EXPERIMENT NUMBER: 1

Date of Performance :

Date of Submission :

Aim: Breaking the Mono-alphabetic Substitution Cipher using Frequency analysis method.

Theory:

Breaking the Mono-alphabetic Substitution Cipher

Consider we have the plain text "cryptography". By using the substitution table below, we can encrypt our plain text as follows: abcdefgh i j k l mnopqr s t u vwxyz

JI BRKTCNOFQYG AUZHSVWMXL DEP

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 ciphertext. For instance, the most frequent character in the ciphertext is likely to be the encryption of the plaintext character "e" which is the most frequently occurring charecter in English. For a very brief theory of the mono-alphabetic substitution cipher and its cryptanalysis.

Procedure:

STEP 1 : For the given ciphertext in the **PART I** of the experiment page, the first step is to generate ciphertext by clicking on the "Next CipherText" button.

STEP 2 : Calculate frequencies of generated ciphertext by clicking on "Calculate Frequencies in Ciphertext" button

STEP 3 : Copy the generated ciphertext from **PART I** and paste in "Scratchpad" area of **PART II**

STEP 4 : Analyse similarties 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 ciphertext

STEP 6 : Replace characters of CipherText in Scratchpad with a character estimated previously using a **Modify** function of **PART II**

STEP 7 : Based on Hints from Ciphertext in "Scratchpad" area make more replacement of ciphertext characters

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

STEP 9 : Finally, observe the deciphered plaintext in Scratchpad Area,if a meaningful English text is formed cut-and-paste it in the text-field named "Solution Plaintext" of **PART III**. Also enter the final character mapping in the"Solution Key" in **PART III** and click on "Check Answer" button.

STEP 10[OPTIONAL] : Verify that your answer is correct, by encrypting the solution plaintext with your key in **PART IV**.

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**
8.1	1.4	2.7	4.2	12.7	2.2	2.0	6.0	6.9	0.1	0.7	4.0	2.4
67	9	82	53	02	28	15	94	66	53	72	25	06
n	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
6.7	7.5	1.9	0.0	5.98	6.3	9.0	2.7	0.9	2.3	0.1	1.9	0.0
49	07	29	95	7	27	56	58	78	60	50	74	74

Ciphertext Frequencies:

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:

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 by plaintext character

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:

PART III

Enter your solution plaintext here:

Solution Key =

PART IV

Plaintext

key = phqgiumeaylnofdxjkrcvstz

□ Remove Punctuation

Ciphertext

CONCLUSION/ Outcome:

we successfully implemented breaking the mono-alphabetic Substitution cipher using frequency analysis method.

Marks & Signature:

R1 (5 Marks)	R2 (5 Marks)	R3 (5 Marks)	Total (15 Marks)	Signature