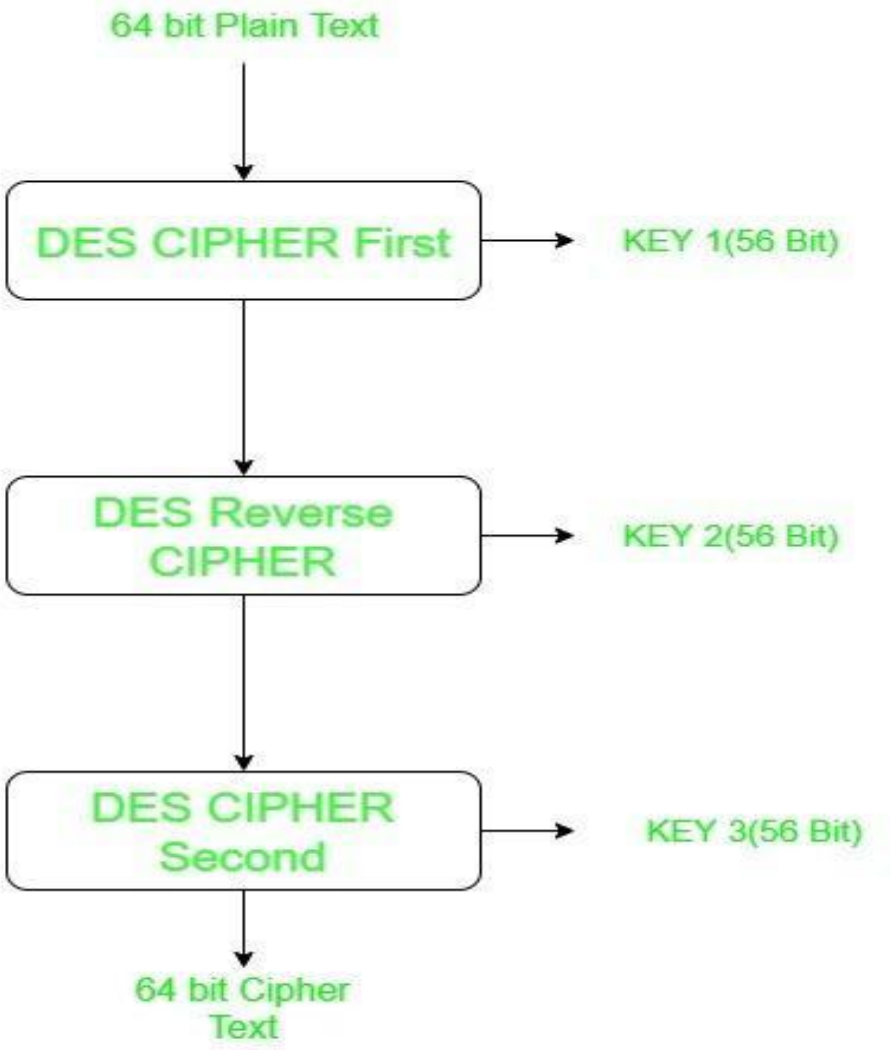
IMAGE SECURITY THROUGH TRIPLE DES

(Image Encryption & Decryption through Triple DES)

SYNOPSIS

Introduced in 1998, 3DES, also known as Triple DES, Triple DEA, TDEA, or the Triple Data Encryption Algorithm, is a cryptographic cipher. It is a symmetric key block cipher, meaning that the same key is used to encrypt and decrypt data in fixed-length groups of bits called blocks.

It is called "Triple DES" because it applies the DES cipher three times when encrypting data. When DES was originally developed in 1976, it used a key size of 56 bits, which was a sufficient level of security to resist brute-force attacks. Since then, computers have become cheaper and more powerful, enabling the 3DES algorithm to apply DES three times consecutively, essentially stopping brute-force on modern computers.



It works by taking three 56-bit keys (K1, K2 and K3), and encrypting first with K1, decrypting next with K2 and encrypting a last time with K3.

3DES has two-key and three-key versions. In the two-key version, the same algorithm runs three times, but uses K1 for the first and last steps. In other words, K1 = K3. Note that if K1 = K2 = K3, then Triple DES is really Single DES.

Triple DES was created back when DES was becoming weaker than users accepted. As a result, they sought an easy way to get more strength. In a system that is dependent on DES, making a composite function out of multiple passes of DES is likely to be easier than bolting in a new symmetric cipher. This has the added benefit of sidestepping the political issues that arise from arguing about the relative strength of a new cipher versus DES.

Working of Image Security by Triple DES

Image will be Encrypted by Triple DES algorithm and then will be Decrypted. This will protect Information as Images from active and passive attacks.

This System will be made through python programming.