SIKSHA ‘O’ ANUSANDHAN DEEMED TO BE UNIVERSITY
INSTITUTE OF TECHNICAL EDUCATION & RESEARCH

Introduction to computer Programming (2023)

Minor Project – 1

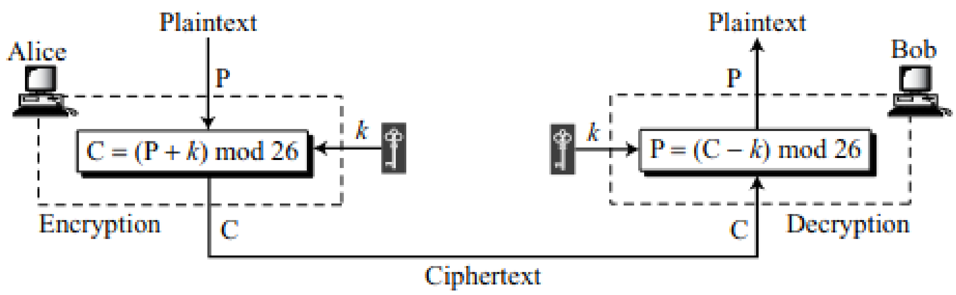
(Submission deadline: 06-02-2023 11:55 PM)

****

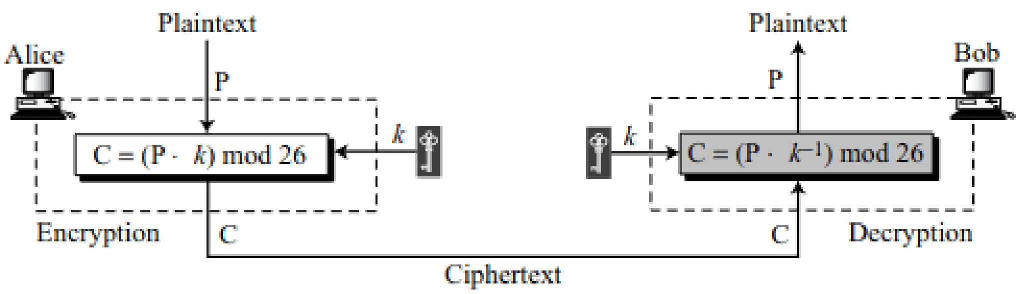
Problem Statement: To design a **Affine chiper**.

Problem Description: In cryptography the general idea of a symmetric chiper is that the sender can send a message to a receiver, over an insecure channel with the assumption that an adversary, cannot understand the contents of the message by simply eavesdropping over the channel. Let the sender is Alice and the receiver is Bob. The original message sent from Alice to Bob is called plaintext; and the message that is sent through the channel is called the ciphertext. To create the ciphertext from the plaintext, Alice uses an encryption algorithm and a shared secret key. To create the plaintext from ciphertext, Bob uses a decryption algorithm and the same secret key.

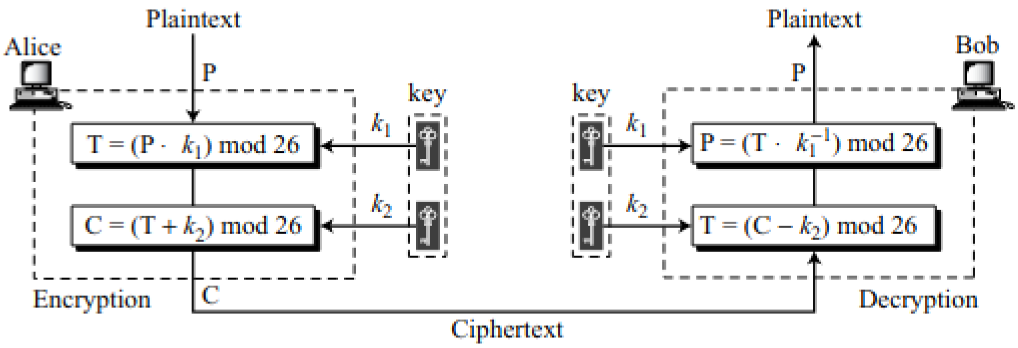
The simplest monoalphabetic cipher is the additive cipher. Here, the encryption algorithm adds the key to the plaintext character; the decryption algorithm subtracts the key from the ciphertext character. The following figure shows the logic of additive chiper.



In a multiplicative cipher, the encryption algorithm multiplies the plaintext characters by the key and the decryption algorithm divides the ciphertext characters by the key as shown in the following Figure.



In this project our goal is to design a **Affine chiper**. Here, we can combine the additive and multiplicative ciphers with a pair of keys to get what is called the affine cipher. The first key is used with the multiplicative cipher; the second key is used with the additive cipher. The following figure shows that the affine cipher is actually two ciphers, applied one after another.



In the affine cipher, the relationship between the plaintext P and the ciphertext C is

$$C = (P \times k1 + k2) \bmod 26$$
$$P = ((C - k2) \times k1^{-1}) \bmod 26$$

Representation of plaintext and ciphertext characters in Z_{26} is shown below.

Plaintext →	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
Ciphertext →	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
Value →	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

Example: Using affine cipher encrypt the message "hello" then decript with key pair (7, 2).

Encryption:
We use 7 for the multiplicative key and 2 for the additive key. We get "ZEBBW".

P: h → 07	Encryption: $(07 \times 7 + 2) \bmod 26$	C: 25 → Z
P: e → 04	Encryption: $(04 \times 7 + 2) \bmod 26$	C: 04 → E
P: l → 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 → B
P: l → 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 → B
P: o → 14	Encryption: $(14 \times 7 + 2) \bmod 26$	C: 22 → W

Decryption:
Add the additive inverse of $-2 \equiv 24 \pmod{26}$ to the received ciphertext. Then multiply the result by the multiplicative inverse of $7^{-1} \equiv 15 \pmod{26}$ to find the plaintext "hello".

C: Z → 25	Decryption: $((25 - 2) \times 7^{-1}) \bmod 26$	P:07 → h
C: E → 04	Decryption: $((04 - 2) \times 7^{-1}) \bmod 26$	P:04 → e
C: B → 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 → l
C: B → 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 → l
C: W → 22	Decryption: $((22 - 2) \times 7^{-1}) \bmod 26$	P:14 → o

Definitions:

1. ***Additive Inverse :*** In Z_n, two numbers a and b are additive inverses of each other if
$$a + b \equiv 0 \pmod{n}$$
For example, the additive inverse of 4 in Z_{10} is $10 - 4 = 6$.
2. ***Multiplicative Inverse :*** In Z_n, two numbers a and b are the multiplicative inverse of each other if
$$a \times b \equiv 1 \pmod{n}$$
For example, if the modulus is 10, then the multiplicative inverse of 3 is 7. In other words, we have $(3 \times 7) \bmod 10 = 1$.

Programming Demonstartion:

Write a Java program to input plaintext from keyboard and display its equivalent chipertext after encryption. Also, decrypt the chipertext to get the same plaintext. Your program should have three methods main(), encrypt() and decrypt(). You are allowed to add extra methods if required. The method headers are as follows:

public static void main(String args[])	**{ }**	[5 marks]
public static String encrypt(String plaintext)	**{ }**	[5 marks]
public static String decrypt(String chipertext)	**{ }**	[5 marks]

(Create a Java file AffineChiper.java and a Description file DescriptionAndOutput.doc, compress both the files into regestrationnumber.zip and submit it to your concern faculty.)

****