Security Lab T21
Pankaj Parihar
74

**Aim:**
Breaking shift cipher and Mono-alphabetic Substitution Cipher using Frequency analysis method.

## LO Mapping: LO1

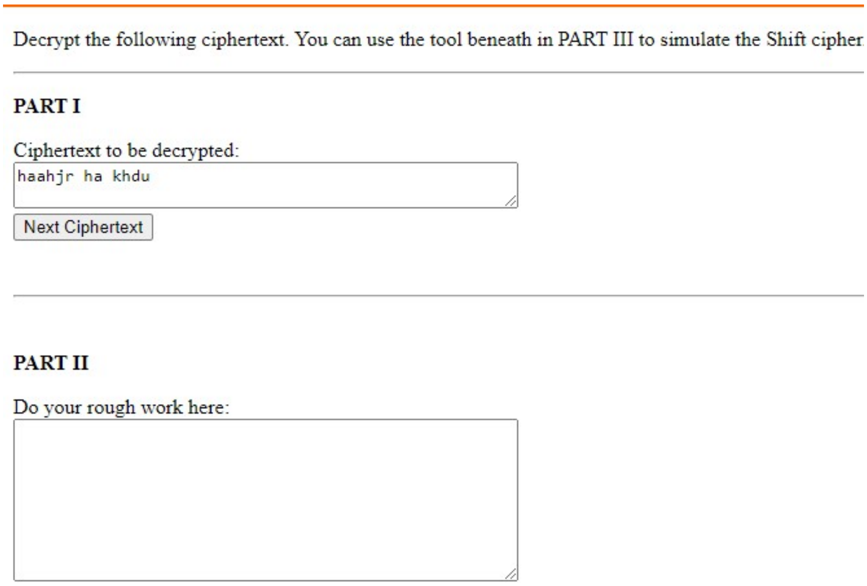
## Theory:

## Symmetric Cryptography:

- In cryptography, symmetric cryptography is a type of encryption where a single secret key is used for both encryption and decryption.
- The sender encrypts the message (plaintext) with the key, resulting in ciphertext (unreadable form).
- The receiver, who possesses the same key, can decrypt the ciphertext back to the original plaintext message.

## Shift Cipher:

- A Shift cipher is a very basic substitution cipher, a classic example of a symmetric cipher.
- It works by shifting each letter in the plaintext a fixed number of positions down the alphabet.



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

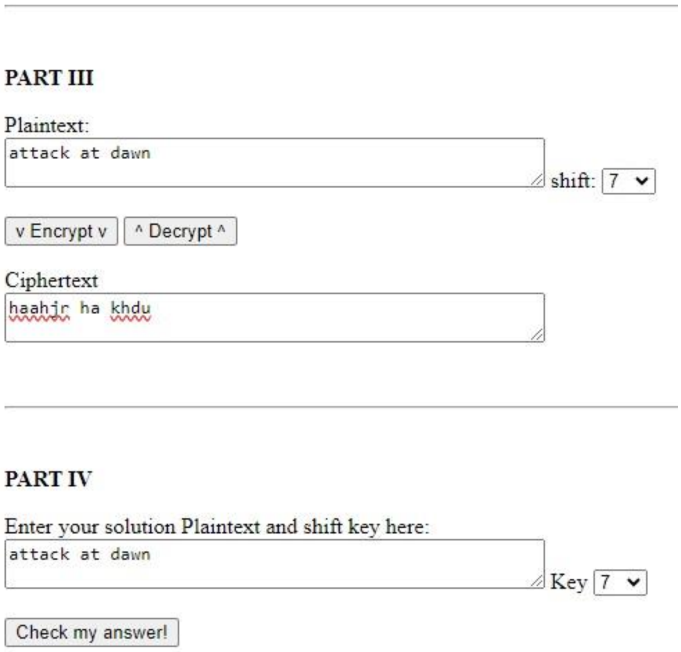
**PART I**

Ciphertext to be decrypted:

```
haahjr ha khdu
```

**PART II**

Do your rough work here:



PART III

Plaintext:

attack at dawn

shift: 7

Ciphertext

haahjr ha khdu

PART IV

Enter your solution Plaintext and shift key here:

attack at dawn

Key 7

Hence we discovered that every letter in the ciphertext was shifted by 7 and we used that to decrypt the cipher and get the original message.

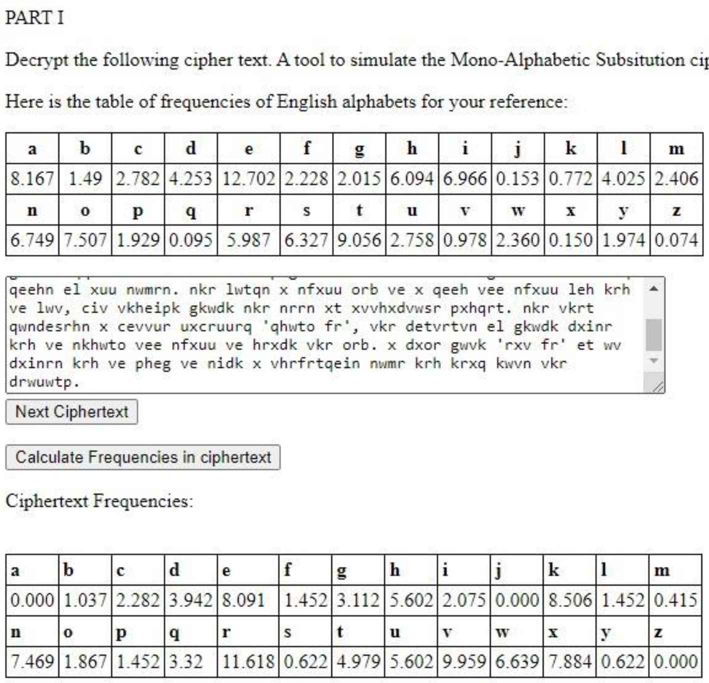
## Frequency Analysis:

- This is a cryptanalysis technique used to break ciphers by analyzing the frequency of letters in the ciphertext.
- The English language has a well-known distribution of letter frequencies, with letters like 'e' and 't' appearing more often than others.
- By comparing the letter frequencies in the ciphertext to the expected frequencies in English, cryptanalysts can try to identify the shift value used in the Caesar cipher.

Security Lab T21

Pankaj Parihar

74



PART I

Decrypt the following cipher text. A tool to simulate the Mono-Alphabetic Subsitution cipher is provided beneath for your assistance.

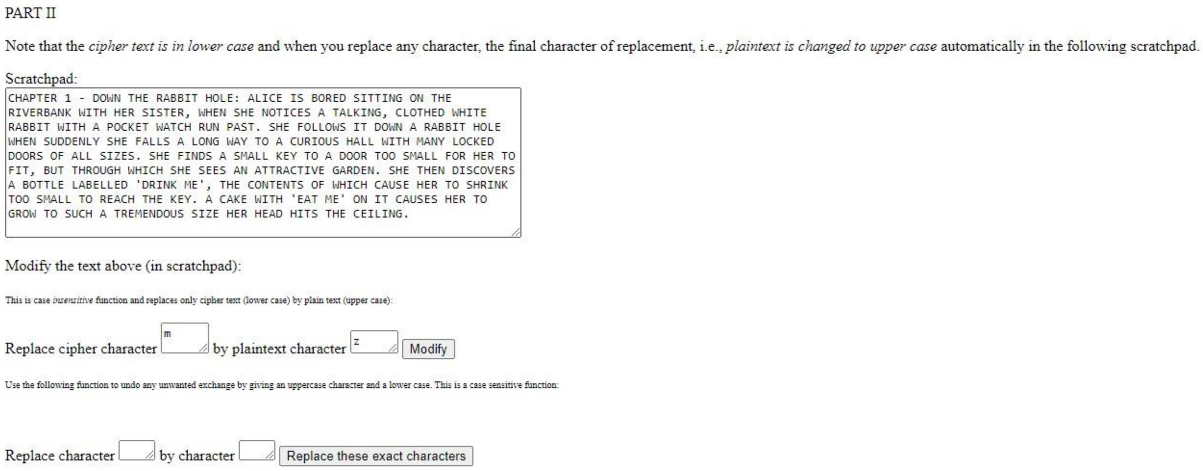
Here is the table of frequencies of English alphabets for your reference:

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **a** | **b** | **c** | **d** | **e** | **f** | **g** | **h** | **i** | **j** | **k** | **l** | **m** |
| 8.167 | 1.49 | 2.782 | 4.253 | 12.702 | 2.228 | 2.015 | 6.094 | 6.966 | 0.153 | 0.772 | 4.025 | 2.406 |
| **n** | **o** | **p** | **q** | **r** | **s** | **t** | **u** | **v** | **w** | **x** | **y** | **z** |
| 6.749 | 7.507 | 1.929 | 0.095 | 5.987 | 6.327 | 9.056 | 2.758 | 0.978 | 2.360 | 0.150 | 1.974 | 0.074 |

```
qeehn el xuu nwmrn. nkr lwtqn x nfxuu orb ve x qeeh vee nfxuu leh krh
ve lwv, civ vkheipk gkwdk nkr nrrn xt xvvhxdvwsr pxhqrt. nkr vkrt
qwndesrhn x cevvur uxcruurq 'qhwto fr', vkr detvrtvn el gkwdk dxinr
krh ve nkhwto vee nfxuu ve hrxdk vkr orb. x dxor gwvk 'rxv fr' et wv
dxinrn krh ve pheg ve nidk x vhrfrtqein nwmr krh krxq kwvn vkr
drwuwtp.
```

Ciphertext Frequencies:

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **a** | **b** | **c** | **d** | **e** | **f** | **g** | **h** | **i** | **j** | **k** | **l** | **m** |
| 0.000 | 1.037 | 2.282 | 3.942 | 8.091 | 1.452 | 3.112 | 5.602 | 2.075 | 0.000 | 8.506 | 1.452 | 0.415 |
| **n** | **o** | **p** | **q** | **r** | **s** | **t** | **u** | **v** | **w** | **x** | **y** | **z** |
| 7.469 | 1.867 | 1.452 | 3.32 | 11.618 | 0.622 | 4.979 | 5.602 | 9.959 | 6.639 | 7.884 | 0.622 | 0.000 |



PART II

Note that the *cipher text is in lower case* and when you replace any character, the final character of replacement, i.e., *plaintext is changed to upper case* automatically in the following scratchpad.

Scratchpad:

```
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 TO
FIT, BUT THROUGH WHICH SHE SEES AN ATTRACTIVE GARDEN. SHE THEN DISCOVERS
A BOTTLE LABELLED 'DRINK ME', THE CONTENTS OF WHICH CAUSE HER TO SHRINK
TOO SMALL TO REACH THE KEY. A CAKE WITH 'EAT ME' ON IT CAUSES HER TO
GROW TO SUCH A TREMENDOUS SIZE HER HEAD HITS THE CEILING.
```

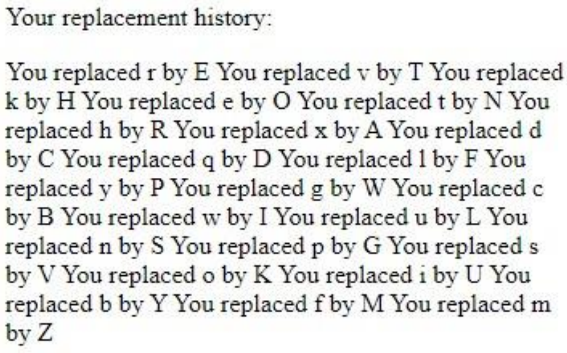
Modify the text above (in scratchpad):

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

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

From this we figured out which letter in cipher was mapped to which letter and were able to decrypt the original message.

## Conclusion:

In conclusion, frequency analysis is a powerful tool for breaking both shift ciphers and mono-alphabetic substitution ciphers. By analyzing the frequency of letters and comparing them to known language frequency distributions, we can effectively reverse-engineer the encryption. This method exploits the inherent weaknesses in these ciphers, particularly their lack of variation in letter substitution, making them vulnerable to cryptographic attacks.