INTRODUCTION TO CRYPTOGRAPHY – LAB 1

B.Tech. Computer Science and Engineering (Cybersecurity)

|  |  |
| --- | --- |
| Name: Anish Sudhan Nair | Roll No.: K041 |
| Batch: K2/A2 | Date of performance: 22/12/2021 |

Aim: To implement shift ciphers and to study various terms related to cryptography.

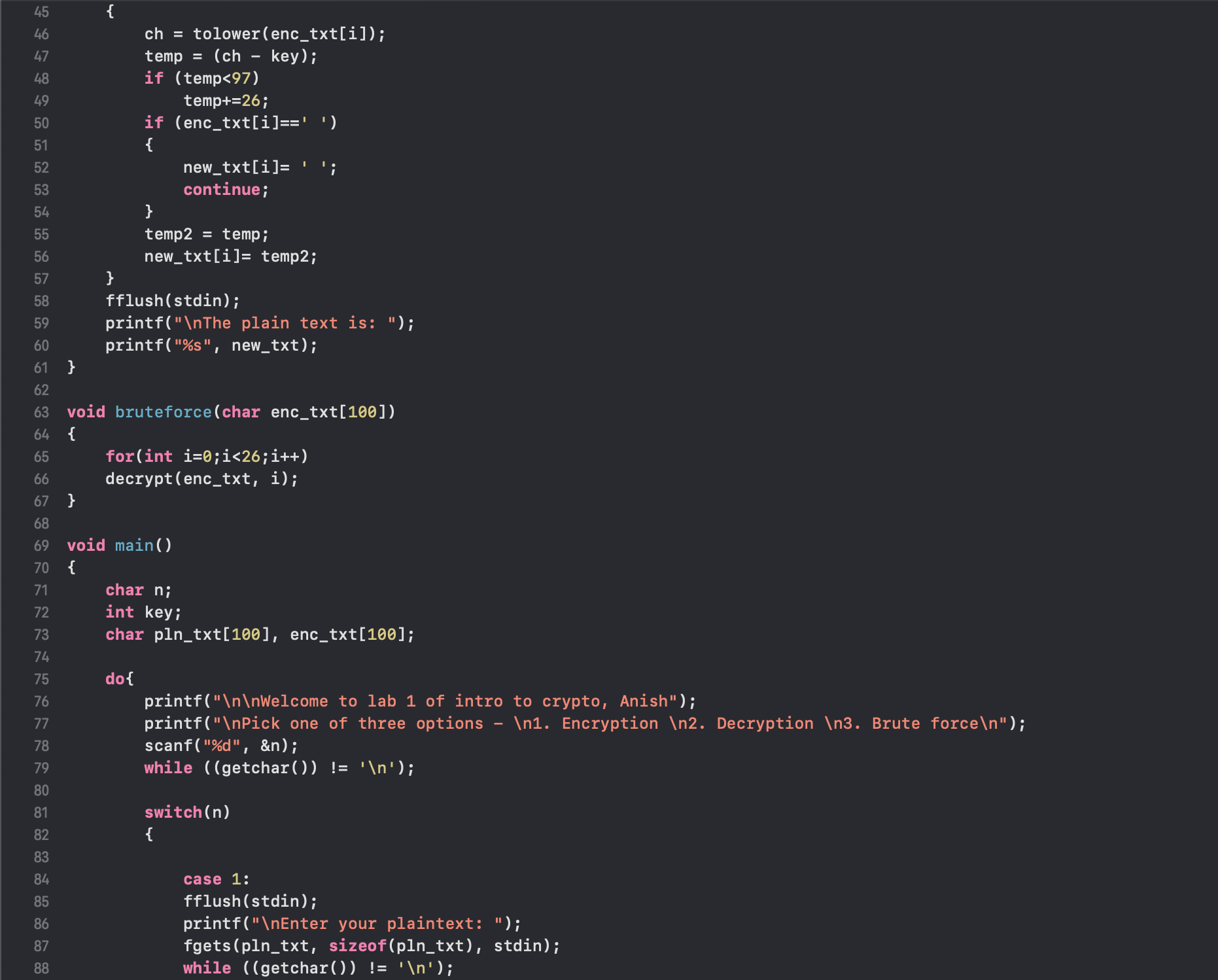
Code:

Language: C

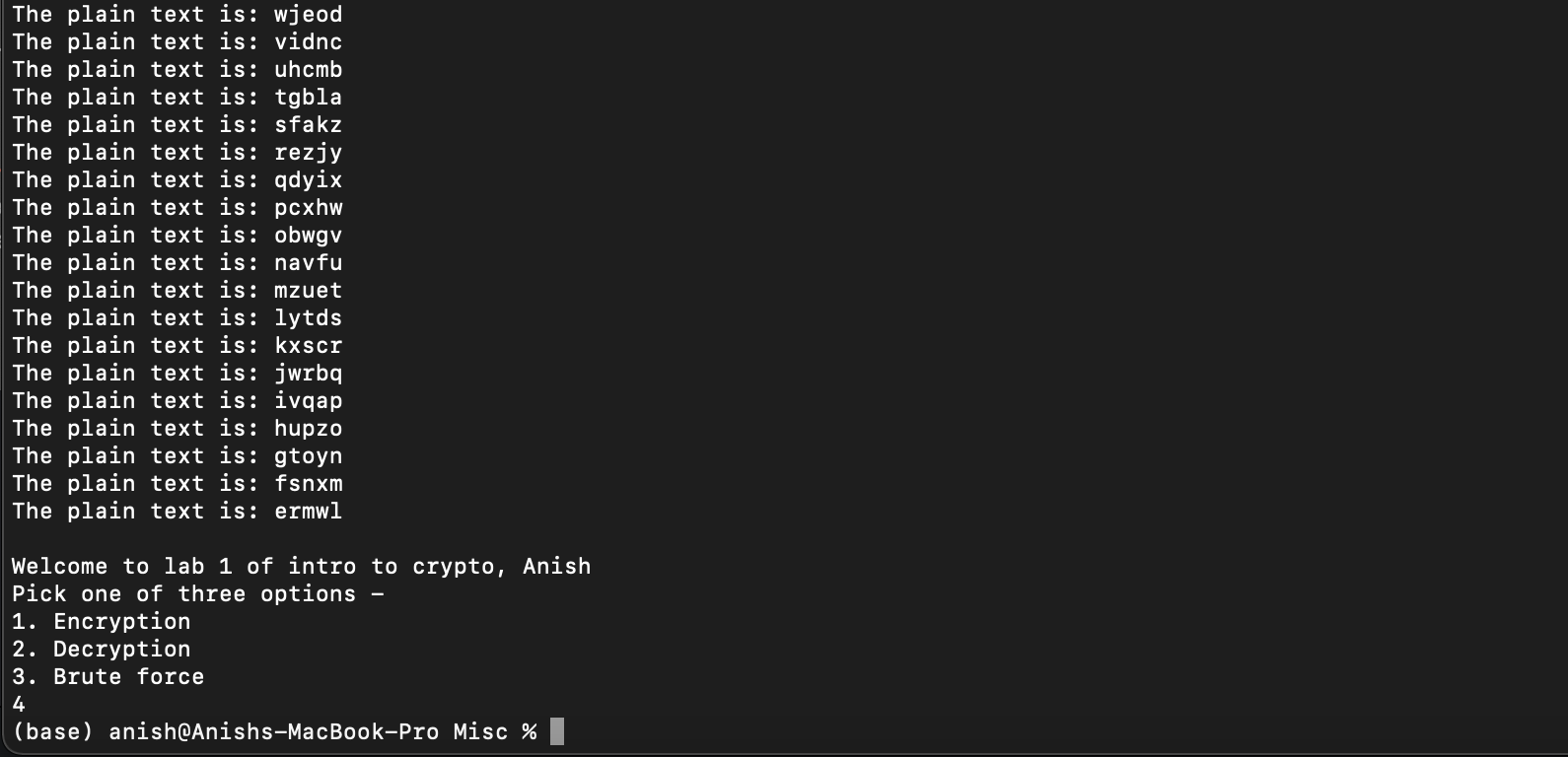
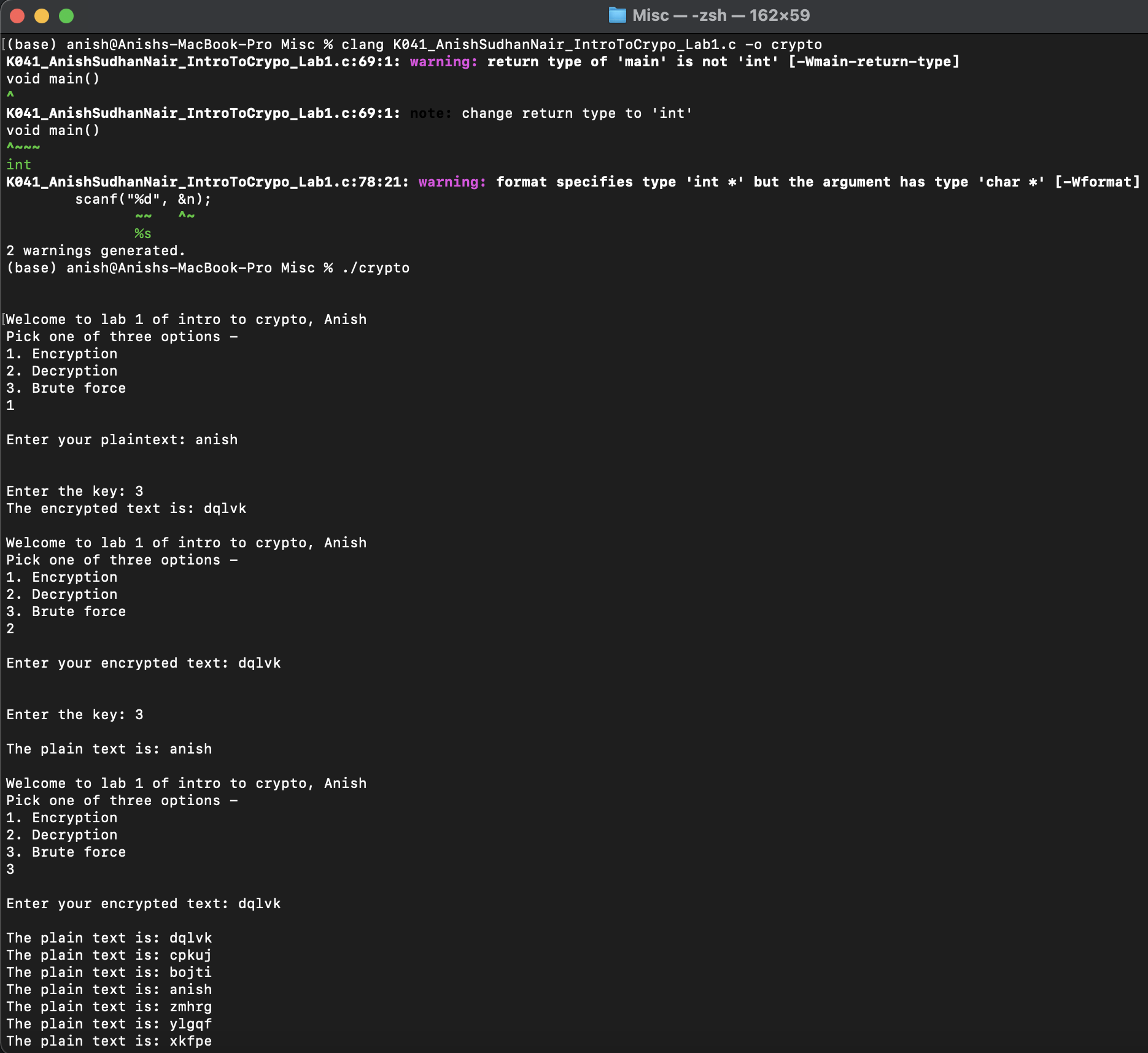
Compiler: clang/ZSH

Editor: XCode





Output:



Questions:

1. What are the goals of cryptography?

The primary goal of cryptography is to facilitate secure communication that remains private between the concerned parties i.e., the sender and the receiver and is unable to be understood by any authorised third party.

2.Explain following terms wrt cryptography.

a. Plain text: This is any text that can be understood by humans in the native human alphabet and doesn’t need to “decoded” in order to be comprehensible. This text is encoded using encryption techniques to derive encoded messages.

b. Cipher text: This is the encoded or encrypted text that needs to be decoded with the help of a particular key or technique known only to the sender and receiver in order to comprehend the message in normal alphabet.

c. Cipher: This is the technique or method of encryption/decryption comprising of algorithms and software that encodes a plain text message into cipher text.

d. Encryption: It is the process by which a plain text is encoded or converted into a cipher text(encrypted incomprehensible text) with the help of a cipher and the relevant key.

e. Decryption: It is the process by which the relevant cipher text is decoded or converted back to plain text with the help of the appropriate cipher and the key.

f. Key: It is a secret code or parameter employed by the relevant cipher to encode/decode a message. Keys are usually kept private to only the sender and receiver to ensure privacy of communication. In systems like RSA, which have a public key-private key system, the private key is always kept hidden.

g. Key space: It is the sample space or complete set of all possible keys for a particular cipher (or algorithm) that may be used for encryption/decryption.

3.What is brute force attack?

A brute force attack also known as an exhaustive key search in cryptographic contexts, is when every key or possible value/passkey for a given cipher(encryption) or authentication is tried sequentially one after the other. It is an attack that rests on guesswork and mathematical probability, trying all combinations until the right key/passkey is found.

4. Explain statistical analysis attack.

Statistical analysis attacks also known as frequency analysis is an integral part of cryptanalysis used against classical ciphers. It is executed by tabulating the frequency of characters appearing in a cipher text or encoded message and comparing it against the frequency tables of the relevant alphabet of the plain text. By comparing the frequencies of appearance of a character in an alphabet’s literature, corresponding assumptions are drawn between the tables and the key is figured out so.