Semester	T.E. Semester VI – Computer Engineering
Subject	Cryptography and cyber security
Subject Professor In-charge	Prof. Amit Nerurkar
Assisting Teachers	Prof. Amit Nerurkar
Laboratory	M312B

Student Name	Deep Salunkhe
Roll Number	21102A0014
TE Division	A

Title: Design and Implementation of Monoalphabetic Cipher

Explanation:

A monoalphabetic substitution cipher is a simple form of encryption where each letter in the plaintext is replaced by a corresponding letter in the ciphertext according to a fixed substitution scheme. In other words, each letter is consistently replaced by another letter throughout the message.

Breaking a monoalphabetic substitution cipher involves identifying the substitution key or pattern used to encrypt the message so that it can be decrypted. Here's a general approach to breaking such a cipher:

1. Frequency Analysis: Since the encryption scheme replaces each letter with another letter, the frequency of letters in the ciphertext should roughly correspond to the frequency of letters in the plaintext language. For instance, in English, 'E' is the most common letter, followed by 'T', 'A', and so on. By analyzing the frequency of letters in the ciphertext, one can make educated guesses about the substitutions.

2. Single-Letter Words: In English, the most common single-letter word is 'I'. If a single-letter word appears frequently in the ciphertext, it's likely to correspond to 'I' in the plaintext. Similarly, if a three-letter word appears, it's often 'THE'. Using such patterns can help deduce some letters.

3. Pattern Recognition: Look for recurring patterns of letters in the ciphertext, which may correspond to common words, prefixes, or suffixes in the plaintext. For example, 'TH', 'ING', 'TION', etc., are common patterns in English.

4. Contextual Analysis: If part of the message is known or can be guessed, it can provide clues about the substitutions. For instance, if the encrypted message is likely to contain certain common words or phrases (like "Dear," "Sincerely," etc.), identifying these can help determine their corresponding ciphertext letters.

5. Trial and Error: Use a combination of the above techniques to make educated guesses about the substitutions. You can start with the most frequently occurring letters and work your way down. As more letters are decrypted, it becomes easier to decipher the rest of the message.

6. Iterative Refinement: As more letters are decrypted, refine the substitutions and reanalyze the ciphertext for additional patterns and clues. This iterative process continues until the entire message is decrypted.

7. Manual or Automated Methods: Breaking a monoalphabetic substitution cipher can be done manually or with the help of computer algorithms. Automated methods can significantly speed up the process, especially for longer messages.

Simulation:

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

```
dkxyvrh 1 - qegt vkr hxccwv keur: xuwdr wn cehrq nwvvwtp et vkr
hwsrhcxto gwvk krh nwnvrh, gkrt nkr tevwdrn x vxuowtp, duevkrq gkwvr
hxccwv gwvk x yedorv gxvdk hit yxnv. nkr leuuegn wv qegt x hxccwv keur
gkrt niqqrtub nkr lxuun x uetp gxb ve x dihwein kxuu gwvk fxtb uedorq
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
```

Next Ciphertext

Calculate Frequencies in ciphertext

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

PART III

Enter your solution plaintext here:

```
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.
```

Solution Key = xcdqrlpkwzoufteyahnvisgjbm

Check Answer!

```
CORRECT!!
```

PART IV

Plaintext

```
with 'eat me' on it causes her to grow to such a
tremendous size her head hits the ceiling.
```

key = xcdqrlpkwzoufteyahnvisgjbm [Generate Random Key]

[v Encrypt v] [^ Decrypt ^]

☐ Remove Punctuation

Ciphertext

```
dkxyvrh 1 - qegt vkr hxccwv keur: xuwdr wn cehrq
nwvvwtp et vkr hwsrhcxto gwvk krh nwnvrh, gkrt nkr
```

Conclusion:

In conclusion, breaking a monoalphabetic substitution cipher involves analyzing the frequency, patterns, and context of the ciphertext to deduce the substitutions used in the encryption. By employing techniques such as frequency analysis, identifying single-letter words, recognizing patterns, considering contextual clues, and employing trial and error, it's possible to decrypt the message. This process may require manual effort or the use of automated methods, depending on the complexity of the cipher and the available resources. Ultimately, with patience, persistence, and careful analysis, the encryption key or pattern can be determined, allowing for the decryption of the message.