IMAGE SECURITY BY TRIPLE DES

- Mehul Thuletiya (210303108237)

CONTENT

1. Abstract
2. DES
3. Triple DES
4. Encryption Decryption
5. Triple DES Algorithm
6. Process
7. Implementation
8. References

Abstract

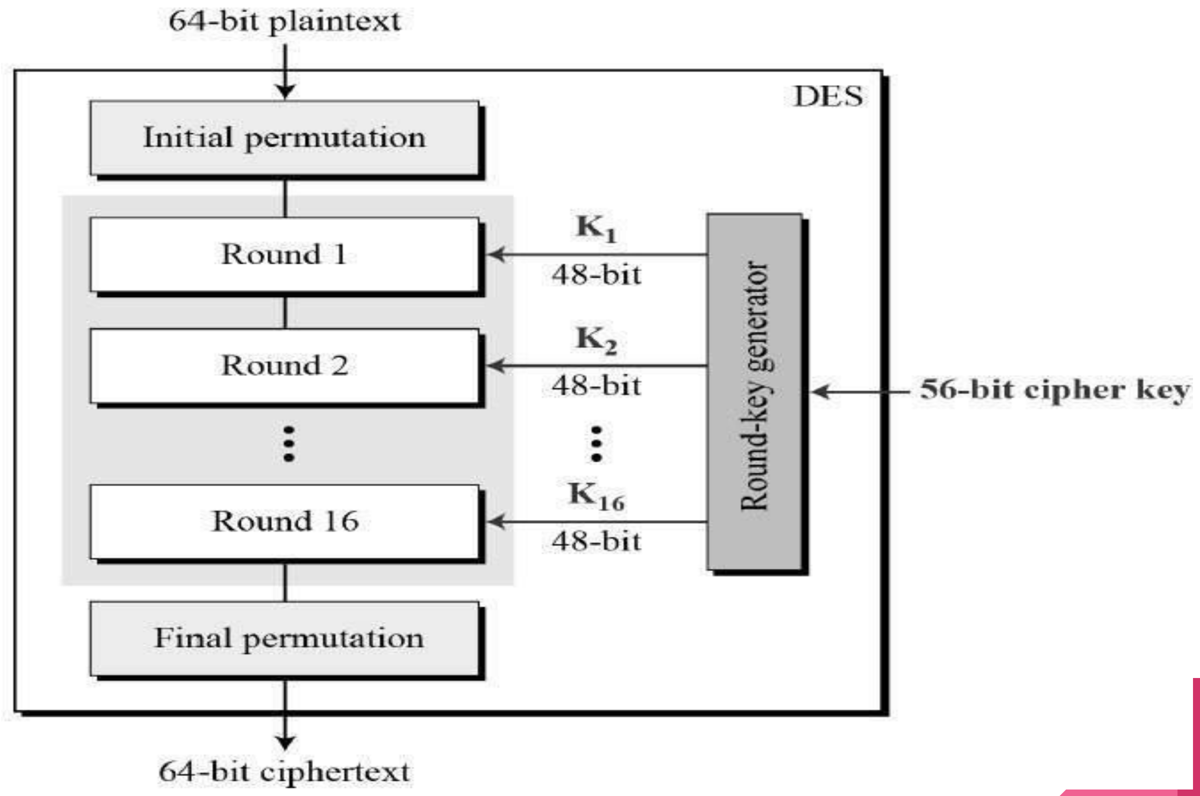
In today’s world almost all digital services like internet communication, medical and military imaging systems, multimedia system needs a high level and Protected security. There is a need for security level in order to safely store and transmit digital images containing critical information. This is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

DES : 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)

DES Structure



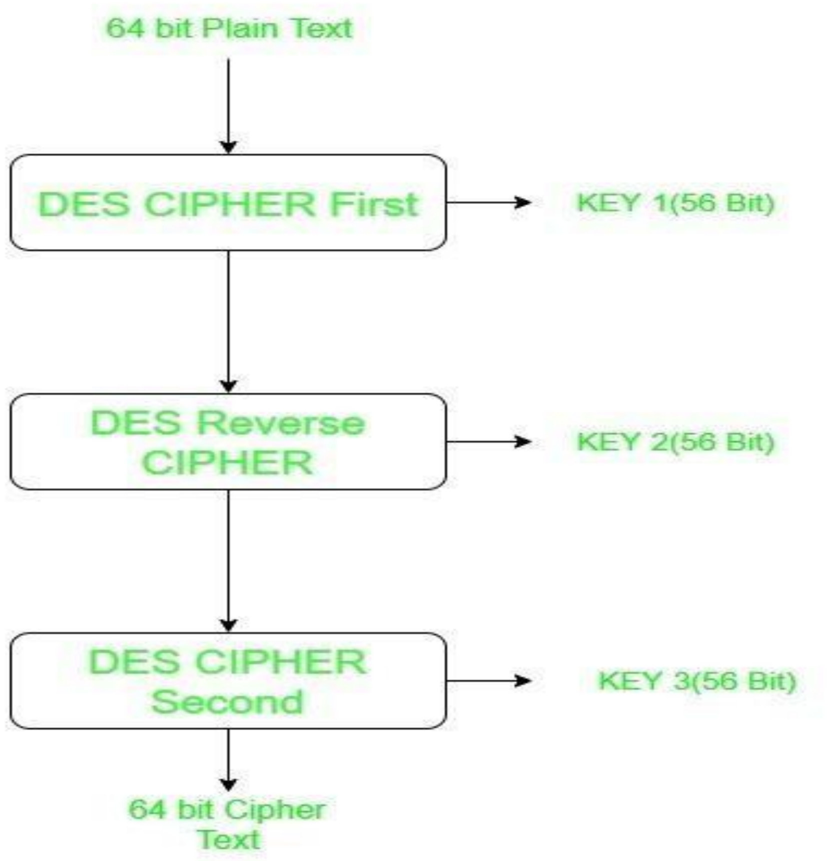
Triple DES

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.

Triple DES Structure



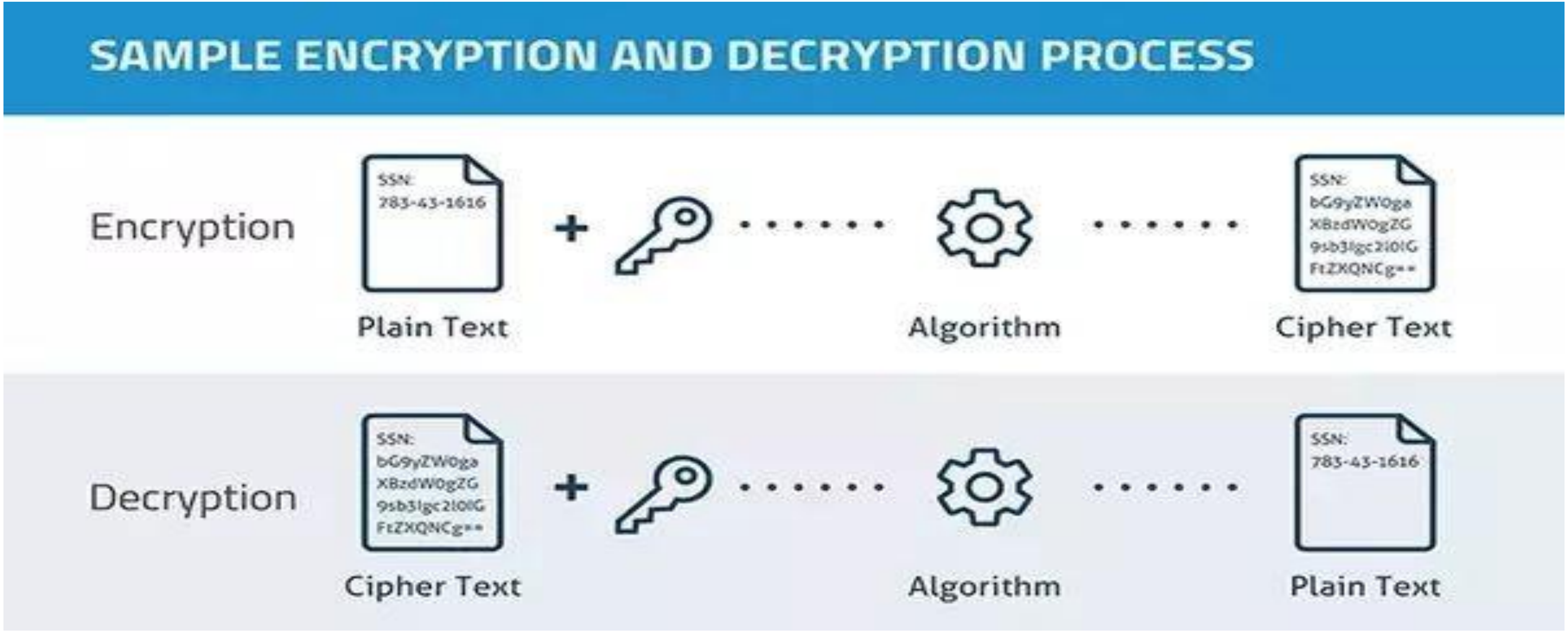
Encryption Decryption

Encryption is the process of converting normal message (plaintext) into meaningless message (Ciphertext).

Encryption is a process which transforms the original information into an unrecognizable form. This new form of the message is entirely different from the original message. That's why a hacker is not able to read the data as senders use an encryption algorithm.

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

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.



SAMPLE ENCRYPTION AND DECRYPTION PROCESS

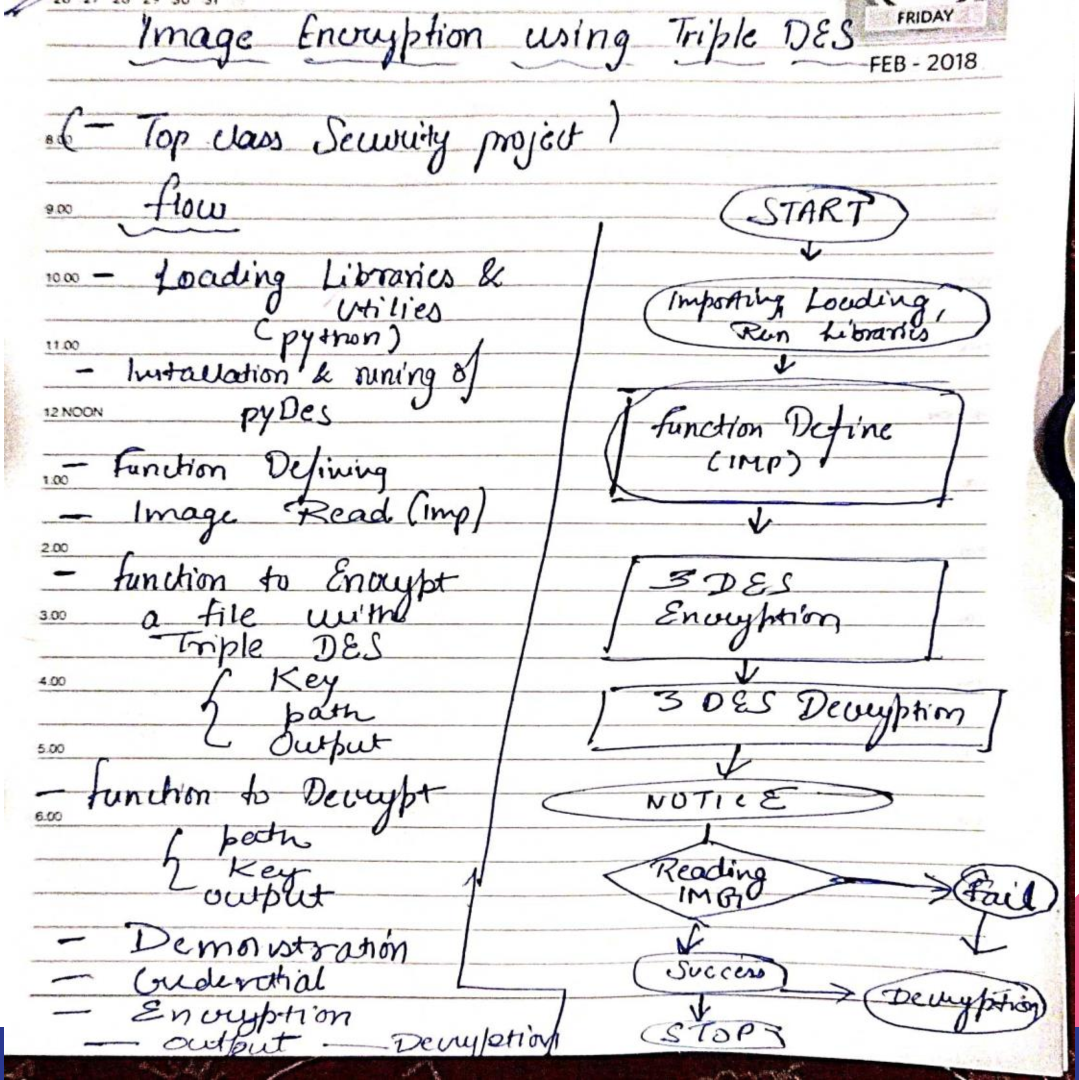
Triple DES Algorithm

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.

Process



FRIDAY

FEB - 2018

Image Encryption using Triple DES

8.00 (– Top class Security project)

9.00 flow

10.00 – Loading Libraries & Utilies (python)

11.00 – Installation & runing of pyDes

12 NOON

1.00 – Function Defining

– Image Read (imp)

2.00 – function to Encrypt a file with

3.00 Triple DES

4.00 { Key
path
5.00 Output

– function to Decrypt

6.00 { path
Key
output

– Demonstration

– Credential

– Encryption

– output – Decryption

Working

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

: Project Code is in Python Programming

References

1. Data Encryption Standard (tutorialspoint.com)
2. DES (Data Encryption Standard): DES Algorithm and Operation (simplilearn.com)
3. Triple DES — PyCryptodome 3.210b0 documentation
4. What is the Data Encryption Standard (DES)? | Encyclopedia (hypr.com)
5. Data encryption standard (DES) | Set 1 - GeeksforGeeks