NAME : Aman Singh BATCH : T23
SUBJECT : CNS LAB ROLL NO : 128

Experiment No 1

Aim : Breaking shift cipher and Mono Alphabetic Substitution cipher using Frequency analysis method.

Lab Outcome :

LO1: Illustrate symmetric cryptography by implementing classical ciphers.

Theory :

1. Shift Cipher:

Shift cipher, also known as Caesar cipher, is a type of substitution cipher where each letter in the plaintext is shifted a certain number of positions down the alphabet. It is one of the simplest and oldest encryption techniques.

Encryption Process:

- Each letter in the plaintext is replaced with the corresponding letter in the shifted alphabet. - The shift value 'k' determines how many positions each letter is moved. For example, with a shift of 3, 'A' becomes 'D', 'B' becomes 'E', and so on.
- Non-alphabetic characters, such as spaces or punctuation, are left unchanged in the ciphertext.
- The encryption formula is: $E(x) = (x + k) \bmod 26$, where 'x' is the numerical value of the letter and 'k' is the shift value.

Decryption Process:

- To decrypt the ciphertext, the receiver knows the shift value 'k' and simply shifts each letter backward in the alphabet. - The decryption formula is: $D(x) = (x - k) \bmod 26$.

Brute Force Attack on Shift Cipher:

Since there are only 25 possible shift values (excluding no shift or 0 shift), a brute force attack is feasible. The attacker can quickly try all combinations of shifts to decrypt the ciphertext and find the correct plaintext. Shift ciphers are not considered secure due to their vulnerability to brute force attacks.

2. Monoalphabetic Cipher:

NAME : Aman Singh BATCH : T23
SUBJECT : CNS LAB ROLL NO : 128

A monoalphabetic cipher is a type of substitution cipher where each letter in the plaintext is replaced by the same corresponding letter in the ciphertext. The substitution remains constant throughout the encryption process.

Encryption Process:

- Each letter in the plaintext is replaced with a corresponding letter from the key. The key is a fixed 26-letter substitution table, where each letter in the alphabet is mapped to its respective substitution.
- For example, 'A' is replaced with the first letter of the key, 'B' with the second letter, and so on. - Non-alphabetic characters are left unchanged in the ciphertext.

Decryption Process:

- To decrypt the ciphertext, the receiver uses the same key to look up the corresponding plaintext letters for each letter in the ciphertext.

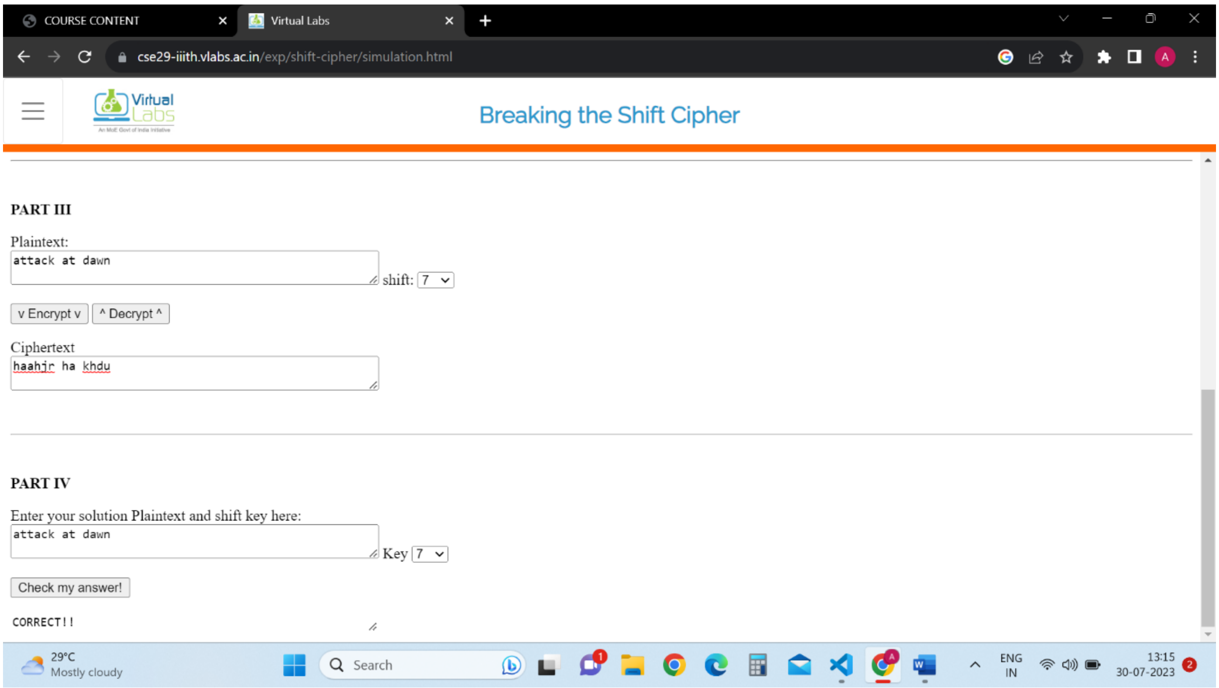
Brute Force Attack on Monoalphabetic Cipher:
A brute force attack on a monoalphabetic cipher is not practical because there are 26! (factorial) possible key combinations. This makes it computationally infeasible to try all combinations and decrypt the message.

Frequency Analysis Attack on Monoalphabetic Cipher:
Frequency analysis is a powerful technique to break monoalphabetic ciphers. It exploits the fact that certain letters or groups of letters occur more frequently in the plaintext. For example, in English, the letter 'E' is the most common. By analyzing the frequency of letters in the ciphertext and comparing it with the expected frequency distribution in the English language, the attacker can deduce the key and decrypt the message.

Output:

1. **Shift Cipher**

NAME : Aman Singh BATCH : T23
SUBJECT : CNS LAB ROLL NO : 128



Breaking the Shift Cipher

PART III

Plaintext:

```
attack at dawn
```

shift: 7

v Encrypt v ^ Decrypt ^

Ciphertext

```
haahjr ha khdu
```

PART IV

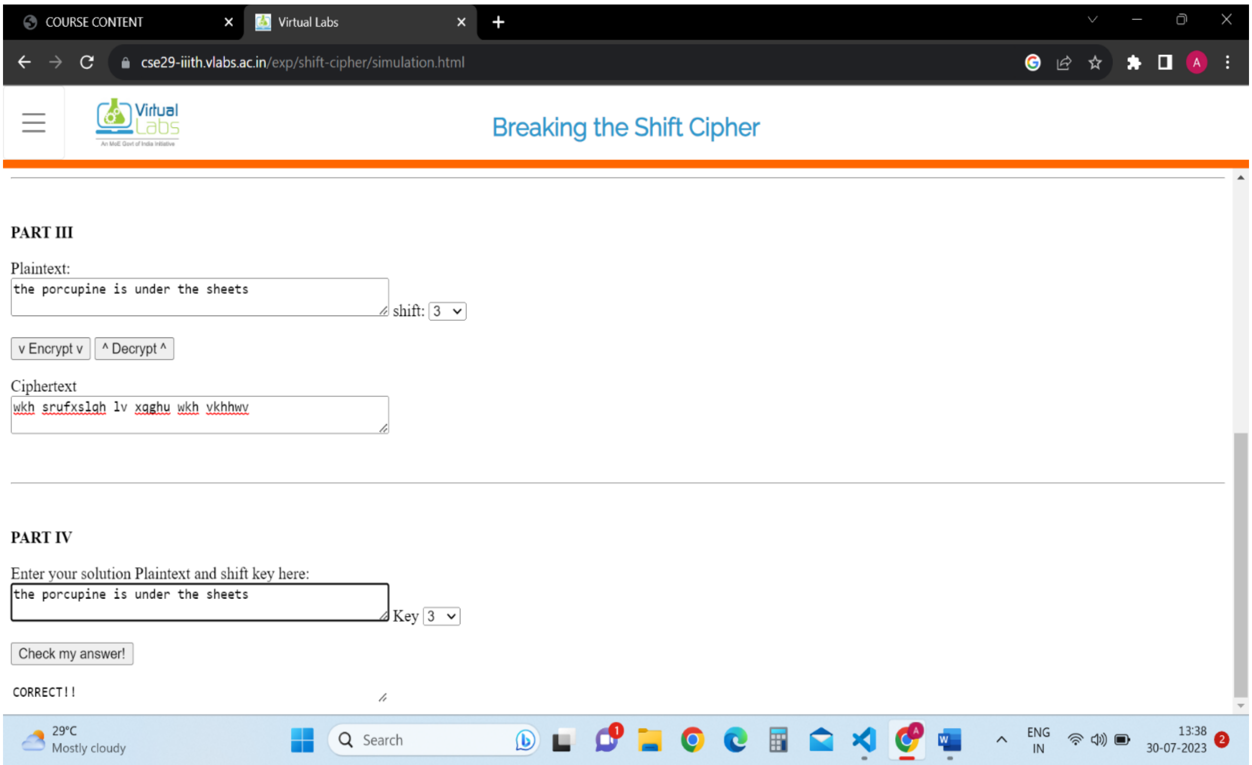
Enter your solution Plaintext and shift key here:

```
attack at dawn
```

Key 7

Check my answer!

```
CORRECT!!
```



Breaking the Shift Cipher

PART III

Plaintext:

```
the porcupine is under the sheets
```

shift: 3

v Encrypt v ^ Decrypt ^

Ciphertext

```
wkh srufxslqh lv xqghu wkh vkhhwv
```

PART IV

Enter your solution Plaintext and shift key here:

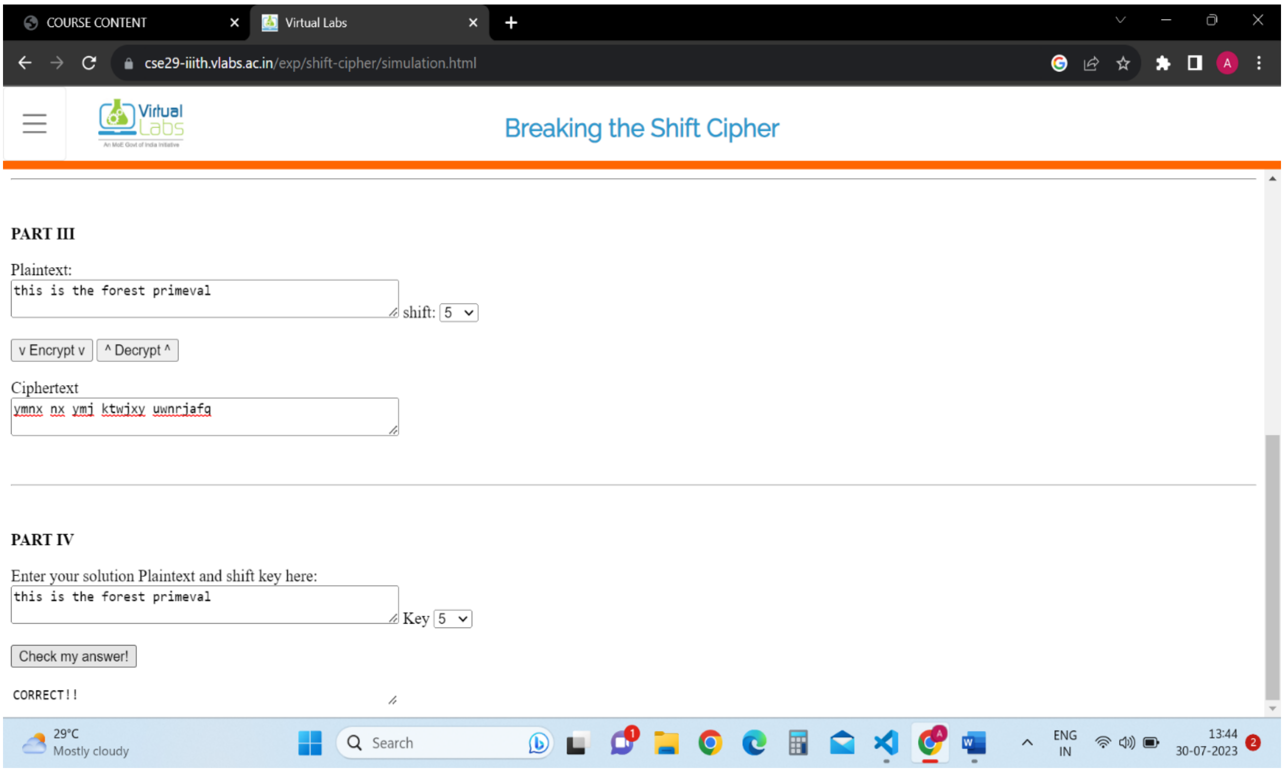
```
the porcupine is under the sheets
```

Key 3

Check my answer!

```
CORRECT!!
```

NAME : Aman Singh   BATCH : T23
SUBJECT : CNS LAB   ROLL NO : 128



PART III

Plaintext:

```
this is the forest primeval
```

shift: 5

Ciphertext

```
ymnx nx ymj ktwjxy uwnrjafq
```

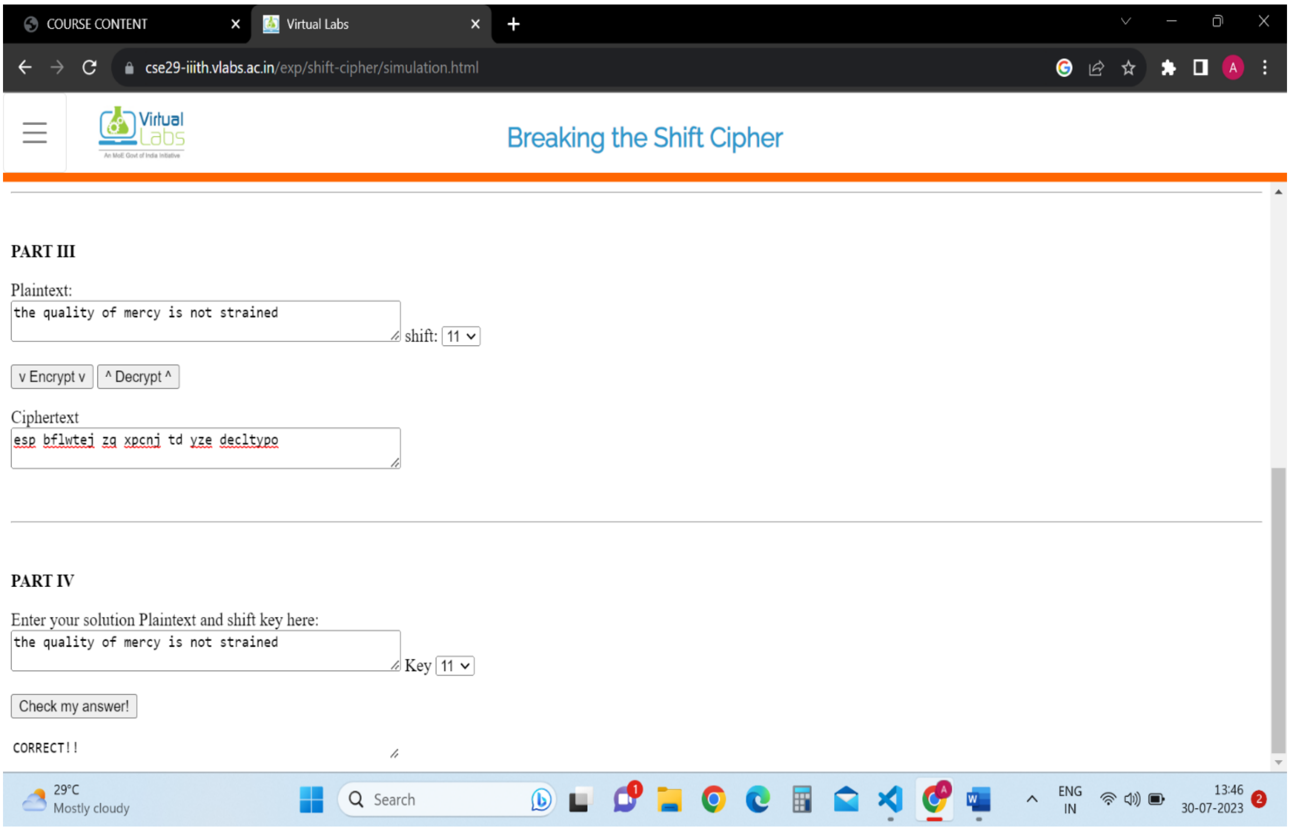
PART IV

Enter your solution Plaintext and shift key here:

```
this is the forest primeval
```

Key 5

```
CORRECT!!
```



PART III

Plaintext:

```
the quality of mercy is not strained
```

shift: 11

Ciphertext

```
esp bflwtej zq xpcnj td yze decltypo
```

PART IV

Enter your solution Plaintext and shift key here:

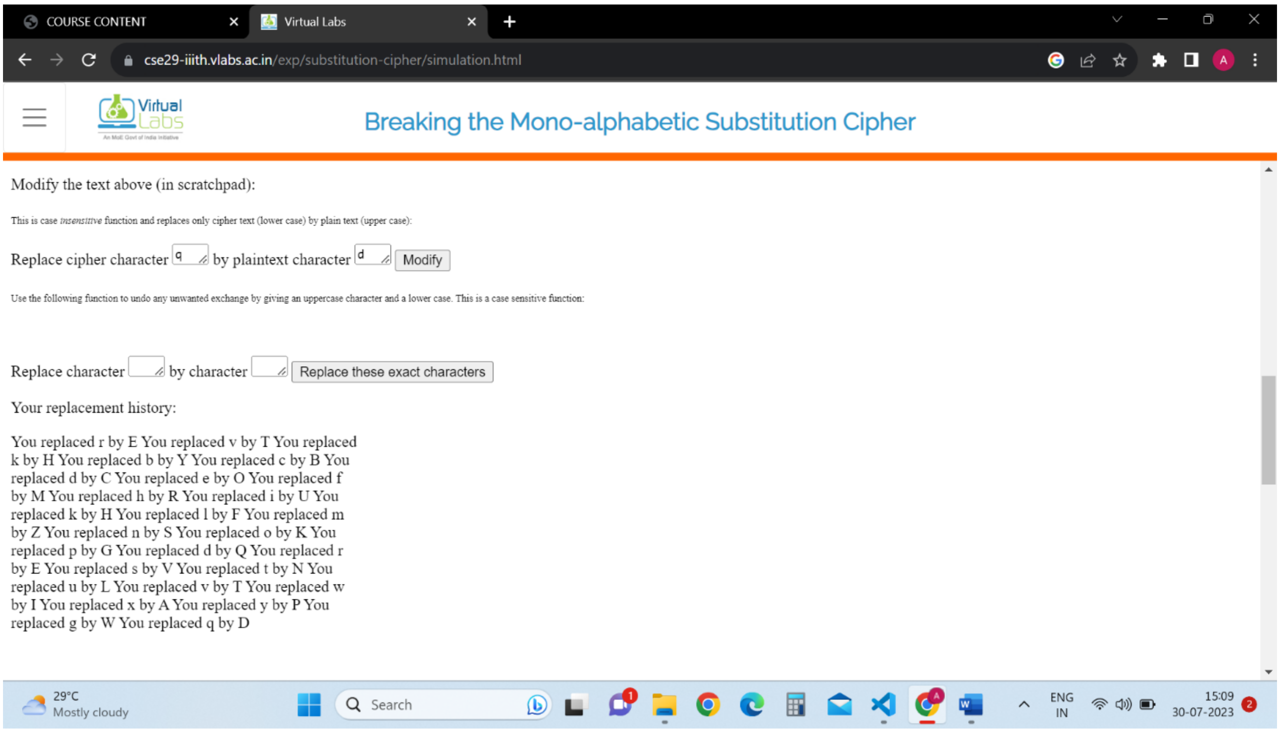
```
the quality of mercy is not strained
```

Key 11

```
CORRECT!!
```

NAME : Aman Singh BATCH : T23
SUBJECT : CNS LAB ROLL NO : 128

2. Substitution Cipher


COURSE CONTENT
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/substitution-cipher/simulation.html
Virtual Labs
An MoE Govt of India Initiative
Breaking the Mono-alphabetic Substitution Cipher
29°C
Mostly cloudy
Search
ENG
IN
15:09
30-07-2023

Modify the text above (in scratchpad):

This is case *insensitive* function and replaces only cipher text (lower case) by plain text (upper case):

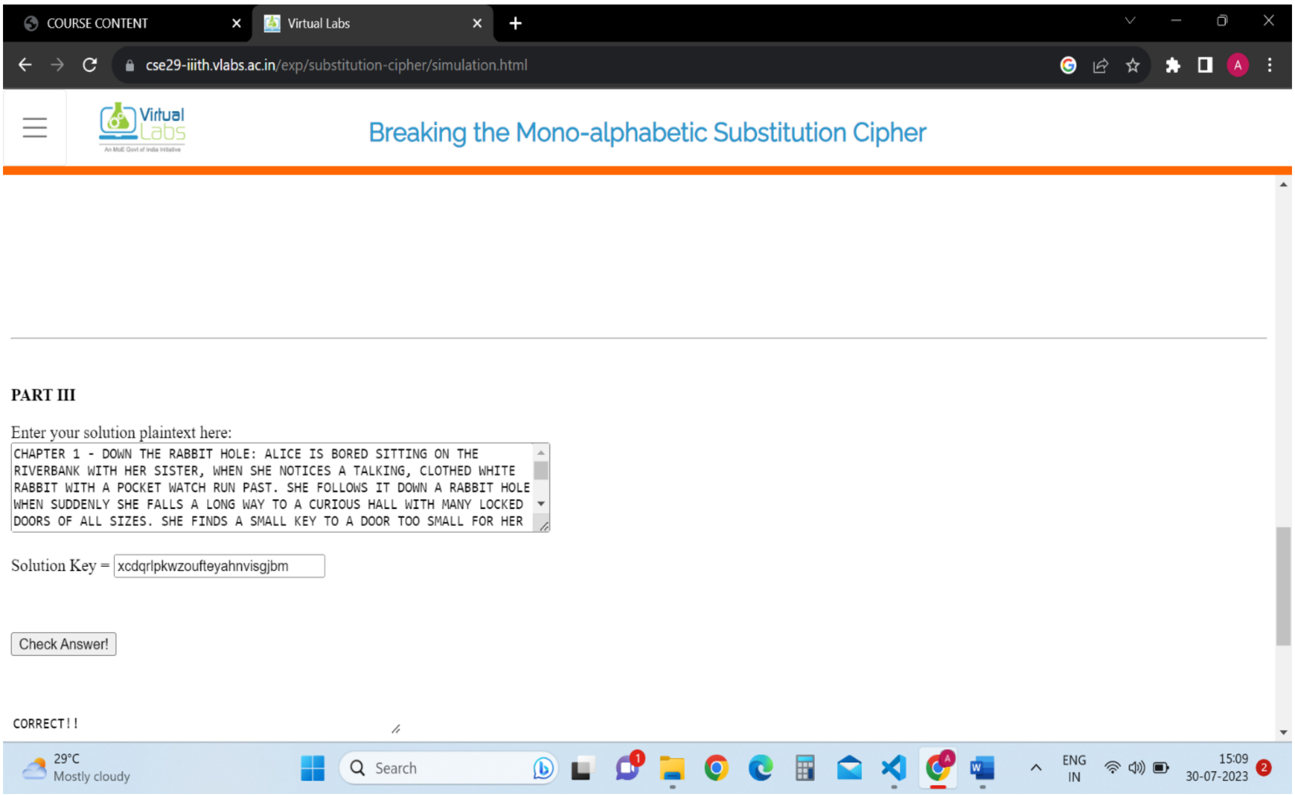
Replace cipher character q by plaintext character d Modify

Use the following function to undo any unwanted exchange by giving an uppercase character and a lower case. This is a case sensitive function:

Replace character by character Replace these exact characters

Your replacement history:

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


COURSE CONTENT
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/substitution-cipher/simulation.html
Virtual Labs
An MoE Govt of India Initiative
Breaking the Mono-alphabetic Substitution Cipher
29°C
Mostly cloudy
Search
ENG
IN
15:09
30-07-2023

PART III

Enter your solution plaintext here:

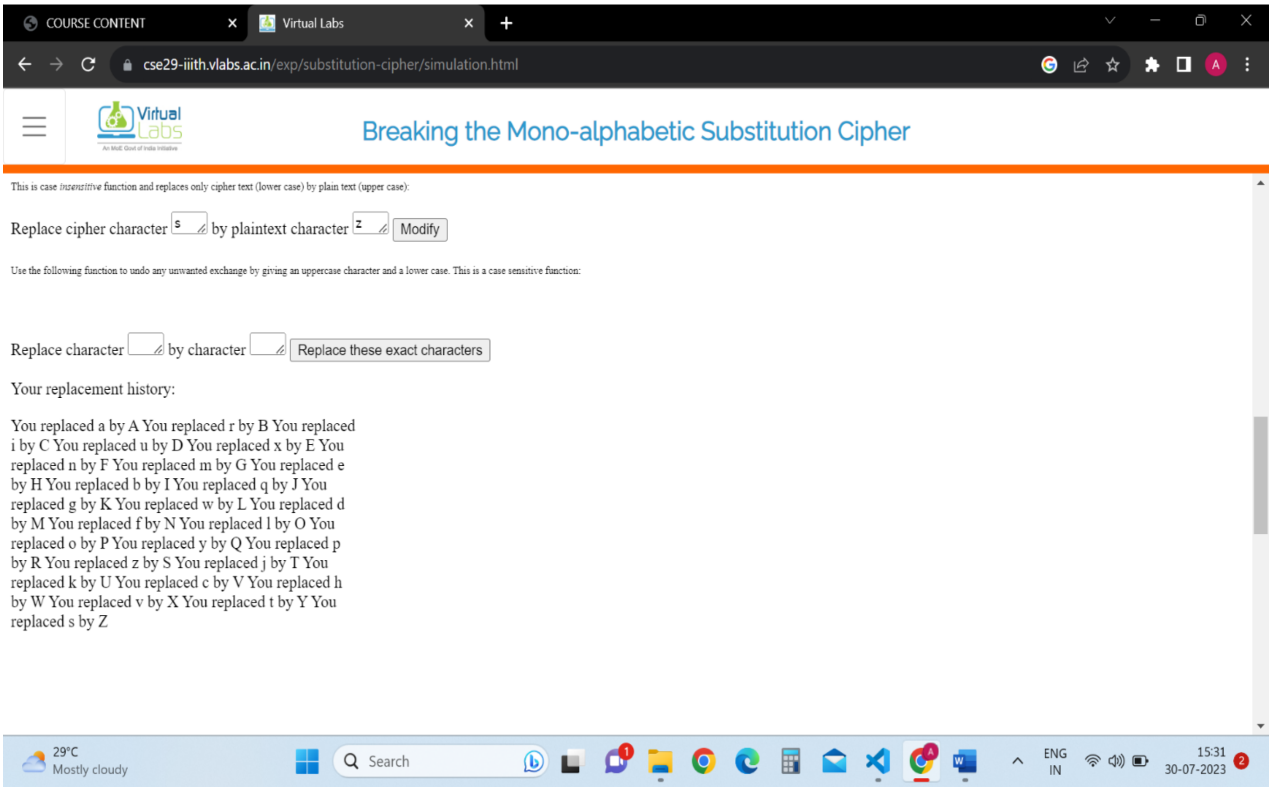
```
CHAPTER 1 - DOWN THE RABBIT HOLE: ALICE IS BORED SITTING ON THE
RIVERBANK WITH HER SISTER, WHEN SHE NOTICES A TALKING, CLOTHED WHITE
RABBIT WITH A POCKET WATCH RUN PAST. SHE FOLLOWS IT DOWN A RABBIT HOLE
WHEN SUDDENLY SHE FALLS A LONG WAY TO A CURIOUS HALL WITH MANY LOCKED
DOORS OF ALL SIZES. SHE FINDS A SMALL KEY TO A DOOR TOO SMALL FOR HER
```

Solution Key = xcdqrlpkwzoufteyahnvisgjbm

Check Answer!

```
CORRECT!!
```

NAME : Aman Singh BATCH : T23
SUBJECT : CNS LAB ROLL NO : 128


COURSE CONTENT
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/substitution-cipher/simulation.html
Virtual Labs
Modify
Replace these exact characters
29°C
Mostly cloudy
Search
ENG
IN
15:31
30-07-2023

Breaking the Mono-alphabetic Substitution Cipher

This is case *insensitive* function and replaces only cipher text (lower case) by plain text (upper case):

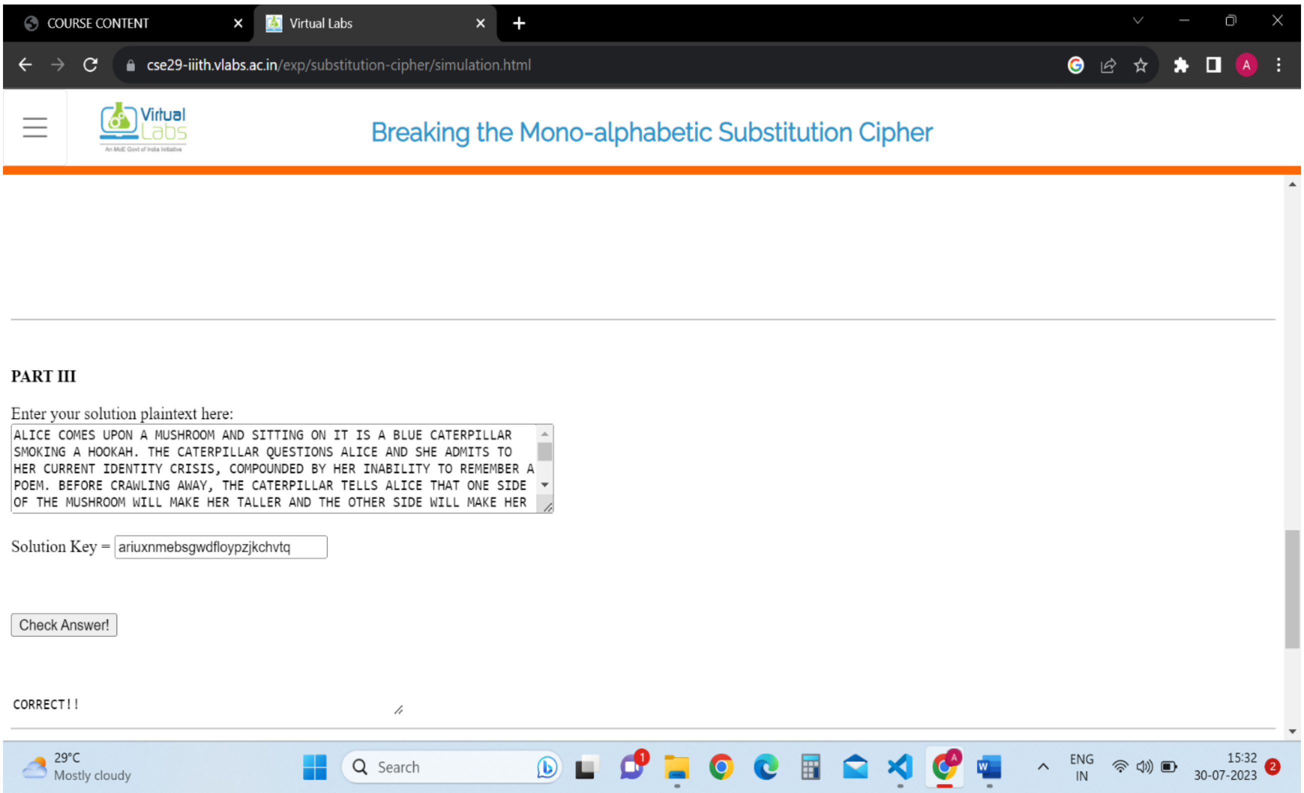
Replace cipher character s by plaintext character z

Use the following function to undo any unwanted exchange by giving an uppercase character and a lower case. This is a case sensitive function:

Replace character by character

Your replacement history:

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



Breaking the Mono-alphabetic Substitution Cipher

PART III

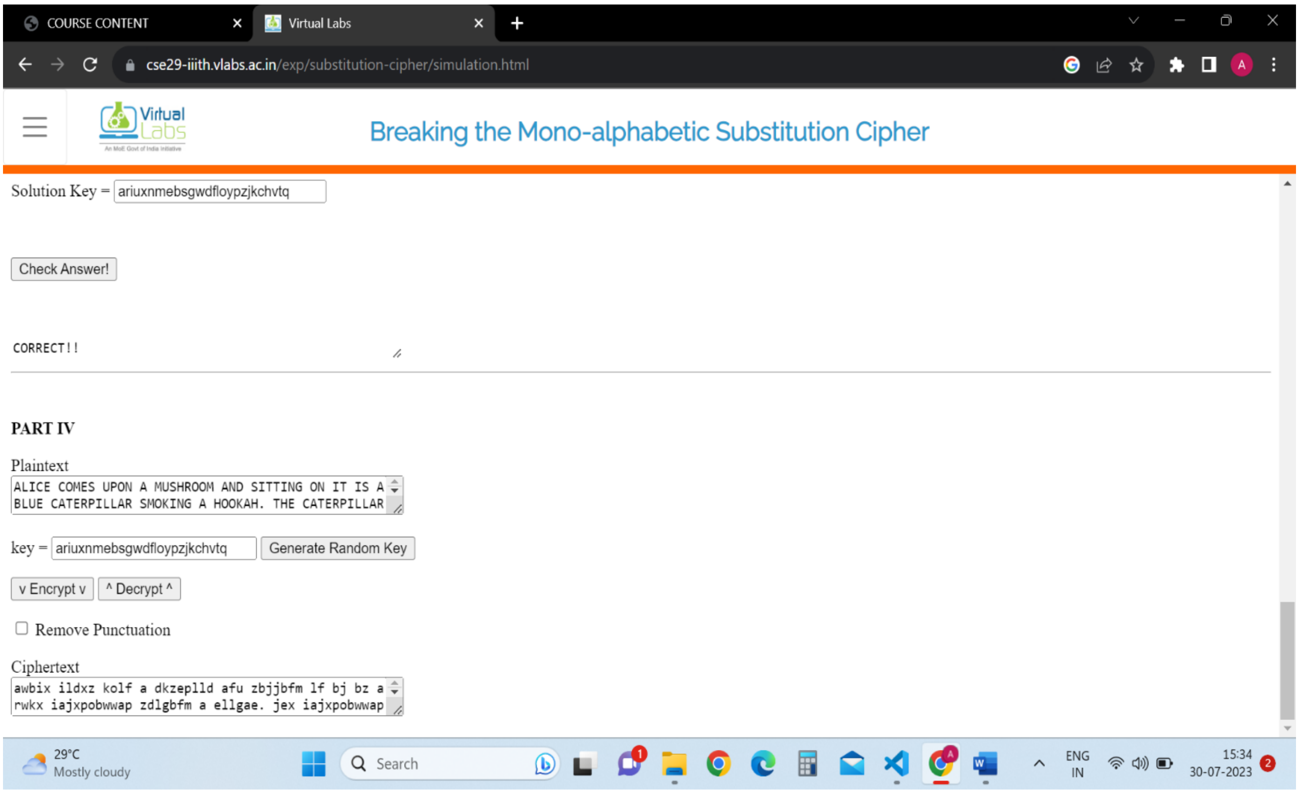
Enter your solution plaintext here:

```
ALICE COMES UPON A MUSHROOM AND SITTING ON IT IS A BLUE CATERPILLAR
SMOKING A HOOKAH. THE CATERPILLAR QUESTIONS ALICE AND SHE ADMITS TO
HER CURRENT IDENTITY CRISIS, COMPOUNDED BY HER INABILITY TO REMEMBER A
POEM. BEFORE CRAWLING AWAY, THE CATERPILLAR TELLS ALICE THAT ONE SIDE
OF THE MUSHROOM WILL MAKE HER TALLER AND THE OTHER SIDE WILL MAKE HER
```

Solution Key = ariuxnmebsgwdfloypzjkchvtq

```
CORRECT!!
```

NAME : Aman Singh BATCH : T23
SUBJECT : CNS LAB ROLL NO : 128



COURSE CONTENT
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/substitution-cipher/simulation.html
Virtual Labs
An MoE Govt of India Initiative

Breaking the Mono-alphabetic Substitution Cipher

Solution Key = ariuxnmebsgwdfloypzjkchvtq

Check Answer!

CORRECT!!

PART IV

Plaintext

```
ALICE COMES UPON A MUSHROOM AND SITTING ON IT IS A
BLUE CATERPILLAR SMOKING A HOOKAH. THE CATERPILLAR
```

key = ariuxnmebsgwdfloypzjkchvtq Generate Random Key

v Encrypt v ^ Decrypt ^

□ Remove Punctuation

Ciphertext

```
awbix ildxz kolf a dkzeplld afu zbjjbfm lf bj bz a
rwkx iajxpobwwap zdlgbfm a ellgae. jex iajxpobwwap
```

CONCLUSION:

Shift ciphers are simple and easy to implement, but they are not secure against brute force attacks due to the limited number of possible keys. On the other hand, monoalphabetic ciphers are more secure against brute force attacks due to the large number of potential keys, but they are vulnerable to frequency analysis attacks. To achieve stronger encryption, more complex encryption techniques like polyalphabetic ciphers or modern encryption algorithms should be used.