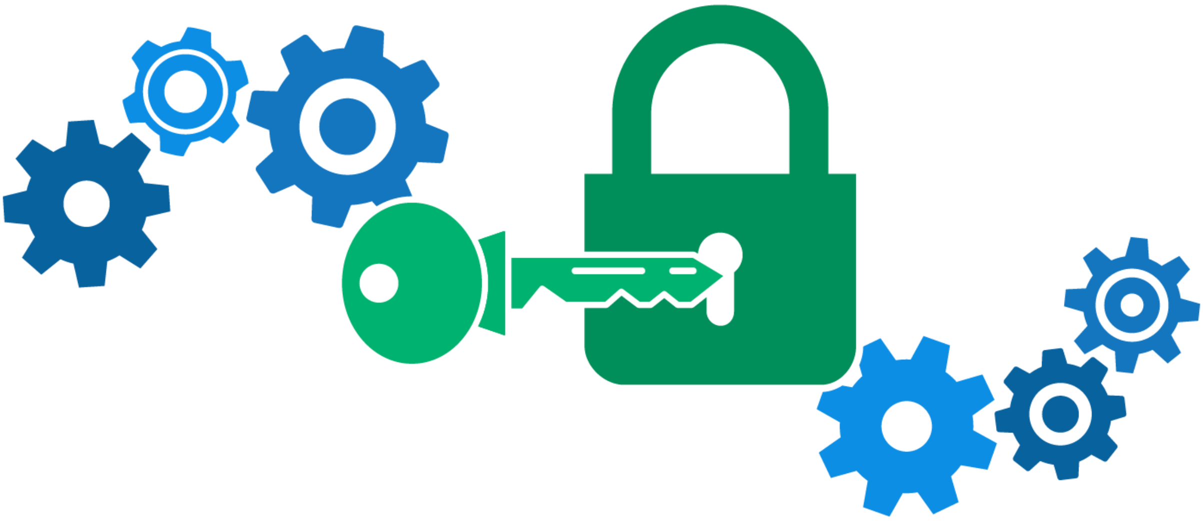
Image encryption using Triple des.



S.Lavan

Reg no:710719205026

Dr.Ngp Institute of Technology

R.Tharshan

Reg no:701719205053

Dr.Ngp Institute of Technology

Contents:

Abstract:

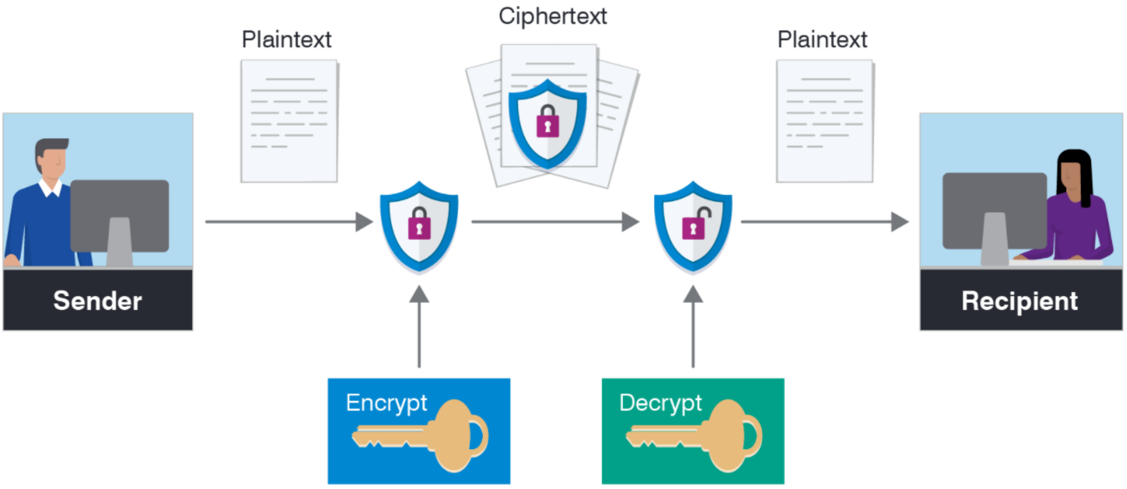
In today’s world almost all digital services like internet communication, medical and military imaging systems, multimedia system needs a high level and Protected security. There is a need for security level in order to safely store and transmit digital images containing critical information. This is 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.

Introduction:

Data Encryption Standard (DES) is the block cipher which takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. It is a symmetric encryption technique which means both sender and receiver use a shared key to encrypt and/or decrypt the data.The problem of this technique is that if the key is known to others the entire conversation is compromised. The 3DES block size is 64 bits and also uses a key to customize the transformation, so that decryption can only be performed by those who know the particular key used to encrypt. The key basically consists of 64 bits however, only 56-bits of these are actually used by the algorithm. Eight bits are used solely for checking parity, and thereafter discarded. Hence the “effective key length is 56-bits” and it is always quoted. Every 8th bit of the selected key is discarded i.e., positions 8, 16, 24, 32, 40, 48, 56, 64 are removed from the 64-bit key leaving behind only the 56-bit key.we are using python pycryptodome library to encrypt and decrypt tha Image.

Existing methods:

What is encryption?



It is process encoding a layer on the raw informations like images and documents etc.. for security purposes.Encryption is done by using keys..Private and public keys.

Types of encryption:

1.Asymmetric Encryption

In public-key encryption schemes, the encryption key is published for anyone to use and for encrypting messages. Only the receiving party has access to the decryption key that enables messages to be read. Public-key encryption was first described in a secret document in 1973. Before that, all encryption schemes were symmetric-key (also called private-key).

2.Symmetric Encryption

In symmetric-key schemes, the encryption and decryption keys are the same. Communicating parties must have the same key in order to achieve secure communication.

Encryption Algorithms:

1.Triple des encryption

2.Twofish encryption algorithm

3.Blowfish encryption algorithm

4.IDEA encryption algorithm

5.MD5 encryption algorithm etc….

Hashing:

Hashing is a form of encryption that uses a specialized one way encryption key. If you hash a given volume of data, it will produce a unique output string to that data, but it is impossible to reconstruct the data from the output string. You can re-encode the original data and compare it to the result string to verify it. This can serve as a type of error correction in encoding. Hashing a message and providing that value to your correspondents ensures that they can hash the message themselves and compare the values. As long as the two output strings match, recipients know the message is complete and unaltered.

Existing Encryption Algorithms:

AES.

The Advanced Encryption Standard (AES) is the trusted standard algorithm used by the United States government, as well as other organizations. Although extremely efficient in the 128-bit form, AES also uses 192- and 256-bit keys for very demanding encryption purposes. AES is widely considered invulnerable to all attacks except for brute force. Regardless, many internet security experts believe AES will eventually be regarded as the go-to standard for encrypting data in the private sector.

RSA.

RSA is a public-key encryption asymmetric algorithm and the standard for encrypting information transmitted via the internet. RSA encryption is robust and reliable because it creates a massive bunch of gibberish that frustrates would-be hackers, causing them to expend a lot of time and energy to crack into systems.

Blowfish.

Blowfish is another algorithm that was designed to replace DES. This symmetric tool breaks messages into 64-bit blocks and encrypts them individually. Blowfish has established a reputation for speed, flexibility, and is unbreakable. It’s in the public domain, so that makes it free, adding even more to its appeal. Blowfish is commonly found on e-commerce platforms, securing payments, and in password management tools.

Twofish

Twofish is Blowfish’s successor. It’s license-free, symmetric encryption that deciphers 128-bit data blocks. Additionally, Twofish always encrypts data in 16 rounds, no matter what the key size. Twofish is perfect for both software and hardware environments and is considered one of the fastest of its type. Many of today’s file and folder encryption software solutions use this method.

Proposed method with Architecture:

Image encryption using Triple-des algorithm:

In cryptography, Triple DES, officially the Triple Data Encryption Algorithm, is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block.

Block sizes: 64 bits Key sizes: 168, 112 or 56 bits (keying option 1, 2, 3 respectively)

Triple DES is a encryption technique which uses three instance of DES on same plain text.It uses there different types of key choosing technique in first all used keys are different and in second two keys are same and one is different and in third all keys are same.

What is encryption?

1.Encryption is the process of converting plain text into a meaningless text(chipper text).

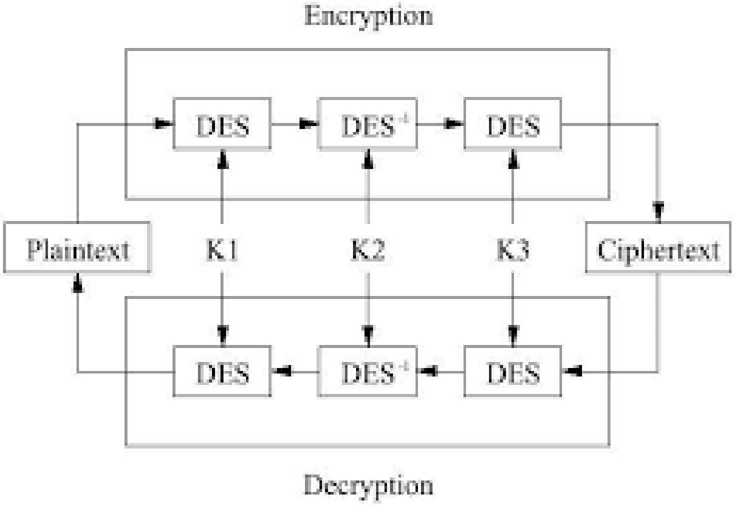
2.Encryption is a process which transforms the original information into an unrecognizable form.

3.This new form of the message is entirely different from the original message.

What is decryption?

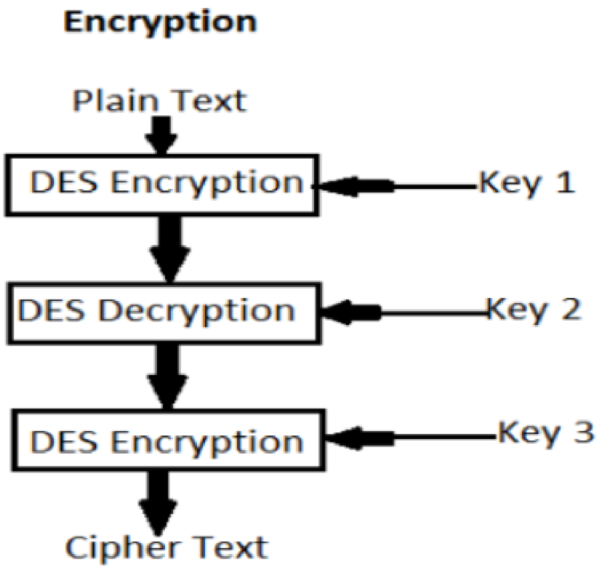
1.It is the process of converting meaningless message (Ciphertext) into its original form (Plaintext)

2. Decryption is a process of converting encoded/encrypted data in a form that is readable and understood by a human or a computer. This method is performed by un-encrypting the text manually or by using keys used to encrypt the original data.



Methodology:

Encryption and decryption using Triple-Des algorithm:



Triple DES Algorithm:

TDES has a fixed data block size of 8 bytes. It consists of the cascade of 3 Single DES ciphers (**EDE: Encryption - Decryption - Encryption**), where each stage uses an independent DES sub-key.

The standard defines 2 Keying Options:

● Option 1: all sub-keys take different values (parity bits ignored). The TDES key is therefore 24 bytes long (concatenation of K1, K2, and K3), to achieve 112 bits of effective security.

● Option 2: K1 matches K3 but K2 is different (parity bits ignored). The TDES key is 16 bytes long (concatenation of K1 and K2), to achieve 90 bits of effective security. In this mode, the cipher is also termed 2TDES

Implementation:

We are using python to do this project.In this project we used pycryptodome python library to encrypt and decrypt the images using Triple des algorithm.

Pycryptodome:

PyCryptodome is a fork of PyCrypto. Here we are using latest version of pycryptodome you can install it by pip install pycryptodome.It brings several enhancements with respect to the last official version of PyCrypto (2.6.1), for instance:

1. Cleaner RSA and DSA key generation (largely based on FIPS 186-4)
2. Random numbers get sourced directly from the OS (and not from a CSPRNG in userspace)
3. Password-protected PKCS#8 key containers
4. Shamir's Secret Sharing scheme
5. It includes sha and many more encryption algorithms.
6. It requires python version more than 2.7.

Working:

1. Running of the Libraries
2. Selecting(Uploading) the Image
3. Triple DES Process
4. Encryption Process
5. Decryption Process

Conclusion:

Encryption is a process of encrypting the plaintext into chipper text(not understood by humans).There is many algorithms and methods to encrypt and decrypt the images and text.Here we are using triple-des encryption algorithm to encrypt and decrypt the Images.Triple-des algorithm is a standard encryption algorithm which is also a stronger algorithm to crack by bruteforcing and other method this algorithm is used to reduce intrusion attacks in between reciver and sender.This method will give more secure to share critical information through images.