**EXPERIMENT NO - 01**

**Name: Kale Komal Janardan**

**Div: TE IT – A**

**Roll No.: ITA539 Batch: A2**

**DOP: Sign:**

**DOS: Grade:**

**---------------------------------------------------------------------------------------------------------**

**Aim:** Breaking the mono-alphabetic substitution cipher using frequency analysis method.

**About the experiment:**

In this experiment, we work with another well-known historical encryption scheme, namely the mono-alphabetic substitution cipher that has a very large key space. However, it is quite easily broken using “Frequency analysis” methods. Your task is to break this cipher. Specifically, given (only) the cipher text in some instance of a mono alphabetic substitution cipher, you need to find the plain text and the secret key.

**Theory:**

Consider we have the plain text "cryptography". By using the substitution table below, we can encrypt our plain text as follows:

abcd efgh ijkl mnop qrst uvwx yz

JIBR KTCN OFQY GAUZ HSVW MXLD EP

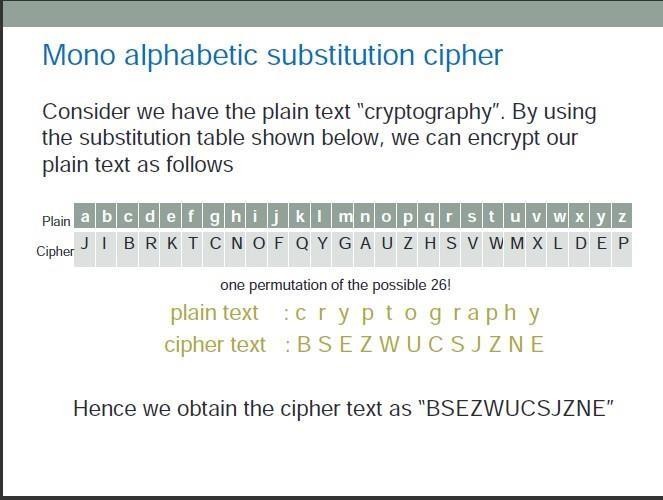
**plain text: c r y p t o g r a p h y**

**cipher text: B S E Z W U C S J Z N E**

Hence, we obtain the cipher text as “BSEZWUCSJZNE”.

**Cryptanalysis**

Note that the frequency of occurrence of characters in the plaintext is "preserved" in the cipher text. For instance, the most frequent character in the cipher text is likely to be the encryption of the plaintext character "e" which is the most frequently occurring character in English. For a very brief theory of the mono-alphabetic substitution cipher and its cryptanalysis.

****

# Procedure:

**STEP 1:** For the given cipher text in the PART Iof the experiment page, the first step is to generate cipher text by clicking on the "Next Cipher Text" button.

**STEP 2:** Calculate frequencies of generated cipher text by clicking on "Calculate Frequencies in Cipher text" button.

**STEP 3:** Copy the generated cipher text from PART Iand paste in "Scratchpad" area of PART II.

**STEP 4:** Analyze similarities between "Calculated Frequencies Table" and "English Alphabet Frequencies Table".

**STEP 5:** Based on similarities, try to make a frequency-based estimation for each character of cipher text.

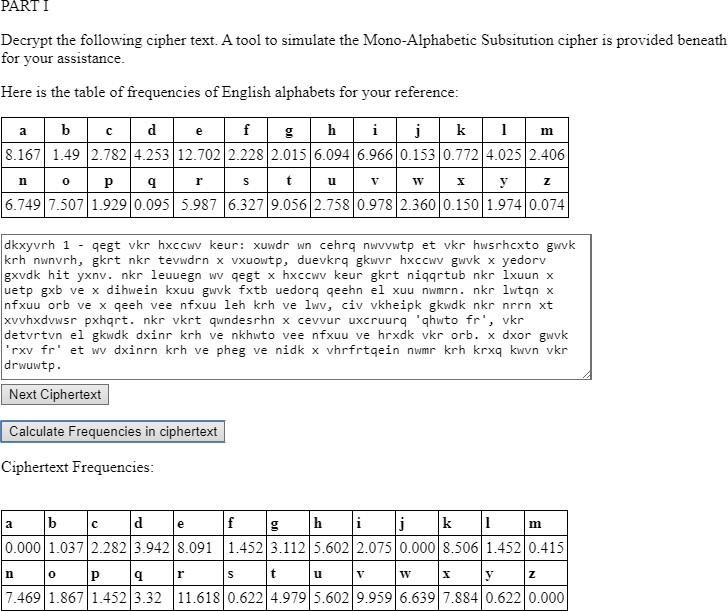
**STEP 6:** Replace characters of Cipher Text in Scratchpad with a character estimated previously using a Modifyfunction of PART II.

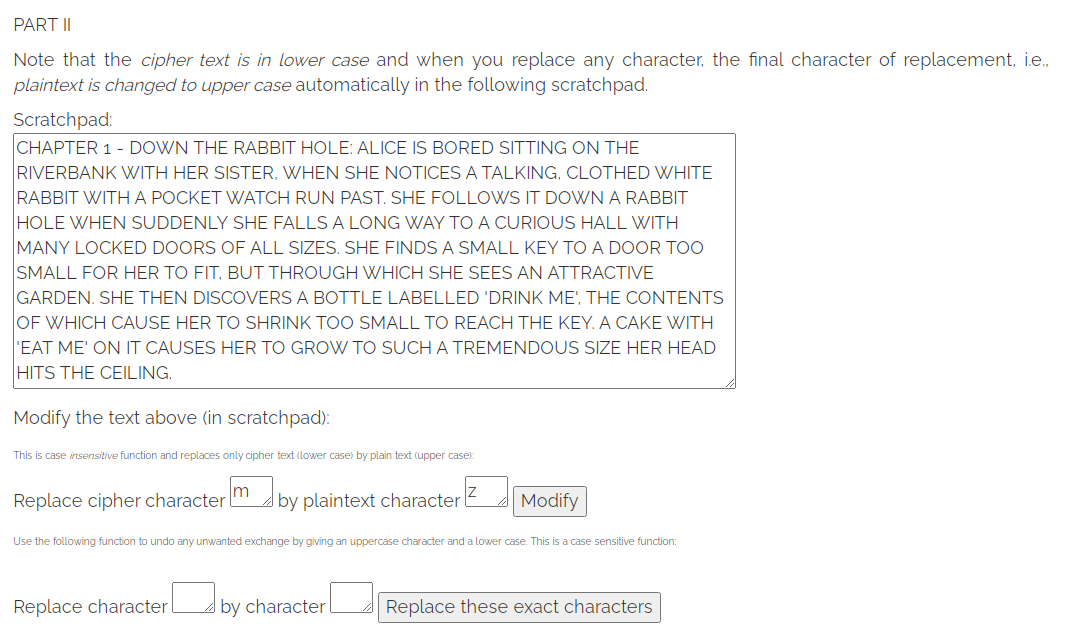
**STEP 7:** Based on Hints from Cipher text in "Scratchpad" area make more replacement of cipher text characters.

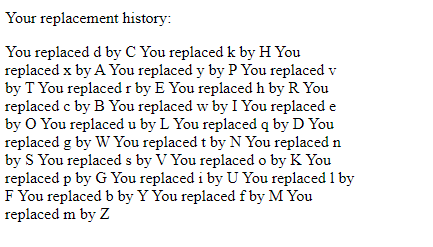
**STEP 8:** Repeat Step 7till you get a meaningful English Text.

**Simulation:**

**PART I:**

**PART II:**

****

****

**Conclusion:**

Thus, we have studied how to break the Mono-alphabetic Substitution Cipher Successfully.