Triple DES algorithm to encrypt and decrypt the data. This provides better process of secure encryption and decryption . It is more secure and faster than double DES. As it has lengthy key chances of attacking the data is less. So, it provides security in storage and transmission of data.