Java Project

Cipher It

H Nidhi 1BM19IS056
Meghana Rathanraj 1BM19IS087

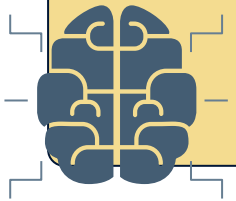
Java Programming
19IS4PCJAV
Mamatha M

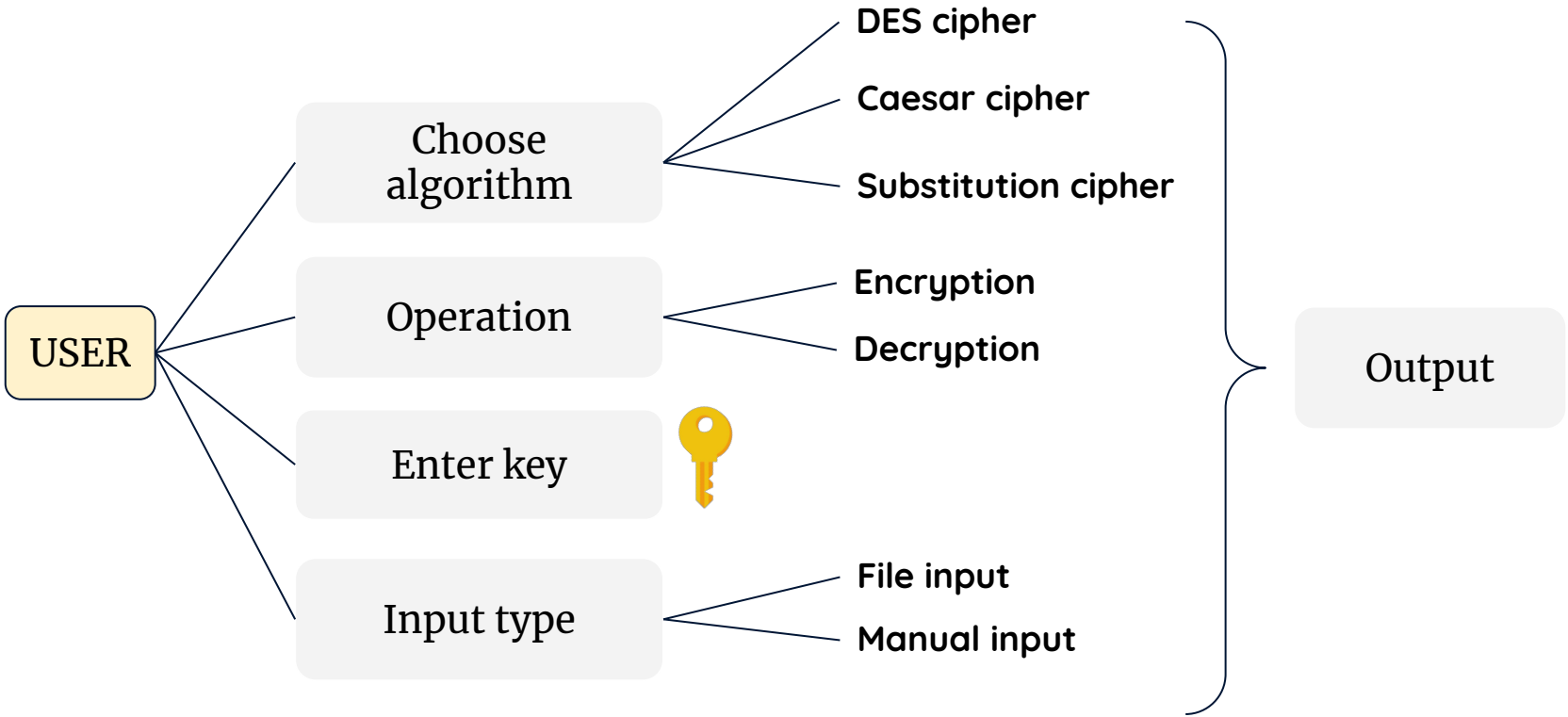
PROBLEM STATEMENT

“Cipher It” is a Java based application which operates on both console and via GUI, to encrypt and decrypt text data, entered manually or present in a text file, using 3 different algorithms

INTRODUCTION

- The user is let to enter an input text
- User gets to decide if they want to encrypt or decrypt their text
- User gets the choice to choose the algorithm they want to use for their purpose
- User must enter a key depending on the algorithm chosen
- Voila! Cipher It will give the output, according to the input parameters on the snap of a finger ;)




USER
Choose algorithm
DES cipher
Caesar cipher
Substitution cipher
Operation
Encryption
Decryption
Enter key
Input type
File input
Manual input
Output

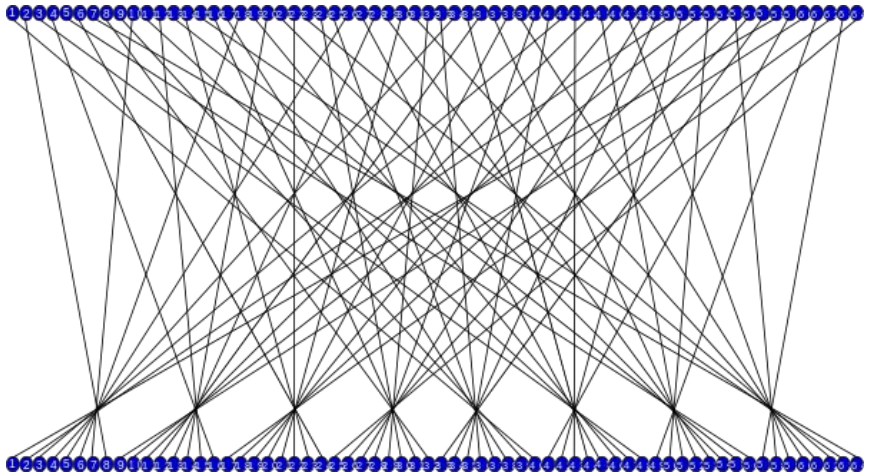
01.

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.

DES

ENCRYPTION
DECRYPTION

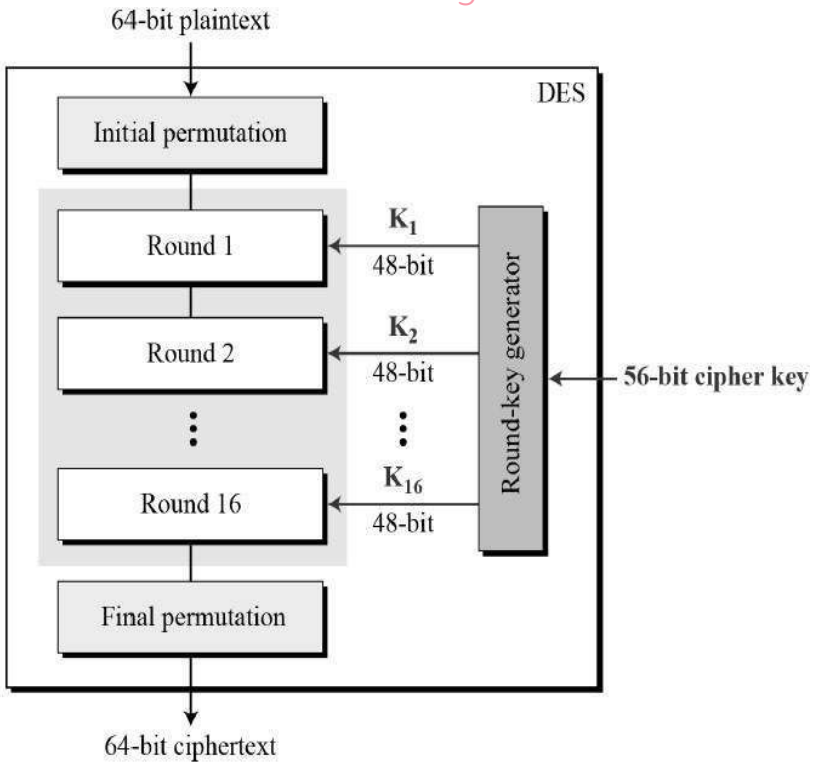


Initial Permutation

WORKING

- In the first step, the 64 bit plain text block is handed over to an initial Permutation (IP) function.
- The initial permutation performed on plain text.
- Next the initial permutation (IP) produces two halves of the permuted block; says Left Plain Text (LPT) and Right Plain Text (RPT).
- Now each LPT and RPT to go through 16 rounds of encryption process.
- In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block
- The result of this process produces 64 bit cipher text.

Overview of working of DES Algorithm



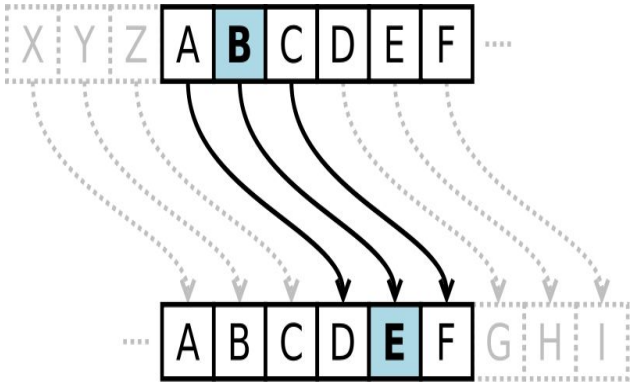
02.

CAESAR

ENCRYPTION
DECRYPTION

Caesar ciphers use a substitution method where letters in the alphabet are shifted by some fixed number of spaces to yield an encoding alphabet.

A Caesar cipher with a shift of 1 would encode an A as a B, an M as an N, and a Z as an A, and so on. The method is named after Roman leader Julius Caesar, who used it in his private correspondence.



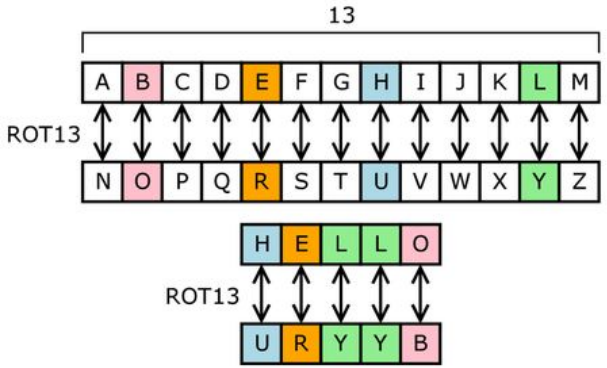
03.

ENCRYPTION
DECRYPTION

SUBSTITUTION

In cryptography, a **substitution cipher** is a method of encrypting in which units of plaintext are replaced with the ciphertext, in a defined manner, with the help of a key.

The "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing the inverse substitution process to extract the original message.

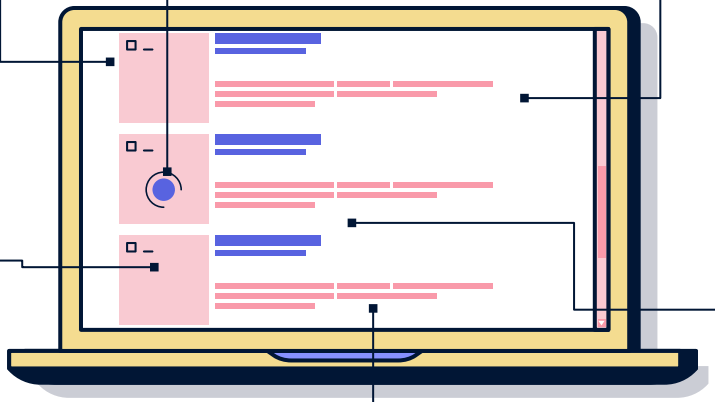


JAVA CONCEPTS USED

SWINGS

FILE HANDLING

PACKAGES AND INTERFACES



COLLECTION FRAMEWORKS

EXCEPTION HANDLING

MULTITHREADING

FUTURE ENHANCEMENTS

ENCRYPTION OF MULTIMEDIA

Encryption of Images, audio and video files

MORE VARIETIES OF ALGORITHMS

Other Algorithms like Blowfish, AES

COMBINATION OF ALGORITHMS

Running DES multiple times or Pass through AES and DES

APPLICATIONS

1

SAFE STORAGE

Sensitive data in encrypted forms are safer

2

Store and handle passwords hassle free! For local file system use

PASSWORD MANAGER

3

COMMUNICATION

Safe email communication / messaging

4

Payment info made easier

PCI COMPLIANCE

5

FUN

Have fun playing with your friends!

THANK YOU!