GraphicEra
(Deemed to be University)
Accredited by NAAC with Grade A

MINI PROJECT REPORT

PROJECT : IMAGE SECURITY WITH ENCRYPTION

NAME : RIDHANSHU JASROTIA
SECTION: CE-CORE
CLASS ROLLNO.: 31
UNIVERSITY ROLLNO.: 2017359

DECLARATION

I, **RIDHANSHU JASROTIA** student of **B-tech, Semester 3,** Department of Computer Science and Engineering, Graphic Era Deemed University, Dehradun, declare that the technical project work entitled **"Image Security With Encryption"** has been carried out by me and submitted in partial fulfillment of the course requirements for the award of degree in B- tech of **Graphic Era Deemed University** during the academic year **2022-2023**. The matter embodied in this synopsis has not been submitted to any other university or institution for the award of any other degree or diploma.

Date: 26/2/22

GraphicEra
(Deemed to be University)
Accredited by NAAC with Grade A

CERTIFICATE

This is to certify that the project report entitled "IMAGE SECURITY WITH ENCRYPTION" is a Bonafede project work carried out by Ridhanshu Jasrotia, roll no- 2017359, in partial fulfilment of award of degree of B- tech of Graphic Era Deemed University, Dehradun during the academic year 2022-2023. It is certified that all corrections/suggestions indicated for internal assessment have been incorporated. The project has been approved as it satisfies the academic requirements associated with the degree mentioned.

Dr. Manoj Diwaker, (CSE DEPT.)

PROBLEM DEFINITION:

Information security is the most frequently used word by any person, device, or peripheral over the past two centuries. Protection from malicious sources has become an element of the invention or the discovery cycle. Multiple methods of protection are used starting from an easy authentication password to the most complex Cryptography. The advancements of the digital revolution weren't achieved without drawbacks like illegal copying and distribution of digital multimedia documents. To provide protection and data security, different encryption methods must be used.

OBJECTIVE:

The main objective of my project is to produce security to the image-based data with the help of a suitable key and protect the image from illegal copying and distribution. This project has been done using the Triple Data Encryption Standard algorithm for the encryption and decryption of the image.

TOOLS USED:

Visual Studio Code

LANGUAGE USED:

Python

LIBRARIES USED:

- Matplotlib
- pyDes
- tkinter

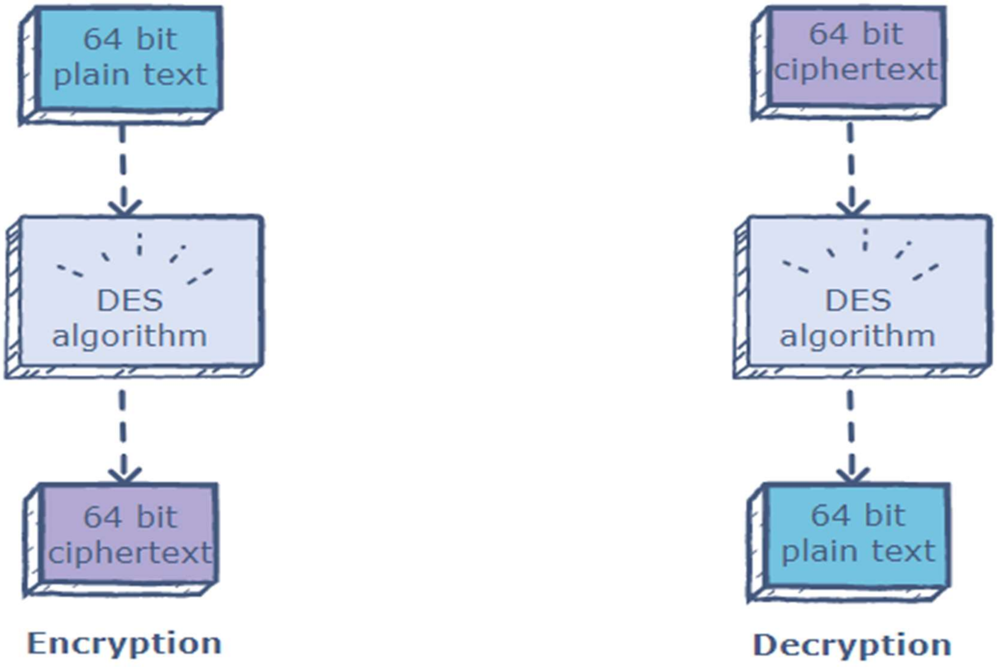
INTRODUCTION:

Today when a considerable amount of information is flowing all around us. It becomes significant to make sure that the info remains secure from any unauthorized user. To deliver such reliability we used Triple DES Algorithm to develop such a system that stores data in cipher form. The sender can encrypt the message with his own key and send it to the recipient. On the receiver's end, the message will arrive in encrypted form. Therefore, to decrypt a message, the recipient must enter the same key that was used to encrypt the message in order to read it. This will make sure that no one apart from the two parties who have the keys can read the message.

ABOUT THE TRIPLE DATA ENCRYPTION STANDARD (3- DES) ALGORITHM:

Triple-DES Algorithm is the same as DES Algorithm except we apply it thrice. So to know Triple DES, we must understand how
data is encrypted using DES Algorithm.

(DES) is a block cipher algorithm that takes a 64-bit block of plaintext and converts it into ciphertext using a 48-bit key. This is a symmetric key algorithm. That is, the keys used to encrypt and decrypt the data must be the same.



Encryption and decryption using the DES algorithm.

DES performs an initial permutation on the 64 bits block of information. Then it divides it into two parts named R and L, sub-blocks with 32-bit each. Then the blocks of messages are encrypted with 16 rounds. From the input key, sixteen 48 bit keys are generated, one for every round. The right half will be extended from 32 bits to 48 bits. The result's 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 one more fixed table. This fully shuffled right half is combined with the left half by XOR. In the next turn, this combination will be used as the new left half. This process is conducted for all 16 rounds.

Triple Data Encryption Standard (3-DES): As the security weaknesses of DES became more frequent, 3DES was proposed as a way of extending its key size without having to create a completely new algorithm. Instead of using a single key as in DES, 3DES runs the DES algorithm thrice, with three 56-bit keys.

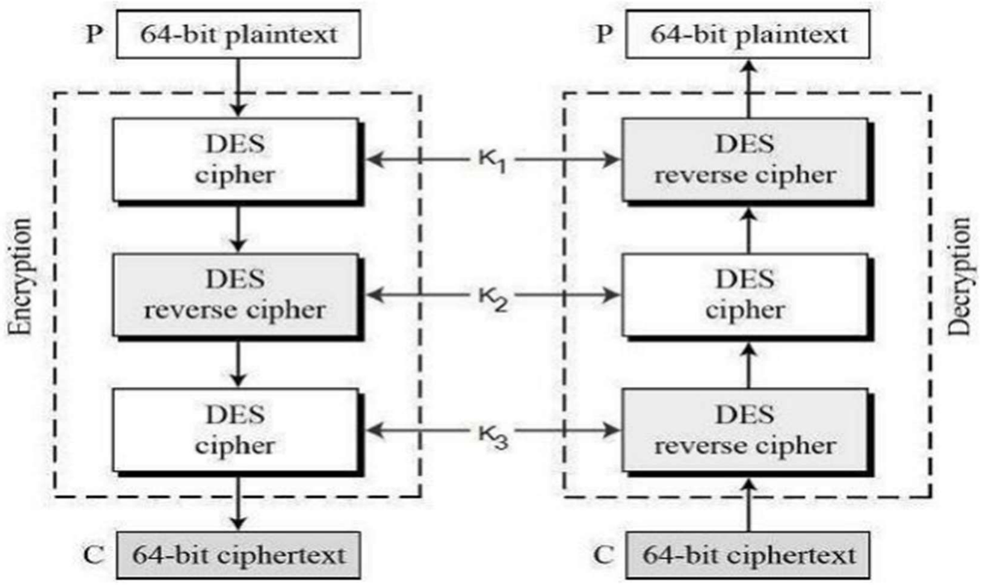
● Key one is used to encrypt the plaintext.

● To decrypt text encrypted with key 1, key 2 is used.

● To encrypt the text that was decrypted by key two, key three is used.

Before using 3DES, the user first generates and distributes a 3DES key K consisting of three different DES keys K1, K2, and K3. This means that the actual 3DES key has a length of 3×56 = 168 bits.

The encryption program is illustrated as follows –



The encryption-decryption process is as follows –

- Using single DES with key K1, Encrypt the plaintext blocks.
- Then use the single DES with key K2 to decrypt the output from step 1.
- Finally, use single DES with key K3 to encrypt the output from step 2.
- The output of step 3 will be ciphertext.
- The decryption of a ciphertext is a reverse process. The user first decrypts with K3, then encrypts with K2, and finally decrypts with K1.

WORKING:

Triple-DES encryption uses a triple-length DATA key consisting of three 8-byte DES keys to encrypt 8-byte data using the following method:

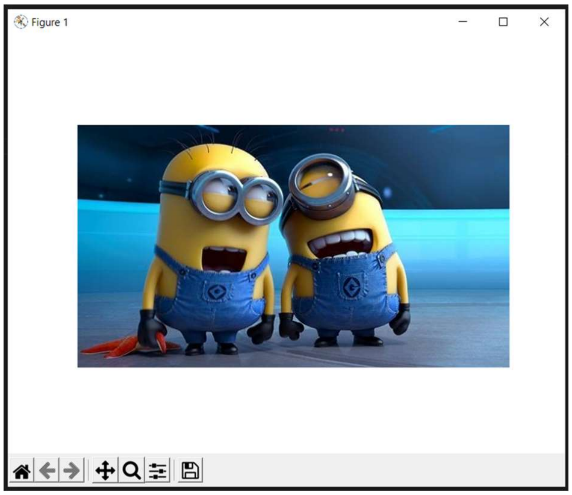
- Using the first key, encipher the data.
- Using the second key, decipher the result.
- Encipher the second result using the third key.

To decrypt data encrypted with Triple DES, do reverse the procedure:

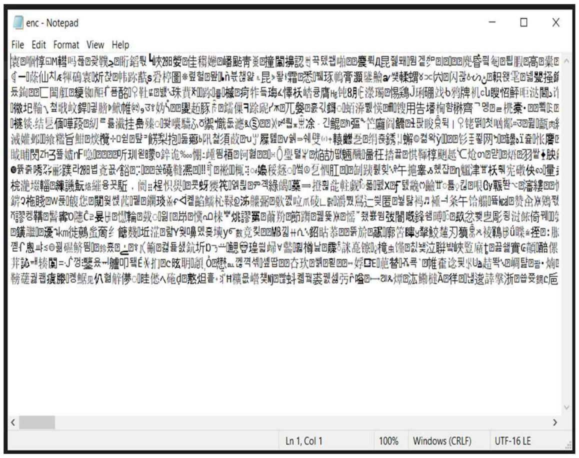
- Using the third key, decipher the data.
- Using the second key, encipher the result.
- Using the first key, decipher the second result.

PRACTICAL WORKING:

ORIGINAL IMAGE

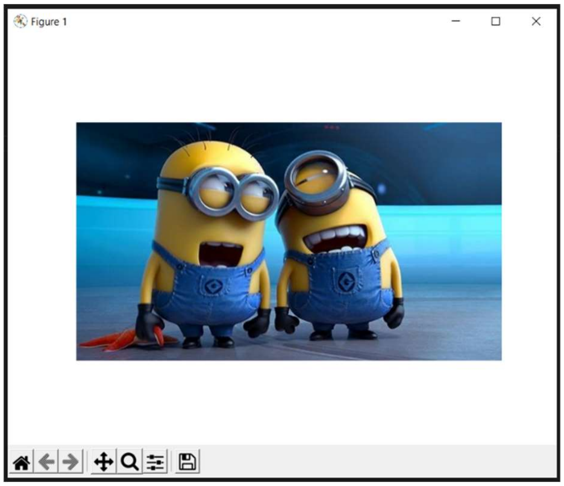


ENCRYPTED IMAGE



[illegible]

DECRYPTED IMAGE



CONCLUSION:

The main purpose of this project was to make sure that the sensible data of every individual should remain secure from any type of attack. I believe that Triple-DES Algorithm has proven itself to be safer than DES Algorithm for securing our data. With its significant key size, it is very effective against brute force attacks. So it's recommended to use Triple DES Algorithm as an encryption algorithm. It involves an Encryption and Decryption process which will be easier for receiver and sender to understand and communicate. This System will protect the Message through both active and passive attacks. This method will run on any platform like Cloud, IDE, or Compilers.