VIT Vidyalankar Institute of Technology
Accredited A+ by NAAC

DEPARTMENT OF COMPUTER ENGINEERING
CSS Lab

Semester	T.E. Semester V I– Computer Engineering
Subject	Cryptography and System Security
Subject Professor In-charge	Prof. Amit K. Nerurkar
Assisting Teachers	Prof. Amit K. Nerurkar
Laboratory	312A

Student Name	Deep Salunkhe
Roll Number	21102A0014
TE Division	A

Title:

Design and Implementation of Ceaser Cipher Technique

Explanation:

A private-key encryption scheme consists of a set of all possible messages, called the message space M, and three algorithms, namely,

(a) Gen

(b) Enc

(c) Dec

The algorithm for key generation Gen is used to choose a key k at random from the set of all possible secert keys, denoted by the key space K.

The algorithm for encryption Enc takes as inputs the message m and the secret key k and outputs the ciphertext c.

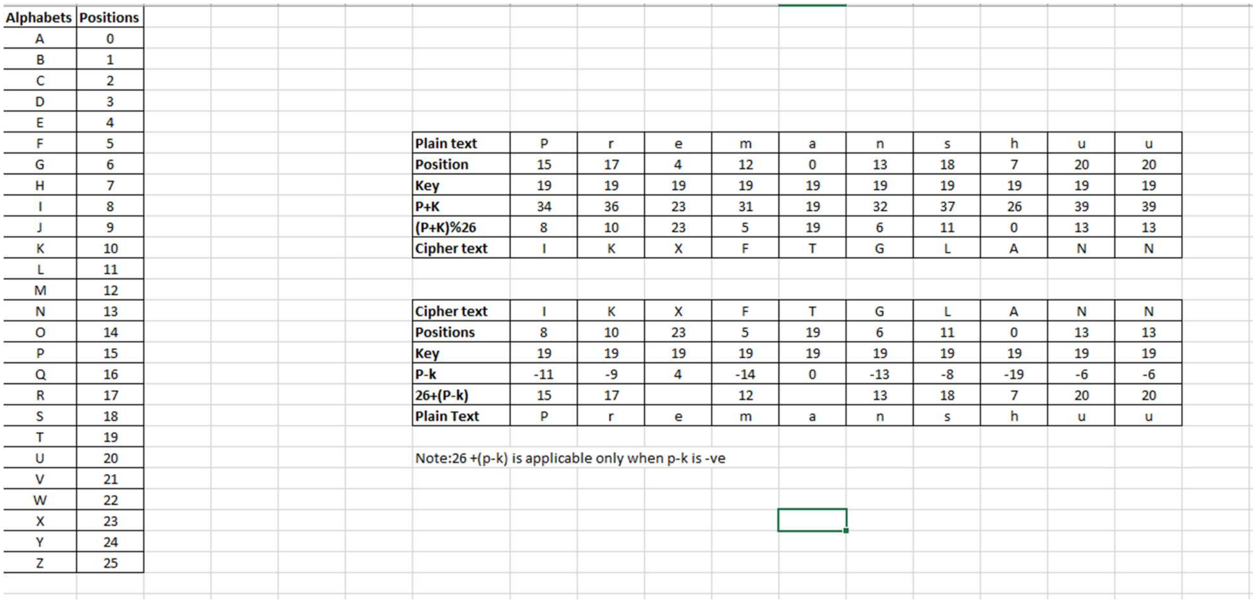
The algorithm for decryption Dec inputs the ciphertext c and the key k and outputs the message m.

About the experiment:

Apparently, the system is easily broken if the total number of distinct secret keys is small, that is the key space K is small.

In this experiment, we work with a well-known historical encryption scheme, namely the shift cipher, that has a very small key space.

Your task is to break the shift cipher. Specifically, given (only) the ciphertext in some instance of a shift cipher, you need to find the plaintext and the secret key.

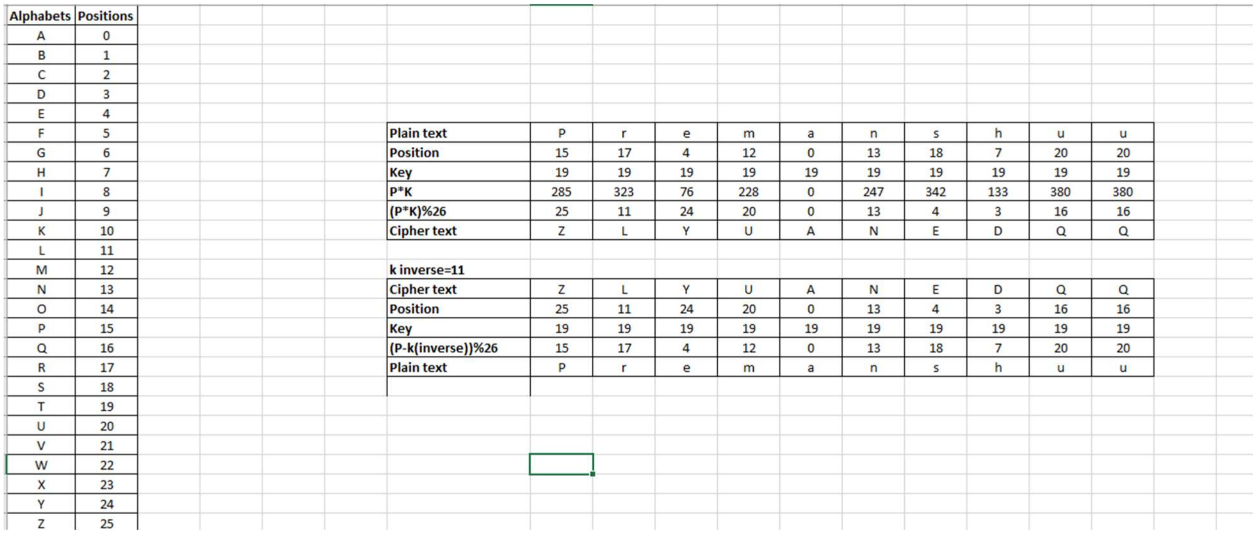


Alphabets	Positions
A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25

Plain text	P	r	e	m	a	n	s	h	u	u
Position	15	17	4	12	0	13	18	7	20	20
Key	19	19	19	19	19	19	19	19	19	19
P+K	34	36	23	31	19	32	37	26	39	39
(P+K)%26	8	10	23	5	19	6	11	0	13	13
Cipher text	I	K	X	F	T	G	L	A	N	N

Cipher text	I	K	X	F	T	G	L	A	N	N
Positions	8	10	23	5	19	6	11	0	13	13
Key	19	19	19	19	19	19	19	19	19	19
P-k	-11	-9	4	-14	0	-13	-8	-19	-6	-6
26+(P-k)	15	17		12		13	18	7	20	20
Plain Text	P	r	e	m	a	n	s	h	u	u

Note:26 +(p-k) is applicable only when p-k is -ve



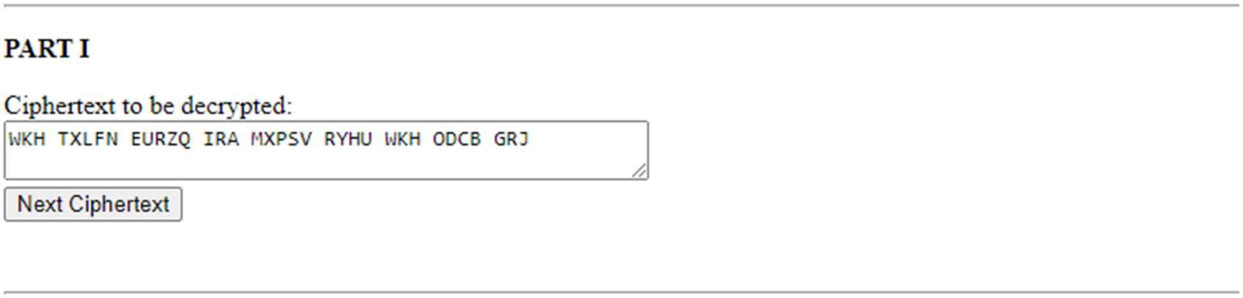
Alphabets	Positions
A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25

Plain text	P	r	e	m	a	n	s	h	u	u
Position	15	17	4	12	0	13	18	7	20	20
Key	19	19	19	19	19	19	19	19	19	19
P*K	285	323	76	228	0	247	342	133	380	380
(P*K)%26	25	11	24	20	0	13	4	3	16	16
Cipher text	Z	L	Y	U	A	N	E	D	Q	Q

k inverse=11

Cipher text	Z	L	Y	U	A	N	E	D	Q	Q
Position	25	11	24	20	0	13	4	3	16	16
Key	19	19	19	19	19	19	19	19	19	19
(P-k(inverse))%26	15	17	4	12	0	13	18	7	20	20
Plain text	P	r	e	m	a	n	s	h	u	u

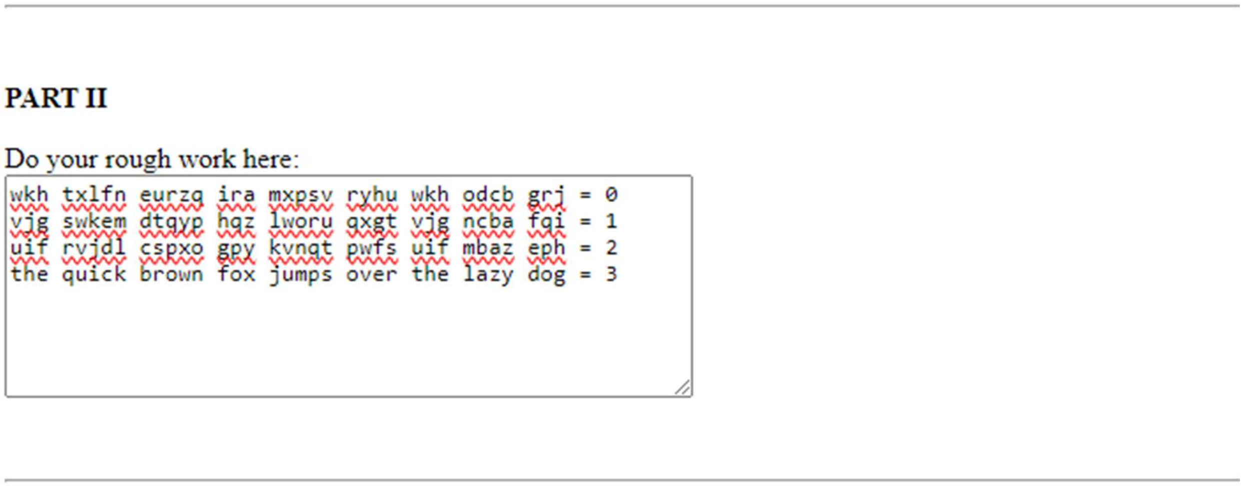
Simulation:



PART I

Ciphertext to be decrypted:

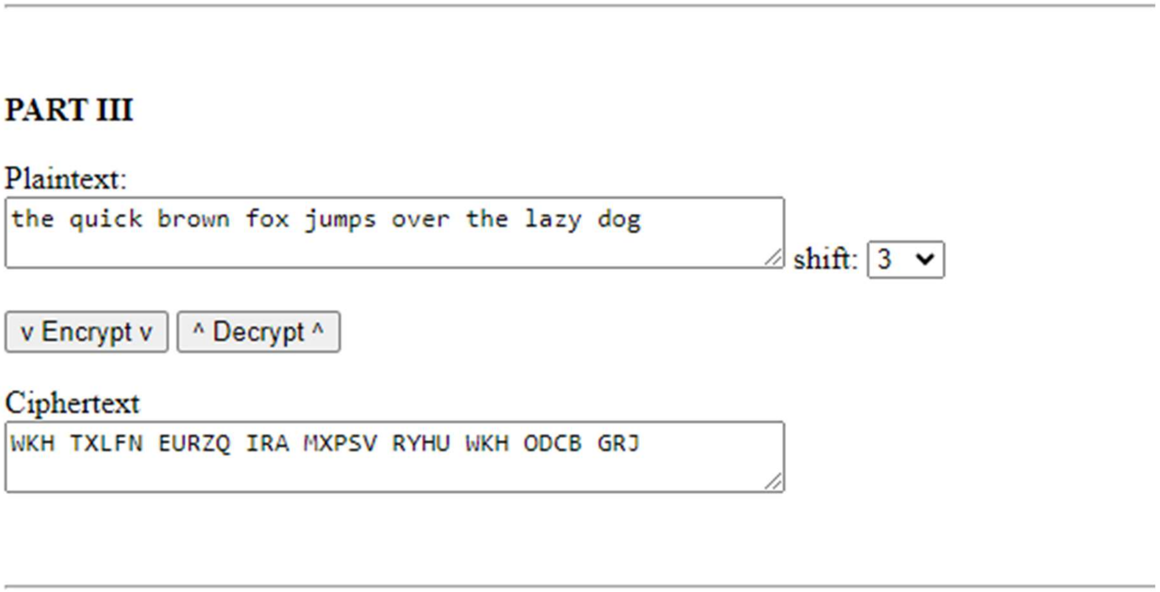
```
WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ
```



PART II

Do your rough work here:

```
wkh txlfn eurzq ira mxpsv ryhu wkh odcb grj = 0
vjg swkem dtqyp hqz lworu qxgt vjg ncba fqi = 1
uif rvjdl cspxo gpy kvnqt pwfs uif mbaz eph = 2
the quick brown fox jumps over the lazy dog = 3
```



PART III

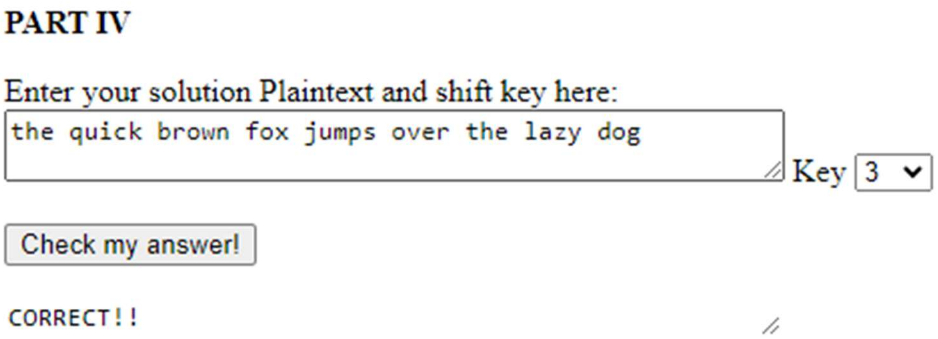
Plaintext:

```
the quick brown fox jumps over the lazy dog
```

shift: 3

Ciphertext

```
WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ
```



PART IV

Enter your solution Plaintext and shift key here:

```
the quick brown fox jumps over the lazy dog
```

Key 3

```
CORRECT!!
```

Conclusion:

In conclusion, the experiment successfully broke the shift cipher, showcasing its vulnerability due to its small key space. By systematically trying all possible keys and analyzing letter frequencies, the plaintext message was deciphered. This highlights the importance of key space size in encryption security and underscores the need for robust cryptographic techniques.