Course Name:	**Information and Cyber Security Laboratory**	**Semester:**	**VII**
Date of Performance:	**23/7/2025**	**Batch No:**	**2**
Faculty Name:	**Prof. Makarand Kulkarni**	**Roll No:**	**16014022050**
Faculty Sign & Date:		**Grade/Marks:**	**25**

Experiment No: 2

Title: Breaking the Shift Cipher using brute force attack

Aim and Objective of the Experiment:

Virtual Laboratory Experiment- (http://cse29- iiith.vlabs.ac.in/): Breaking the Shift Cipher using brute force attack.

COs to be achieved:

CO1: Explain various security goals, threats, vulnerabilities and controls with various cryptographic algorithms for software security.

:

Books/Journals/Websites referred:

Virtual Laboratory Experiment- (http://cse29- iiith.vlabs.ac.in/)

Tools required:

Virtual Laboratory Experiment- (http://cse29- iiith.vlabs.ac.in/)

Theory: A private-key encryption scheme consists of a set of all possible messages, called the messa age 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**.

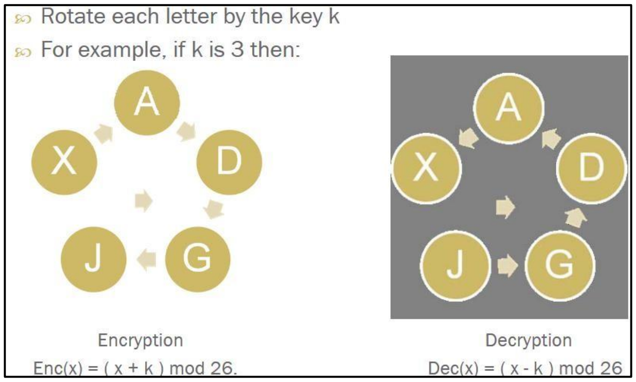
The algorithm for decryption **Dec** inputs the ciphertext **c** and the key **k** and outputs the message **m**.

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.

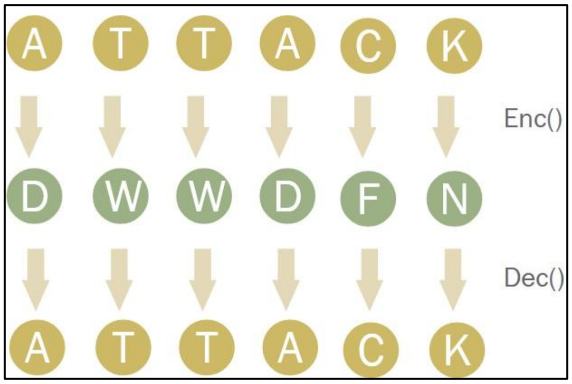
Your task is to break the shift cipher. Specifically, given (only) the ciphertext in some instance of a shift cipher, you need to find the plaintext and the secret key.



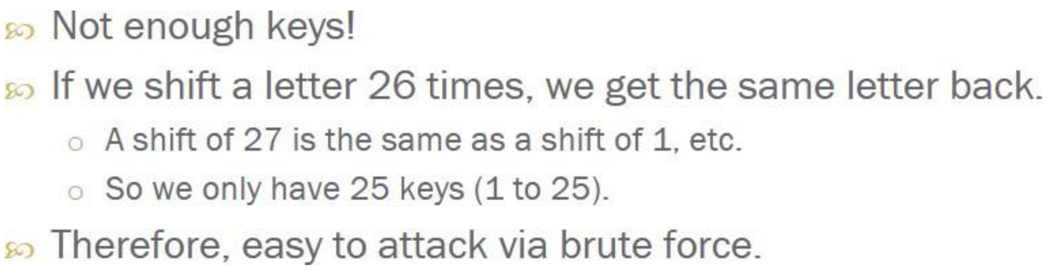
- Rotate each letter by the key k
- For example, if k is 3 then:

Encryption
Enc(x) = (x + k) mod 26.

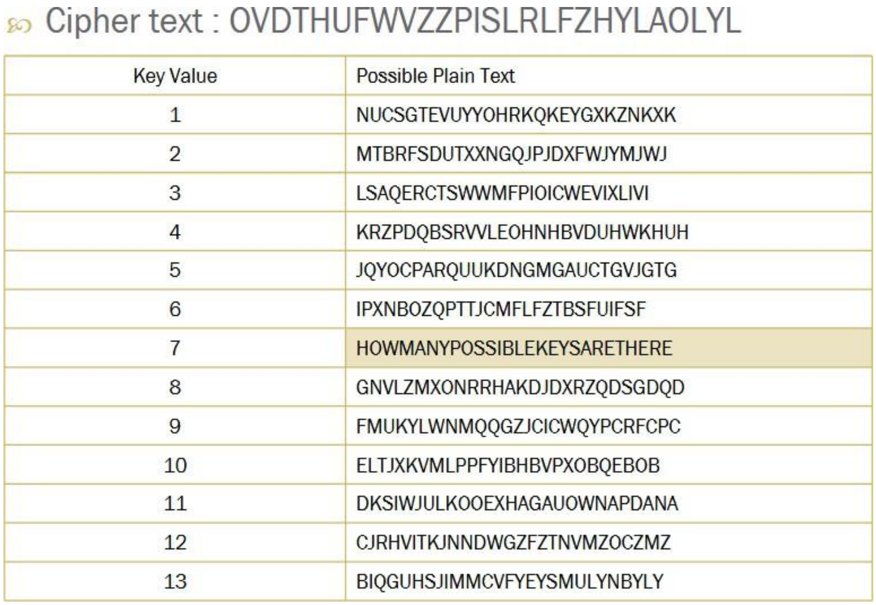
Decryption
Dec(x) = (x - k) mod 26



Problems with Shift Ciphers:



- Not enough keys!
- If we shift a letter 26 times, we get the same letter back.
  - A shift of 27 is the same as a shift of 1, etc.
  - So we only have 25 keys (1 to 25).
- Therefore, easy to attack via brute force.



Cipher text : OVDTHUFWVZZPISLRLFZHYLAOLYL

Key Value	Possible Plain Text
1	NUCSGTEVUYYOHRKQKEYGXKZNKXK
2	MTBRFSDUTXXNGQJPJDXFWJYMJWJ
3	LSAQERCTSWWMFPIOICWEVIXLIVI
4	KRZPDQBSRVVLEOHNHBVDUHWKHUH
5	JQYOCPARQUUKDNGMGAUCTGVJGTG
6	IPXNBOZQPTTJCMFLFZTBSFUIFSF
7	HOWMANYPOSSIBLEKEYSARETHERE
8	GNVLZMXONRRHAKDJDXRZQDSGDQD
9	FMUKYLWNMQQGZJCICWQYPCRFCPC
10	ELTJXKVMLPPFYIBHBVPXOBQEBOB
11	DKSIWJULKOOEXHAGAUOWNAPDANA
12	CJRHVITKJNNDWGZFZTNVMZOCZMZ
13	BIQGUHSJIMMCVFYEYSMULYNBYLY

Stepwise Implementation details:

STEP 1: For the given ciphertext in the **PART I** of the simulation page, the first step is to decrypt it using each of the twenty-six different keys, k=0,1,...,25 and obtain the corresponding plaintexts. For decryption, you may use the tool given in the **PART III** of the simulation page.

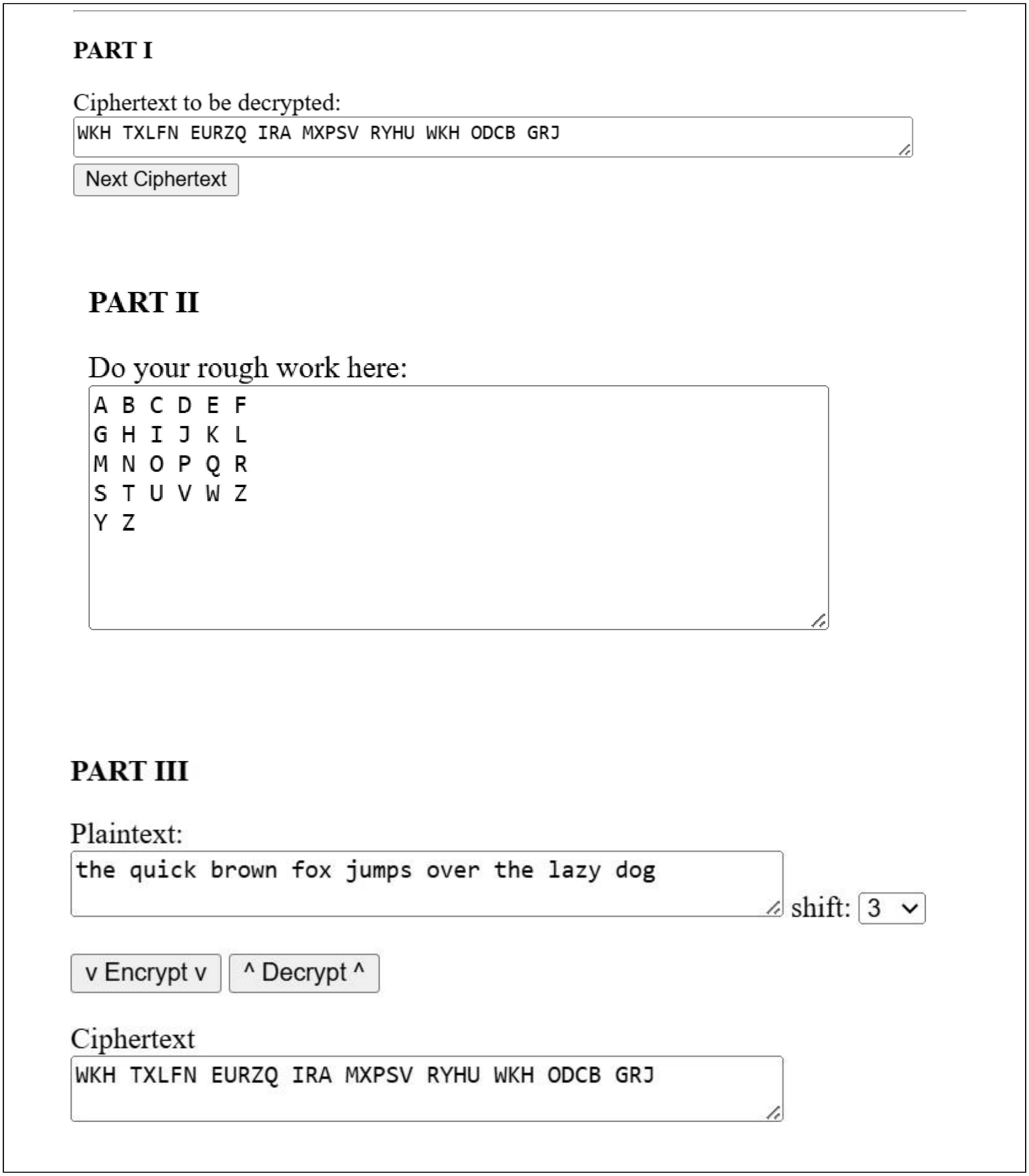
STEP 2: After each decryption, you may cut-and-paste the resultant plaintext in the scratch-pad in the **(PART II)** of the simulation page, if you need to remember it.

STEP 3: Finally, observe the plaintexts and choose the most appropriate one (the one that is a meaningful English text) as the recovered plaintext and cut-and-paste it in the text-field named **PART IV** "Solution Plaintext". Also select the corresponding key in the text-field named "Key" and click on "Check My answer" Button.

STEP 4 [OPTIONAL]: Verify that your answer is correct, by encrypting the solution plaintext with your key.

ScreenShots

Question 1



PART I

Ciphertext to be decrypted:

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

PART II

Do your rough work here:

```
A B C D E F
G H I J K L
M N O P Q R
S T U V W Z
Y Z
```

PART III

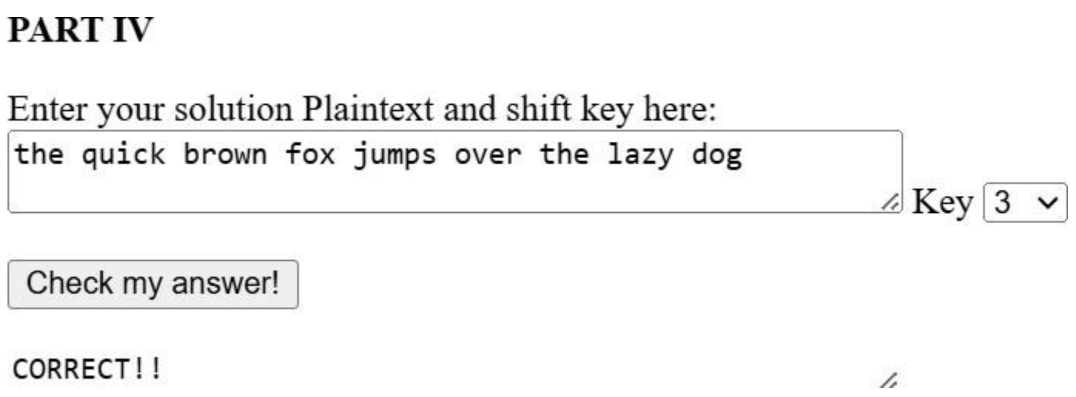
Plaintext:

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

shift: 3

Ciphertext

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



PART IV

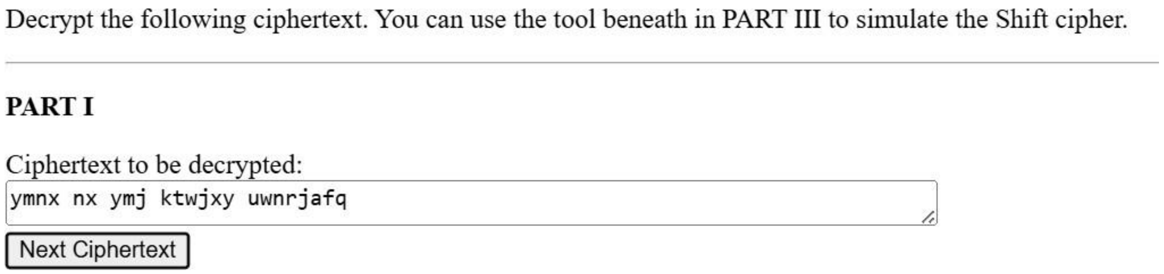
Enter your solution Plaintext and shift key here:

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

Key 3

```
CORRECT!!
```

Question 2

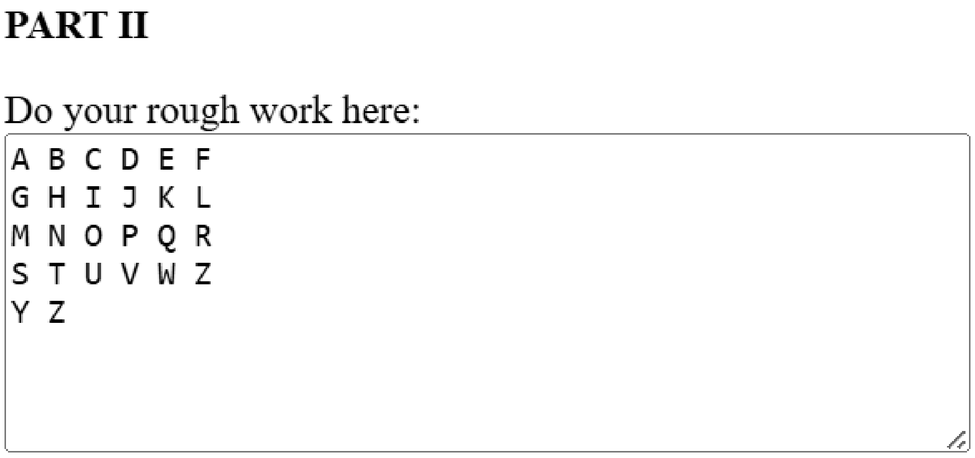


Decrypt the following ciphertext. You can use the tool beneath in PART III to simulate the Shift cipher.

PART I

Ciphertext to be decrypted:

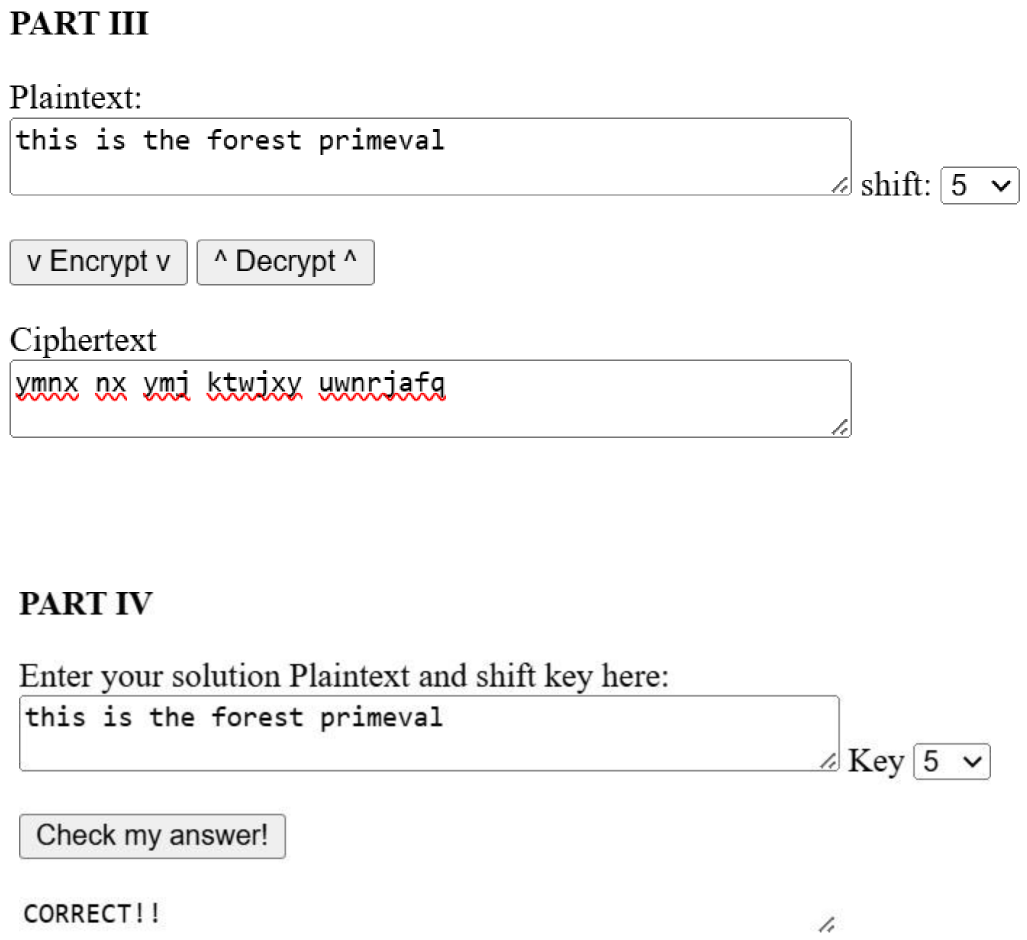
```
ymnx nx ymj ktwjxy uwnrjafq
```



PART II

Do your rough work here:

```
A B C D E F
G H I J K L
M N O P Q R
S T U V W Z
Y Z
```



PART III

Plaintext:
```
this is the forest primeval
```
shift: 5

Ciphertext
```
ymnx nx ymj ktwjxy uwnrjafq
```

PART IV

Enter your solution Plaintext and shift key here:
```
this is the forest primeval
```
Key 5

```
CORRECT!!
```

Output/ program results after execution:

Post Lab Subjective/Objective type Questions:

1. Use Encrypt the following plain text using key k = 7.
   Plain Text: Lord Rama was a good king.

   Encrypted Text: ehkw ktft ptl t zhhw dbgz.

2. A Given a plain text and its corresponding cipher text, find out the key used for the encryption of the plain text.

   Plain Text : abcdefghijklmnopqrstuvwxyz
   Cipher Text: TDNUCBZROHLGYVFPWIXSEKAMQJ

Conclusion:

In this experiment, we learned how to break a cipher text using basic cryptanalysis techniques. It showed that simple ciphers like the Caesar cipher can be easily decoded by analyzing letter patterns and shifts.

Signature of faculty in-charge with Date: