CNS

Chaitanya Padol
Roll No-74 T2

Assignment 1

Aim : Breaking shift ~~Gy~~ cipher and Mono-alphabetic substitution Cipher

Theory: **Shift Cipher**

Shift Ciphers work by using the modulo operator to encrypt and decrypt messages. The Shift Cipher has a key (K), which is an integer from 0 to 25. The key is only shared with people that we want to see our message

Example: Plain text = PADOL

key = 7

Encryption

P A D O L

16 1 4 15 12

+ 7 7 7 7 7

(23 8 11 22 19) mod 26

23 8 11 22 19

W H K V S (cipher text)

How and why shift cipher can be broken using a brute force attack?

The Frequency of the letter pattern provides a big clue in deciphering the entire message. Plaintext can be received by using brute force by studying the frequency of characters and linking them to their usage in regular language

Mono alphabetic cipher

In monoalphabetic ciphers, letters of the plain text are mapped to cipher text letters based on a single alphabet key

Example:- STRESS - plain text

S → A   E → B
T → E   S → C
R → S

Encrypted - AESBCC

Can it be broken using Brute force Attack ? Why ?

Yes, Monoalphabetic Cipher can be broken using Brute force Attack such as Frequency Analysis

How are they broken using frequency analysis

Frequency of all characters appearing in the ciphertext are noted

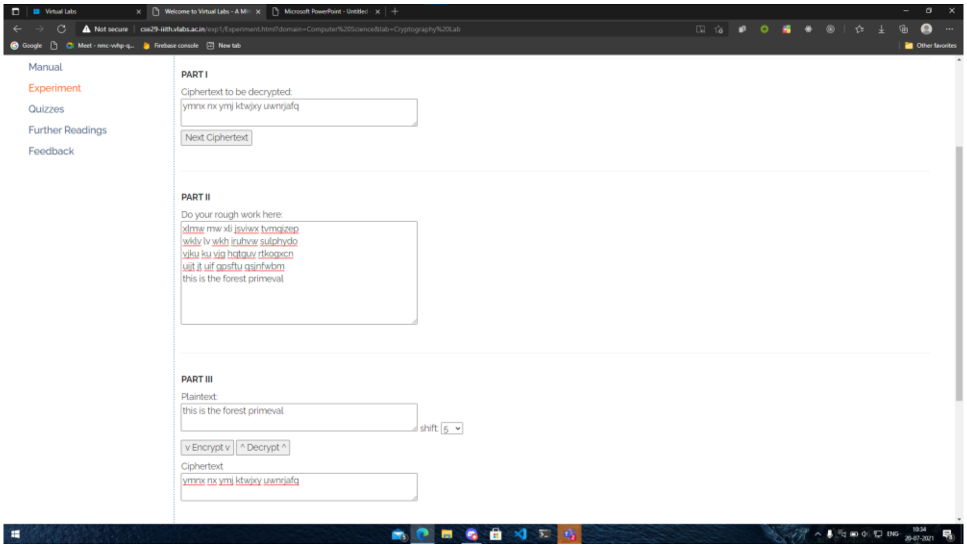
These frequencies are mapped starting from mapping the most commonly seen cipher character to the most commonly seen character in regular language

After utilizing frequency values and common knowledge of the language, words like 'the' are mapped.

We can try various combination for the unassigned characters

Conclusion : In this experiment we learnt about shift and monoalphabetic ciphers. These techniques are easy to implement but they are easy to decrypt as well hence providing less security. But they provide a better solution than plain text.

Shift Cipher


Virtual Labs
Welcome to Virtual Labs - A MH
Microsoft PowerPoint - Untitled
Not secure
cse29-iiith.vlabs.ac.in/exp1/Experiment.html?domain=Computer%20Science&lab=Cryptography%20Lab
Google
Meet - nmc-whp-q...
Firebase console
New tab
Manual
Experiment
Quizzes
Further Readings
Feedback
Next Ciphertext
v Encrypt v
^ Decrypt ^

PART I

Ciphertext to be decrypted:

ymnx nx ymj ktwjxy uwnrjafq

PART II

Do your rough work here:

xlmw mw xli jsviwx tvmqizep
wklv lv wkh iruhvw sulphydo
vjku ku vjg hqtguv rtkogxcn
uijt jt uif gpsftu qsjnfwbm
this is the forest primeval

PART III

Plaintext:

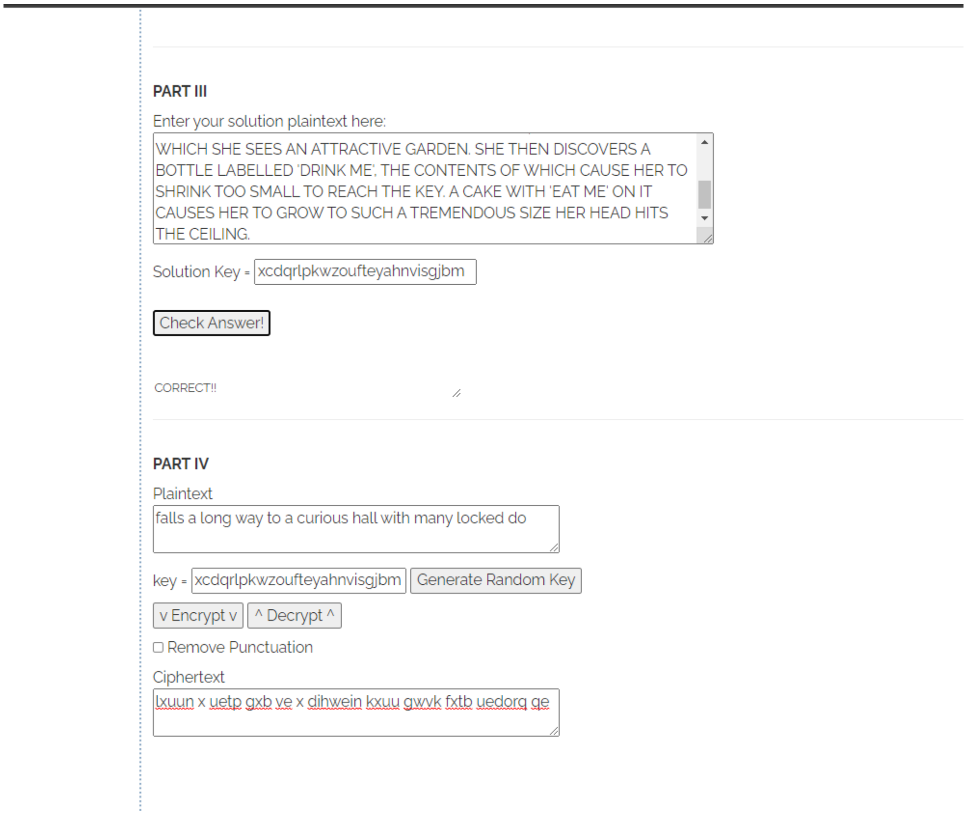
this is the forest primeval

shift: 5

Ciphertext

ymnx nx ymj ktwjxy uwnrjafq

Monoalphabetic Cipher



PART III

Enter your solution plaintext here:

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

CORRECT!!

PART IV

Plaintext

falls a long way to a curious hall with many locked do

key = xcdqrlpkwzoufteyahnvisgjbm

□ Remove Punctuation

Ciphertext

lxuun x uetp gxb ve x dihwein kxuu gwvk fxtb uedorq qe