Crypto

① Caesar chiper Encryption and Decryption technique →

Plain text: BUZZX

Feature:
- stream
- substitution
- monoalphabetic

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Q	R	S	T	U	V	W	X	Y	Z						
16	17	18	19	20	21	22	23	24	25						

Encryption:

For B

(B+3) mod 26

⇒ (1+3) mod 26

4 (E)

For U

(U+3) mod 26

(20+3) mod 26

(23) X

For Z

(Z+3) mod 26

(25+3) mod 26

28 mod 26

(2) C

26 | 28 | 1
26
(2)

For Z

(Z+3) mod26

(25+3) mod26

28 mod 26

(2) C

For X

(X+3) mod 26

(23+3) mod 26

26 mod 26

(0) A

So, chiper text = EXCCA

For Decryption:

For E

(E-3) mod 26

(4-3) mod 26

1 mod 26

(1) B

For x

(x-3) mod 26

(23-3) mod 26

20 mod 26

(20) U

For c

(c-3) mod 26

(2-3) mod 26

-1 mod 26

26-1 = 25

(25) z

For C

(C-3) mod 26

(2-3) mod 26

(25) z

For A

(A-3) mod 26

(0-3) mod 26

-3 mod 26

26-3 = 23

(23) x

So, Decrypted text = BUzzX

② Write a program to implement encryption and decryption using Mono-Alphabetic cipher.

Input text: Live the moment.

Mapping characters to cipher text letters which used in our code :-

a	b	c	d	e	f	g	h	i	j
Q	W	E	R	T	Y	U	I	O	P
k	l	m	n	o	p	q	r	s	t
A	S	D	F	G	H	J	K	L	Z
u	v	w	x	y	z				
X	C	V	B	N	M				

Explanation of output:

L → S
i → O
v → C
e → T

t → Z
h → I
e → T

m → D
o → G
m → D
e → T
n → F
t → Z

So, Encrypted message ⇒ SOCT ZIT DGDTFZ
~~Decrypted~~ Decrypted messag →

output :

plain text : Live the moment

Encrypted message: SOCT ZJT DQDTFZ

Decrypted message: live the moment.