Don Bosco Institute of Technology, Mumbai 400070
Department of Information Technology

Experiment No. : 2

Date: 09/09/2022

Title : Cryptanalysis of Mono-alphabetic Substitution Cipher

Problem Definition : Break down the Mono-alphabetic Substitution Cipher using Frequency analysis method. Decode the given cipher text “slaz tlla avupnoa ha aol whyr”.

Pre-requisite : Any programming knowledge – C, C++, Java, Python and concepts of symmetric cryptography.

Theory :

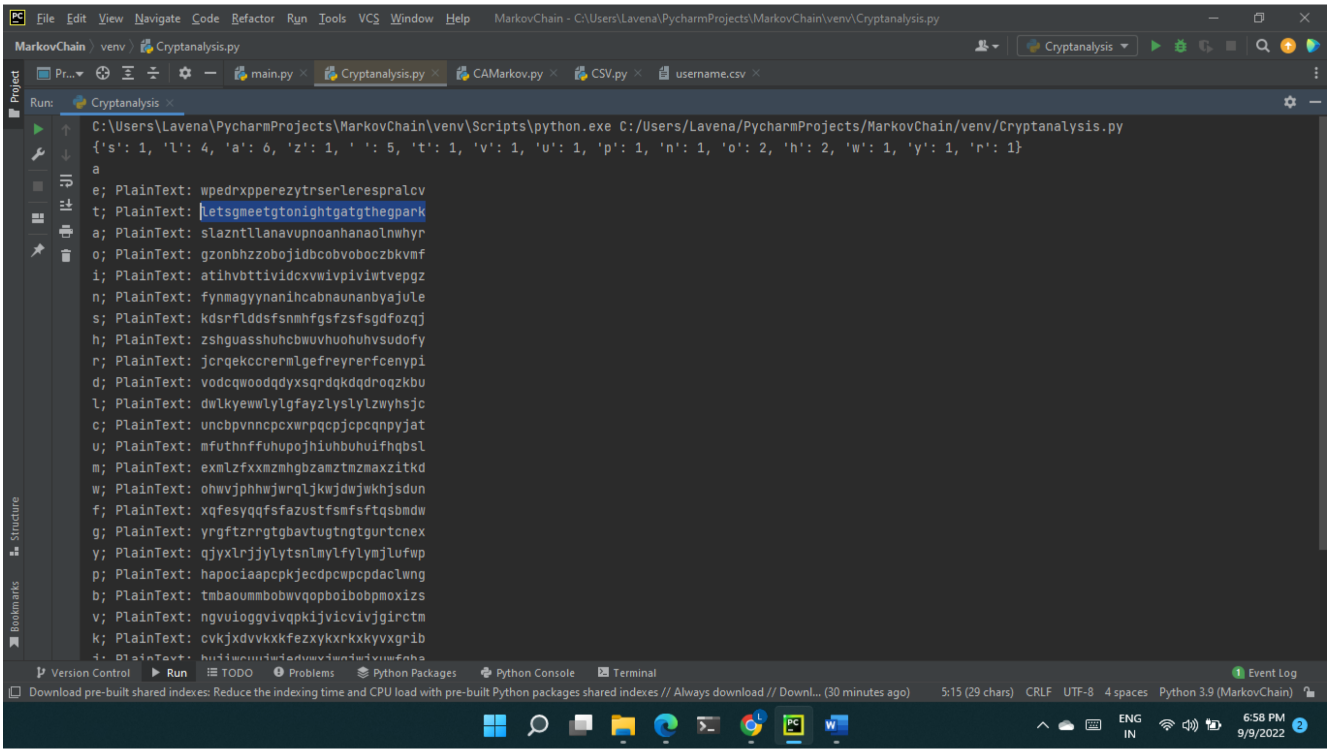
A monoalphabetic substitution is a cipher in which each occurrence of a plaintext symbol is replaced by a corresponding ciphertext symbol to generate ciphertext. The key for such a cipher is a table of the correspondence or a function from which the correspondence is computed.

Cryptanalysis is the decryption and analysis of codes, ciphers or encrypted text. Cryptanalysis uses mathematical formulas to search for algorithm vulnerabilities and break into cryptography or information security systems.

Procedure/ Algorithm :

```
most_used = ['e', 't', 'a', 'o', 'i', 'n', 's', 'h', 'r', 'd', 'l', 'c', 'u', 'm',
'w', 'f', 'g', 'y', 'p', 'b', 'v', 'k', 'j',
'x', 'q', 'z']

cipher_text =  'slaz tlla avupnoa ha aol whyr'

occurence = {}

for symbol in cipher_text:
    if symbol in occurence:
        occurence[symbol] += 1
    else:
        occurence[symbol] = 1

print(occurence)

def decrypt(cipher_text, k):
    plain_text = ""
    for symbol in cipher_text:
        pt = (ord(symbol) - 97 - k)%26
        pt = chr(pt+97)
        plain_text += "".join(pt)
    print(f"{letter}; PlainText: {plain_text}")

word = max(occurence, key=occurence.get)
print(word)

for letter in most_used:
    k = (ord(word) - ord(letter))%26
    decrypt(cipher_text, k)
```

Results :



```
C:\Users\Lavena\PycharmProjects\MarkovChain\venv\Scripts\python.exe C:/Users/Lavena/PycharmProjects/MarkovChain/venv/Cryptanalysis.py
{'s': 1, 'l': 4, 'a': 6, 'z': 1, ' ': 5, 't': 1, 'v': 1, 'u': 1, 'p': 1, 'n': 1, 'o': 2, 'h': 2, 'w': 1, 'y': 1, 'r': 1}
a
e; PlainText: wpedrxpperezytrserlerespralcv
t; PlainText: letsgmeetgtonightgatgthegpark
a; PlainText: slazntllanavupnoanhanaolnwhyr
o; PlainText: gzonbhzzobojidbcobvoboczbkvmf
i; PlainText: atihvbttividcxvwivpiviwtvepgz
n; PlainText: fynmagyynanihcabnaunanbyajule
s; PlainText: kdsrflddsfsnmhfgsfzsfsgdfozqj
h; PlainText: zshguasshuhcbwuvhuohuhvsudofy
r; PlainText: jcrqekccrermlgefreyrerfcenypi
d; PlainText: vodcqwoodqdyxsqrdqkdqdroqzkbu
l; PlainText: dwlkyewwlylgfayzlyslylzwyhsjc
c; PlainText: uncbpvnncpcxwrpqcpjcpcqnpyjat
u; PlainText: mfuthnffuhupojhiuhbuhuifhqbsl
m; PlainText: exmlzfxxmzmhgbzamztmzmaxzitkd
w; PlainText: ohwvjphhwjwrqljkwjdwjwkhjsdun
f; PlainText: xqfesyqqfsfazustfsmfsftqsbmdw
g; PlainText: yrgftzrrgtgbavtugtngtgurtcnex
y; PlainText: qjyxlrjjylytsnlmylfylymjlufwp
p; PlainText: hapociaapcpkjecdpcwpcpdaclwng
b; PlainText: tmbaoummbobwvqopboibobpmoxizs
v; PlainText: ngvuioggvivqpkijvicvivjgirctm
k; PlainText: cvkjxdvvkxkfezxykxrkxkyvxgrib
j; PlainText: hujjwcuujwjedvwxjwqjwjxuwfqba
```

File Edit View Navigate Code Refactor Run Tools VCS Window Help
MarkovChain - C:\Users\Lavena\PycharmProjects\MarkovChain\venv\Cryptanalysis.py
MarkovChain 〉 venv 〉 Cryptanalysis.py
Cryptanalysis
main.py
Cryptanalysis.py
CAMarkov.py
CSV.py
username.csv
Run: Cryptanalysis
Version Control
Run
TODO
Problems
Python Packages
Python Console
Terminal
Event Log
Download pre-built shared indexes: Reduce the indexing time and CPU load with pre-built Python packages shared indexes // Always download // Downl... (30 minutes ago)
5:15 (29 chars) CRLF UTF-8 4 spaces Python 3.9 (MarkovChain)
ENG IN
6:58 PM 9/9/2022

References :

https://uregina.ca/~kozdron/Teaching/Cornell/135Summer06/Handouts/monoalphabet.pdf
https://www.techopedia.com/definition/1769/cryptanalysis

Lab practice (optional):

L1. Decode "Iwoo xqjg bkn haypqnao pkzwu"

Questions (Short, Long, MCQs) (optional):

S1. What is cryptology, cryptography and cryptanalysis?

Cryptology is the mathematics, such as number theory and the application of formulas and algorithms, that underpin cryptography and cryptanalysis.

Cryptography is technique of securing information and communications through use of codes so that only those people for whom the information is intended can understand it and process it.

Cryptanalysis is the decryption and analysis of codes, ciphers or encrypted text. Cryptanalysis uses mathematical formulas to search for algorithm vulnerabilities and break into cryptography or information security systems.

S2. What is Mono-alphabetic Substitution Cipher?

A monoalphabetic substitution is a cipher in which each occurrence of a plaintext symbol is replaced by a corresponding ciphertext symbol to generate ciphertext. The key for such a cipher is a table of the correspondence or a function from which the correspondence is computed.