Ishita Hardasmalani

C14-2103058

EXPERIMENT NO. 2

Aim: Implementation of Caesar Cipher

Theory:

The Caesar Cipher is a simple and ancient encryption technique that involves shifting the letters of the alphabet by a fixed number of positions. It is a type of substitution cipher where each letter in the plaintext is replaced by a letter some fixed number of positions down or up the alphabet.

→	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
→	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
→	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

1. Key Generation: The key in a Caesar Cipher is the number of positions each letter of the alphabet is shifted. This key is typically a positive integer.

2. Encryption: Each letter in the plaintext is shifted by the key value. For example, with a key of 3, 'A' would become 'D', 'B' would become 'E', and so on. The alphabet wraps around, so 'Z' would become 'A'.

The general encryption formula for a Caesar Cipher is:

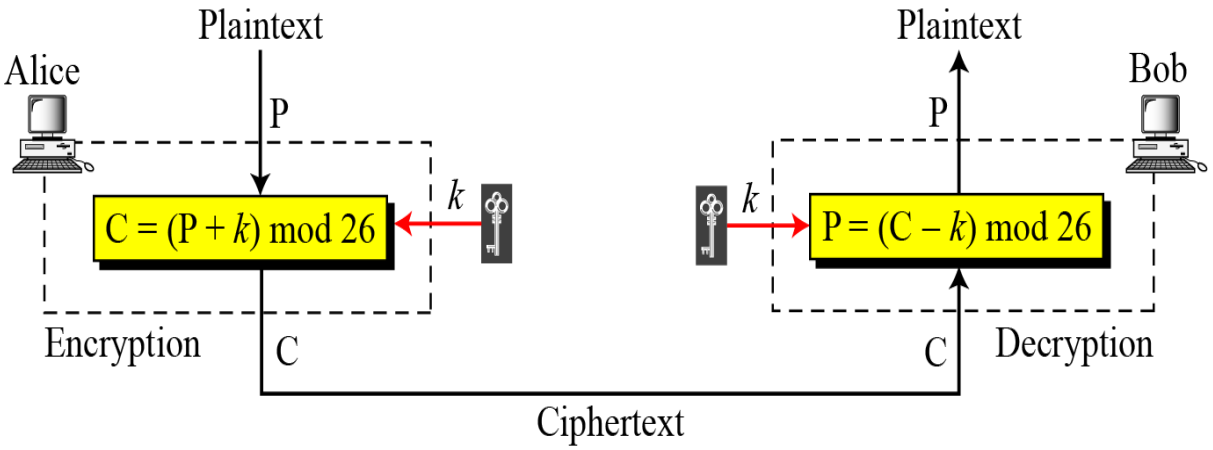
$E(x) = (x + k) \bmod 26$

where E(x) is the encrypted letter, x is the original letter's position in the alphabet, and k is the key.

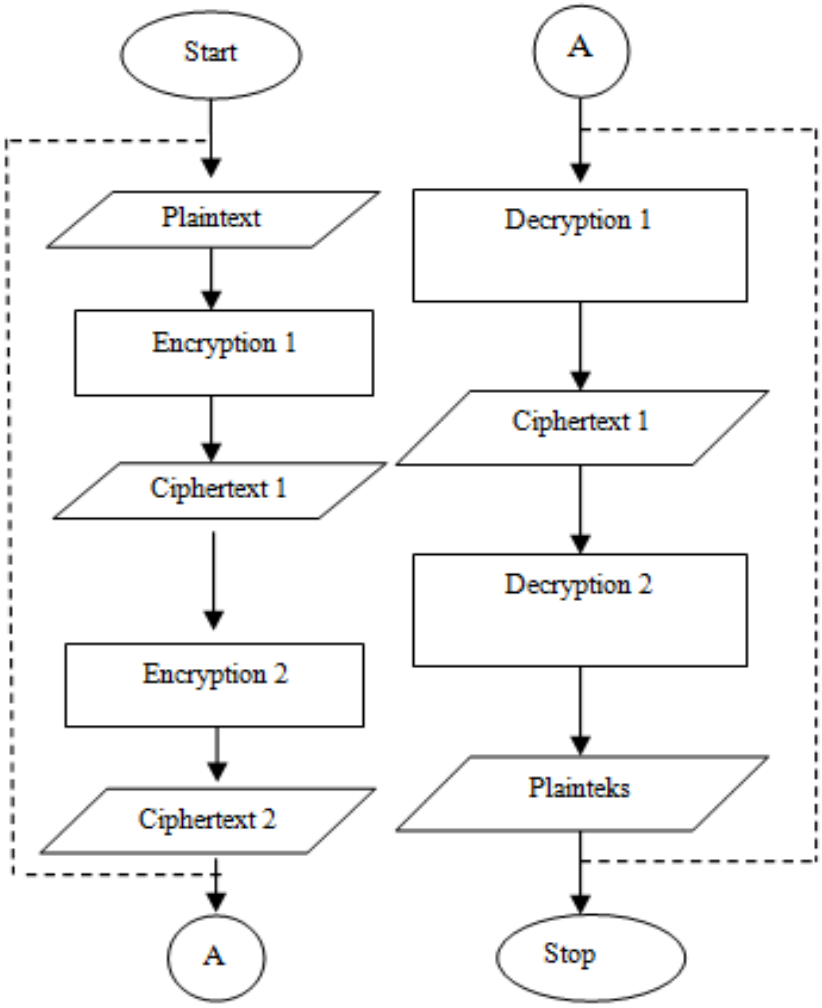
3. Decryption: To decrypt the message, the recipient needs to know the key. Each letter in the ciphertext is shifted back by the key value using the decryption formula:

$D(x) = (x - k) \bmod 26$

where D(x) is the decrypted letter, x is the position of the encrypted letter in the alphabet, and k is the key.



The Caesar Cipher is a straightforward encryption method and is considered relatively weak by modern standards. It can be easily broken through brute-force attacks, where all possible key values are tested. Despite its simplicity, the Caesar Cipher serves as a foundational concept in cryptography.



Code:

```
import java.util.*;
class caeser{

        public static String cipher(String text,int key){
        StringBuilder ciphertext = new StringBuilder();

        for(int i=0;i<text.length();i++){
                char currentChar = text.charAt(i);
                int asciiValue = (int) currentChar;

                int newAsciiValue = (asciiValue + key)%128;

                while(newAsciiValue < 0){
                  newAsciiValue+=128;
                }

                char newchar = (char) newAsciiValue;
                ciphertext.append(newchar);
                System.out.println((char)asciiValue+" -> "+newchar);
        }

        return ciphertext.toString();
        }
        public static String encrypt(String text,int key){
        return cipher(text,key);
        }

        public static String decrypt(String text,int key){
```

```
        return cipher(text,-key);
        }
        public static void main(String args[]){
                Scanner sc = new Scanner(System.in);
                System.out.println("Enter a plain text:- ");
                String text = sc.nextLine();
                System.out.println("Enter the key");
                int key = sc.nextInt();
                System.out.println("Text "+text+" key "+key);
                String encryptText = encrypt(text,key);
                String decryptText = decrypt(encryptText,key);
                System.out.println("Encrypted: "+encryptText);
                System.out.println("Decrypted: "+decryptText);
        }
}
```