EXPOSYS DATA LABS

IMAGE ENCRYPTION & DECRYPTION THROUGH TRIPLE DES

Project Report

Name : Aniket S Datar
E mail : anidatar2@gmail.com
Duration: December 21 2021 - January 22 2022

IMAGE ENCRYPTION USING TRIPLE DES

INTRODUCTION

Cryptography:

Cryptography provides for secure communication in the presence of malicious third-parties—known as adversaries. Encryption uses an algorithm and a key to transform an input (i.e., plaintext) into an encrypted output (i.e., ciphertext). A given algorithm will always transform the same plaintext into the same ciphertext if the same key is used.

Algorithms are considered secure if an attacker cannot determine any properties of the plaintext or key, given the ciphertext. An attacker should not be able to determine anything about a key given a large number of plaintext/ciphertext combinations which used the key.

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

Description: Earlier cryptography was effectively synonymous with encryption but nowadays cryptography is mainly based on mathematical theory and computer science practice.

Modern cryptography concerns with:

Confidentiality - Information cannot be understood by anyone

Integrity - Information cannot be altered.

Non-repudiation - Sender cannot deny his/her intentions in the transmission of the information at a later stage

Authentication - Sender and receiver can confirm each

Cryptography is used in many applications like banking transactions cards, computer passwords, and e- commerce transactions.

Three types of cryptographic techniques used in general.

1. Symmetric-key cryptography

2. Hash functions.

3. Public-key cryptography

Symmetric-key Cryptography: Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.

Public-Key Cryptography: This is the most revolutionary concept in the last 300-400 years. In Public-Key Cryptography two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key remains a secret. The public key is used for encryption and for decryption private key is used.

Hash Functions: No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.

symmetric cryptography, the same key is used for both encryption and decryption. A sender and a recipient must already have a shared key that is known to both. Key distribution is a tricky problem and was the impetus for developing asymmetric cryptography.

With asymmetric crypto, two different keys are used for encryption and decryption. Every user in an asymmetric cryptosystem has both a public key and a private key.
The private key is kept secret at all times, but the public key may be freely distributed.

Data encrypted with a public key may only be decrypted with the corresponding private key. So, sending a
message to John requires encrypting that message with John's public key. Only John can decrypt the message, as only John has his private key. Any data encrypted with a private key can only be decrypted with the corresponding public key. Similarly, Jane could digitally sign a message with her private key, and anyone with Jane's public key could decrypt the signed message and verify that it was in fact Jane who sent it.

Symmetric is generally very fast and ideal for encrypting large amounts of data (e.g., an entire disk partition or database). Asymmetric is much slower and can only encrypt pieces of data that are smaller than the key size (typically 2048 bits or smaller). Thus, asymmetric crypto is generally used to encrypt symmetric encryption keys which are then used to encrypt much larger blocks of data. For digital signatures, asymmetric crypto is generally used to encrypt the hashes of messages rather than entire messages.

A cryptosystem provides for managing cryptographic keys including generation, exchange, storage, use, revocation, and replacement of the keys.

Cyber Security

Definition: Cyber security or information technology security are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation.

Description: Major areas covered in cyber security are:

1) Application Security

2) Information Security

3) Disaster recovery

4) Network Security

Application security encompasses measures or counter-measures that are taken during the development life-cycle to protect applications from threats that can come through flaws in the application design, development, deployment, upgrade or maintenance. Some basic techniques used for application security are: a) Input parameter validation, b) User/Role Authentication & Authorization, c) Session management, parameter manipulation & exception management, and d)Auditing and logging.

Information security protects information from unauthorized access to avoid identity theft and to protect privacy. Major techniques used to cover this are: a) Identification, authentication & authorization of user, b) Cryptography.

Disaster recovery planning is a process that includes performing risk assessment, establishing priorities, developing recovery strategies in case of a disaster. Any business should have a concrete plan for disaster recovery to resume normal business operations as quickly as possible after a disaster.

Network security includes activities to protect the usability, reliability, integrity and safety of the network. Effective network security targets a variety of threats and stops them from entering or spreading on the network. Network security components include: a) Anti-virus and anti-spyware, b) Firewall, to block unauthorized access to your network, c) Intrusion prevention systems (IPS), to identify fast-spreading threats, such as zero-day or zero-hour attacks, and d) Virtual Private Networks (VPNs), to provide secure remote access

DES

Data Encryption Standard (DES)

Data Encryption Standard (DES) is a symmetric block cipher that was once the US Government's gold standard in methods it and others used to encrypt sensitive data. DES was succeeded by the Advanced Encryption Standard (AES) when, in the face of adversaries' more potent brute-force capability, DES was deprecated.

IBM developed DES in the 1970s based on Horst Feistel's earlier design. It was submitted to the US Government's precursor to the National Institute of Standards and Technology (NIST) in response to calls for a data-protection algorithm. In 1976 the NIST precursor consulted with the National Security Agency (NSA) and adopted a modified version that became DES.

The five-year competitive process that NIST used to create AES (1997-2000) was far more collaborative, transparent, and open than the one used for DES. The latter process was rather closed and this harmed its reputation, as did suspicions that the NSA sought a backdoor to DES.

DES's viability suffered as a result of a modification to it, which increased difficulty against differential cryptanalysis but diminished its resistance to brute force attacks. On the whole, DES's short key length of 56 bits made it short-lived in the face of rapid developments in computing, including for cracking encryption.

A symmetric cipher is one that uses the same key for encryption and decryption. Aside from DES and AES, notable examples of symmetric ciphers include Blowfish and International Data Encryption Algorithm (IDEA).

The DES (Data Encryption Standard) algorithm is a symmetric-key block cipher created in the early 1970s by an IBM team and adopted by the National Institute of Standards and Technology (NIST). The algorithm takes the plain text in 64-bit blocks and converts them into ciphertext using 48-bit keys.

Since it's a symmetric-key algorithm, it employs the same key in both encrypting and decrypting the data. If it were an asymmetrical algorithm, it would use different keys for encryption and decryption.

DES is based on the Feistel block cipher, called LUCIFER, developed in 1971 by IBM cryptography researcher
Horst Feistel. DES uses 16 rounds of the Feistel structure, using a different key for each round.

DES became the approved federal encryption standard in November 1976 and subsequently reaffirmed as the standard in 1983, 1988, and 1999. For the longest time, DES was the data encryption standard in information security.

DES's dominance came to an end in 2002, when the Advanced Encryption Standard (AES) replaced the DES encryption algorithm as the accepted standard, following a public competition to find a replacement. The NIST officially withdrew FIPS 46-3 (the 1999 reaffirmation) in May 2005, although Triple DES (3DES), remains approved for sensitive government information through 2030.

Triple DES is a symmetric key-block cipher which applies the DES cipher in triplicate. It encrypts with the first key (k1), decrypts using the second key (k2), then encrypts with the third key (k3). There is also a two-key variant, where k1 and k3 are the same keys.

The NIST had to replace the DES algorithm because its 56-bit key lengths were too small, considering the increased processing power of newer computers. Encryption strength is related to the key size, and DES found itself a victim of the ongoing technological advances in computing. It reached a point where 56-bit was no longer good enough to handle the new challenges to encryption.

Note that just because DES is no longer the NIST federal standard, it doesn’t mean that it’s no longer in use. Triple DES is still used today, but it’s considered a legacy
encryption algorithm. Note that NIST plans to disallow all forms of Triple-DES from 2024 onward. All things being equal, you may want to familiarize yourself with AES as well, considering that it has knocked DES off the top of the data encryption heap.

Now in our understanding of what is DES, let us next look into the DES algorithm steps.

DES Algorithm Steps

To put it in simple terms, DES takes 64-bit plain text and turns it into a 64-bit ciphertext. And since we’re talking about asymmetric algorithms, the same key is used when it’s time to decrypt the text.

The algorithm process breaks down into the following steps:

1. The process begins with the 64-bit plain text block getting handed over to an initial permutation (IP) function.
2. The initial permutation (IP) is then performed on the plain text.
3. Next, the initial permutation (IP) creates two halves of the permuted block, referred to as Left Plain Text (LPT) and Right Plain Text (RPT).
4. Each LPT and RPT goes through 16 rounds of the encryption process.
5. Finally, the LPT and RPT are rejoined, and a Final Permutation (FP) is performed on the newly combined block.
6. The result of this process produces the desired 64-bit ciphertext.

The encryption process step (step 4, above) is further broken down into five stages:

1. Key transformation
2. Expansion permutation
3. S-Box permutation

4. P-Box permutation
5. XOR and swap

For decryption, we use the same algorithm, and
we reverse the order of the 16 round keys.

Next, to better understand what is DES, let us learn the various modes of operation for DES.

DES Modes of Operation

Data encryption experts using DES have five different modes of operation to choose from.

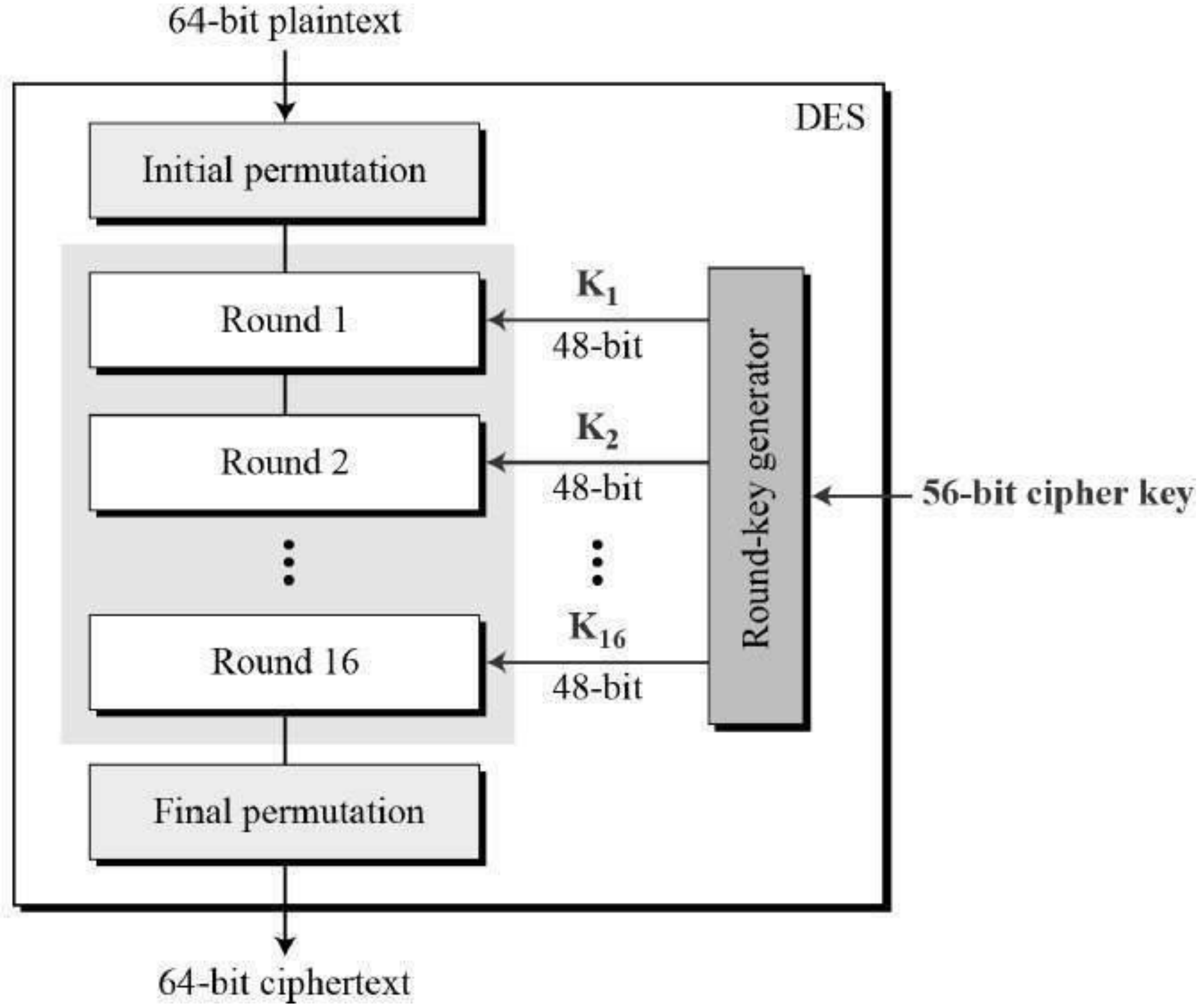
- Electronic Codebook (ECB). Each 64-bit block is encrypted and decrypted independently
- Cipher Block Chaining (CBC). Each 64-bit block depends on the previous one and uses an
  Initialization Vector (IV)
- Cipher Feedback (CFB). The preceding ciphertext becomes the input for the encryption algorithm, producing pseudorandom output, which in turn is XORed with plaintext, building the next ciphertext unit
- Output Feedback (OFB). Much like CFB, except that the encryption algorithm input is the output from the preceding DES

- Counter (CTR). Each plaintext block is XORed with an encrypted counter. The counter is then incremented for each subsequent block

We will next improve our understanding of what DES is, let us look into the DES implementation and testing.

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 a 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). General Structure of DES is depicted in the following illustration −

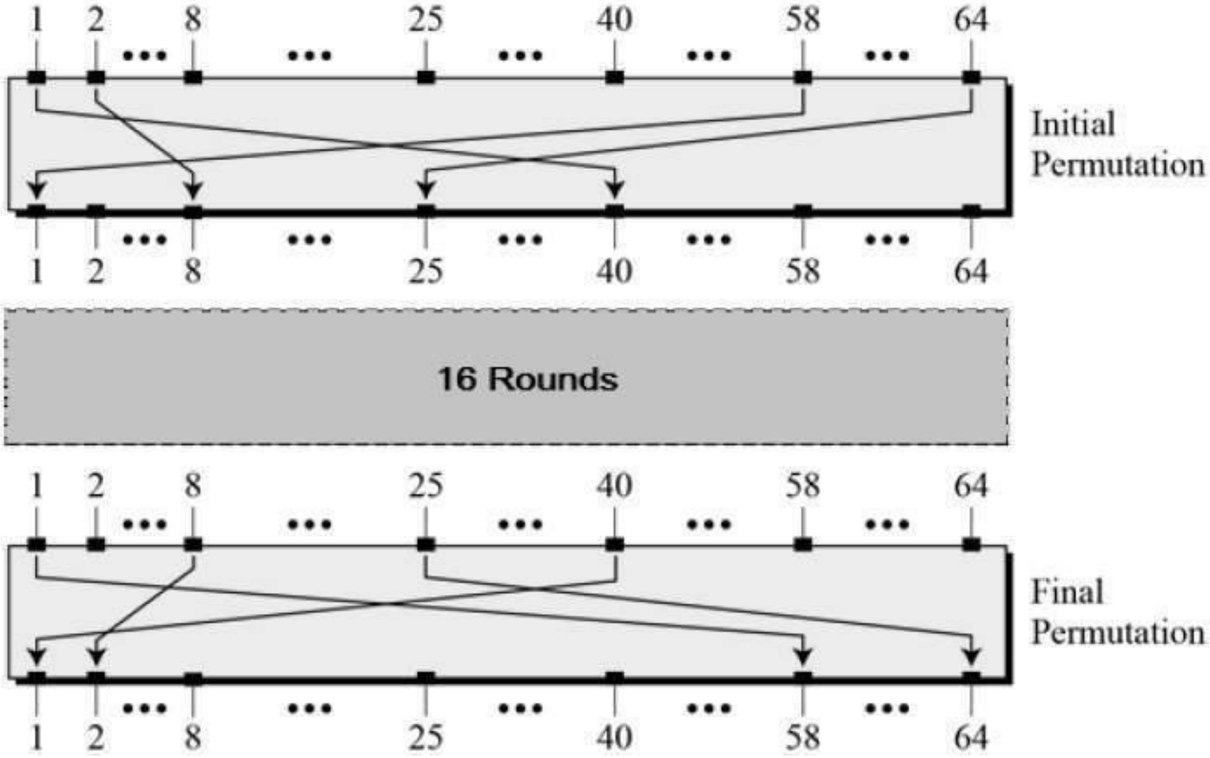


Since DES is based on the Feistel Cipher, all that is required to specify DES is −

- Round function
- Key schedule
- Any additional processing − Initial and final permutation

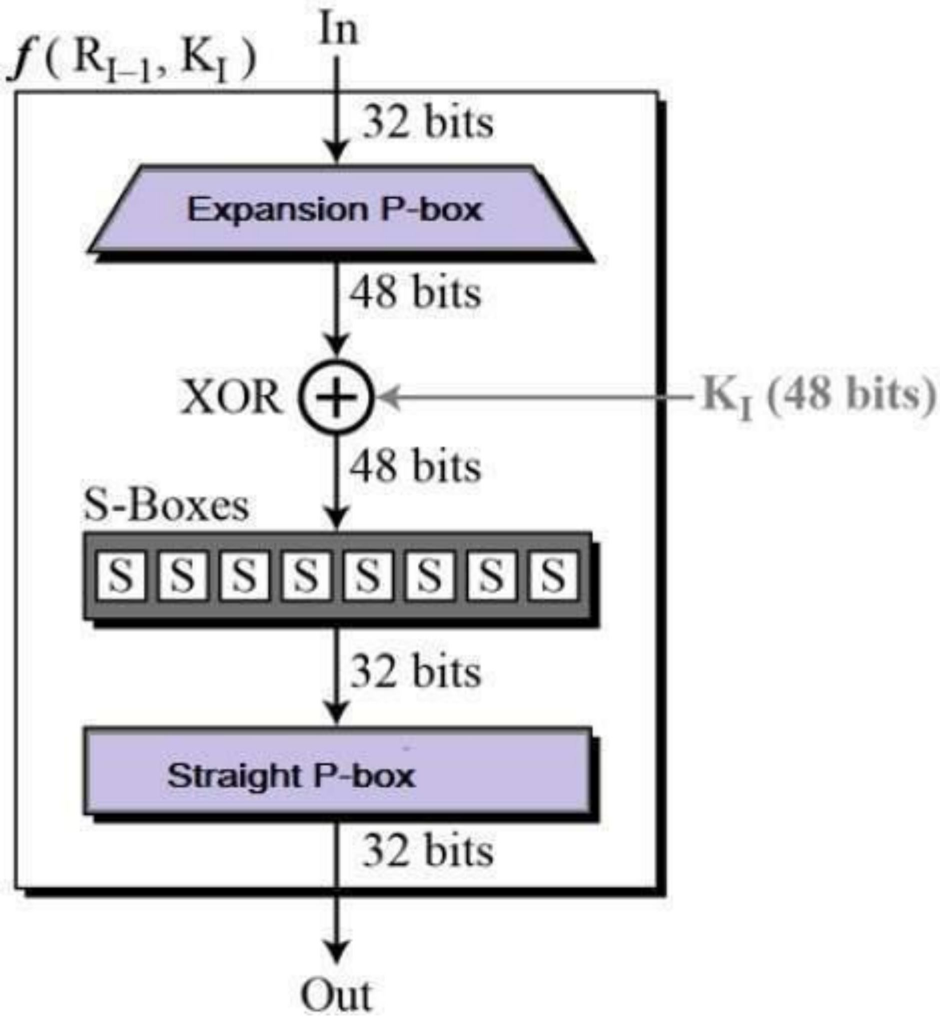
Initial and Final Permutation

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown as follows −

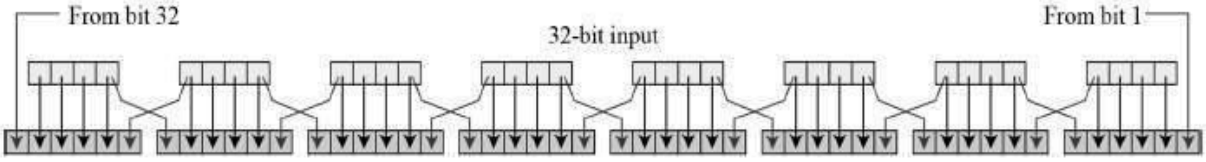


Round Function

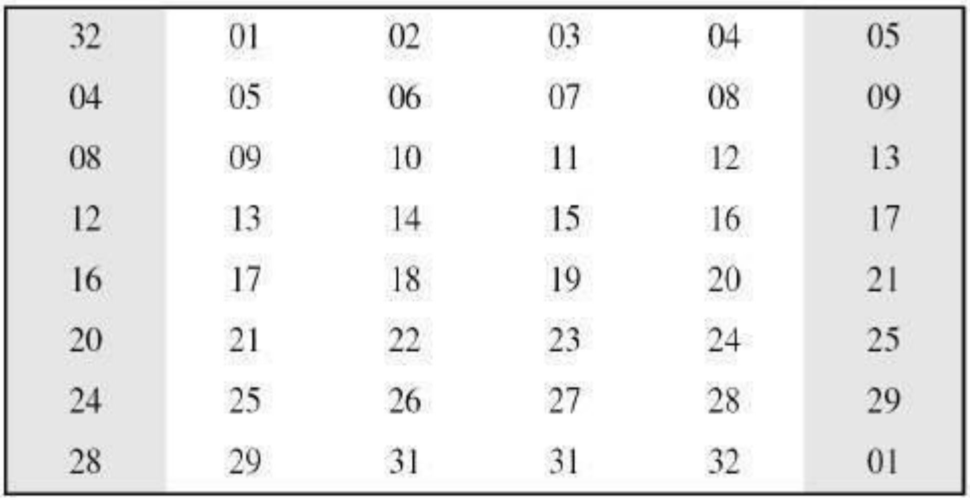
The heart of this cipher is the DES function, f. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



- Expansion Permutation Box − Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically depicted in the following illustration −

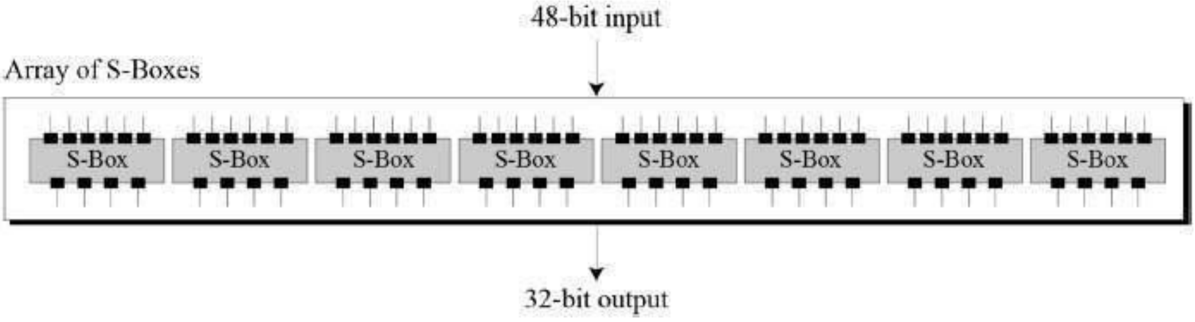


- The graphically depicted permutation logic is generally described as table in DES specification illustrated as shown −

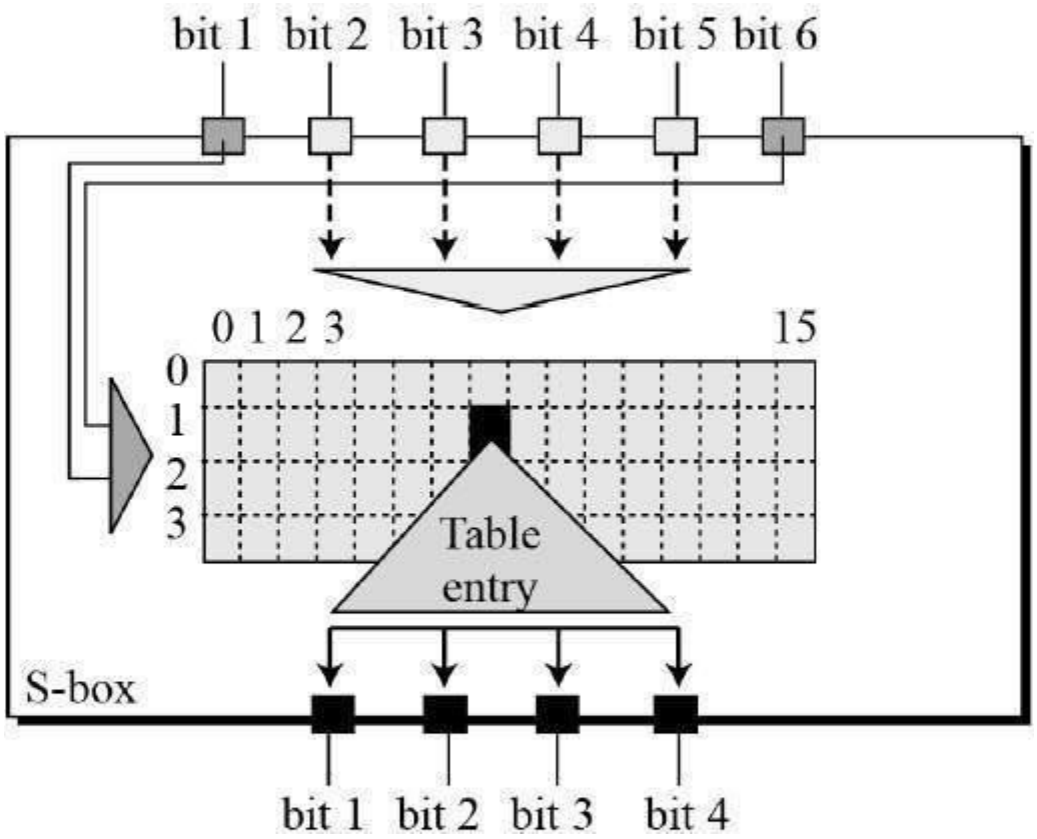


32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

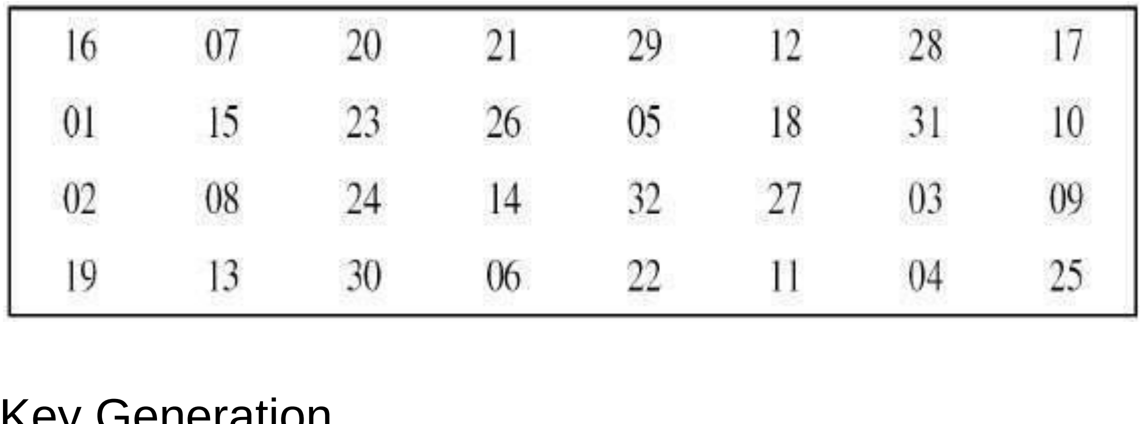
- XOR (Whitener). − After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.
- Substitution Boxes. − The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output. Refer the following illustration −



- The S-box rule is illustrated below −



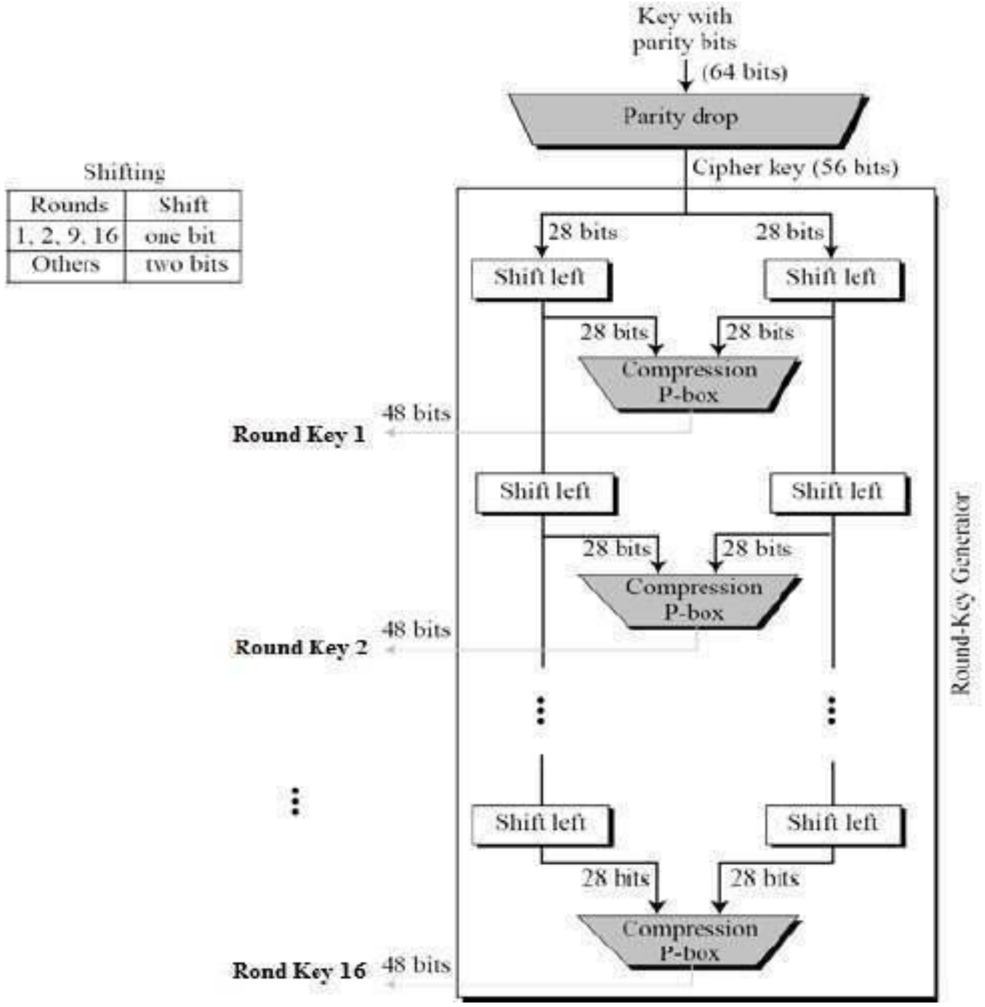
- There are a total of eight S-box tables. The output of all eight s-boxes is then combined in to 32 bit section.
- Straight Permutation − The 32 bit output of S-boxes is then subjected to the straight permutation with rule shown in the following illustration:



16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Key Generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration −



The logic for Parity drop, shifting, and Compression P-box is given in the DES description.

DES Analysis

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

- Avalanche effect − A small change in plaintext results in the very great change in the ciphertext.

- Completeness − Each bit of ciphertext depends on many bits of plaintext.

During the last few years, cryptanalysis have found some weaknesses in DES when key selected are weak keys. These keys shall be avoided.

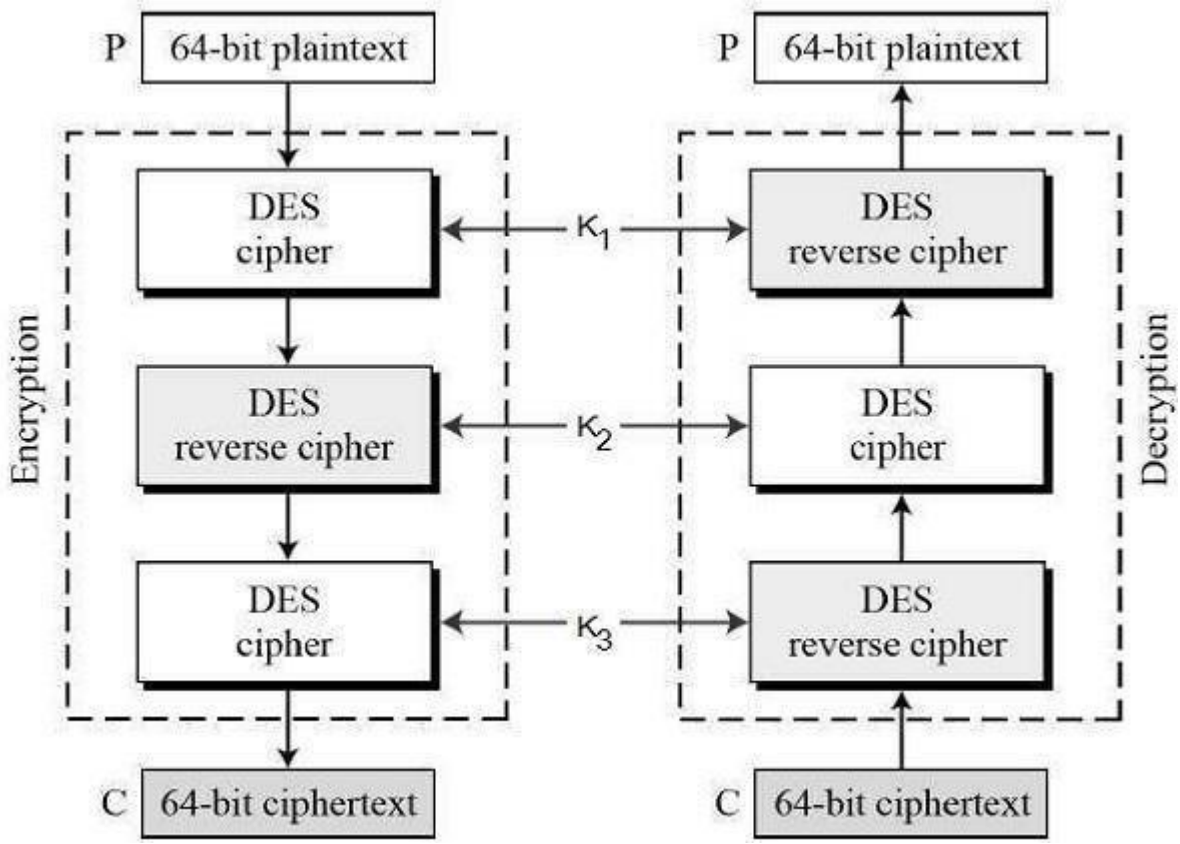
DES has proved to be a very well designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search.

3-KEY Triple DES

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.

Before using 3TDES, user first generate and distribute a 3TDES key K, which consists of three different DES keys K1, K2 and K3. This means that the actual 3TDES key has length 3×56 = 168 bits. The encryption scheme is illustrated as follows −



The encryption-decryption process is as follows −

- Encrypt the plaintext blocks using single DES with key K1.
- Now decrypt the output of step 1 using single DES with key K2.
- Finally, encrypt the output of step 2 using single DES with key K3.
- The output of step 3 is the ciphertext.

- Decryption of a ciphertext is a reverse process. User first decrypt using K3, then encrypt with K2, and finally decrypt with K1.

Due to this design of Triple DES as an encrypt–decrypt–encrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting K1, K2, and K3 to be the same value. This provides backwards compatibility with DES.

Second variant of Triple DES (2TDES) is identical to 3TDES except that K3is replaced by K1. In other words, user encrypt plaintext blocks with key K1, then decrypt with key K2, and finally encrypt with K1 again. Therefore, 2TDES has a key length of 112 bits.

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

WORKING

Triple-DES encryption uses a triple-length DATA key comprised of three 8-byte DES keys to encipher 8 bytes of data using this method:

- Encipher the data using the first key
- Decipher the result using the second key
- Encipher the second result using the third key

The procedure is reversed to decipher data that has been triple-DES enciphered:

- Decipher the data using the third key
- Encipher the result using the second key
- Decipher the second result using the first key

Image Encryption using Triple DES

FRIDAY

FEB - 2018

8.00 (– Top class Security project)

9.00 flow

10.00 – Loading Libraries & Utilies (python)

11.00

– Installation & running of pyDes

12 NOON

– Function Defining

1.00

– Image Read (Imp)

2.00

– function to Encrypt a file with Triple DES

3.00

4.00 { Key
path
5.00 Output

– function to Decrypt

6.00

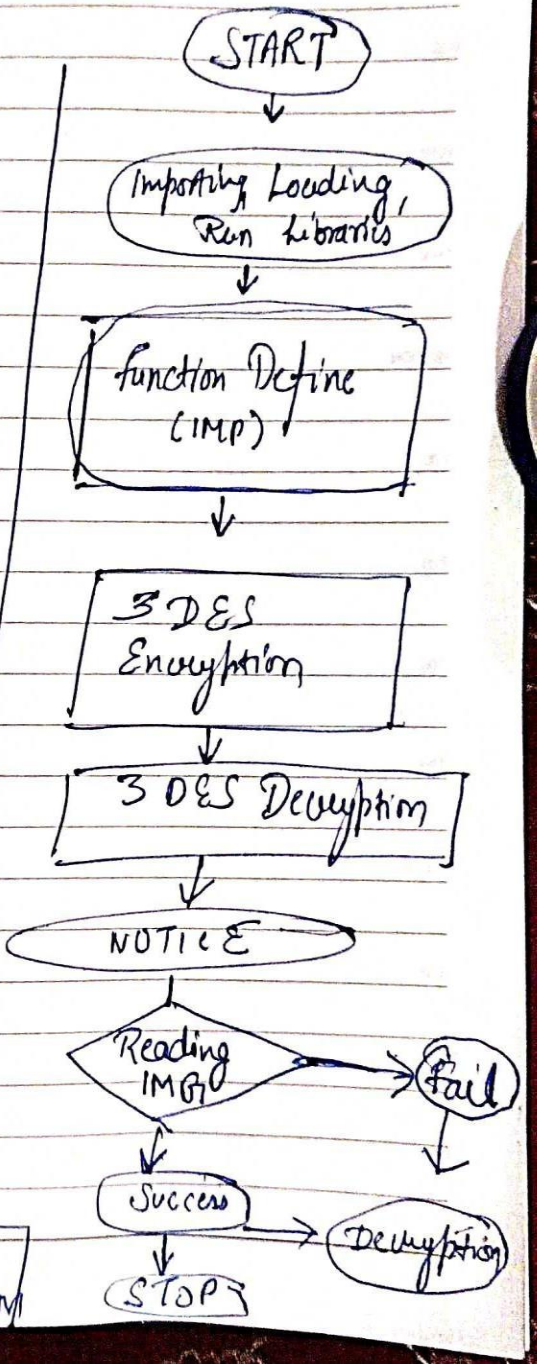
{ path
Key
output

– Demonstration

– Credential

– Encryption

— output — Decryption



IMPLEMENTATION:

1. Importing libraries in the system
2. Uploading / Selecting the Image in the System
3. Running the Triple DES (3DES) Algorithm
4. Running the Encryption Process
5. Running the Decryption Process

CONCLUSION:

System will become very Protected and Secure by applying the Triple DES Process. It is more Secure and complex than the DES algorithm. It will involve an Encryption and Decryption process which will be easier for Sender and Receiver to communicate and understand. This System will protect the Message through both active and passive attacks.

This System will run on any platform such as Cloud, IDE or Compilers.

Future Enhancement is Implementation of this algorithm in Bluetooth chip for secure Data transfer.

REFERENCES

1. https://www.ibm.com/docs/en/zos/2.1.0?topic=operation-triple-des-encryption
2. https://www.comparitech.com/blog/information-security/3des-encryption/
3. https://pycryptodome.readthedocs.io/en/latest/src/cipher/des3.html
4. https://www.semanticscholar.org/paper/Image-Encryption-Based-on-the-Modified-Triple-DES-Silva-Garc%C3%ADa-Flores-Carapia/ca1360649511f2e818f76c4769b51922d31d4d76
5. https://github.com/Vatshayan/Image-Security-by-Triple-DES-Final-Year-Project/blob/main/README.md
6. http://www.onlinejournal.in/IJIRV3I5/159.pdf
7. https://www.geeksforgeeks.org/encrypt-and-decrypt-image-using-python/
8. https://www.researchgate.net/publication/228400978_Hardware_Implementation_of_Triple-DES_EncryptionDecryption_Algorithm