Roll Number:- 2105048
Name:-Manav Jain
Date:- 26/07/2023

Lab Assignment No:-2

Aim:- Cryptanalysis or decoding of polyalphabetic ciphers:Playfair,Vigenere Cipher.

Lab Outcome Attained :- LO1

Theory:-

How vigenere cipher works?(with eg)

A technique for encrypting and decrypting messages is the Vigenere Cipher. It is a polyalphabetic substitution cipher, which implies that it encrypts the plaintext using a variety of cipher alphabets.

A keyword, generally a word or phrase, serves as the foundation for encryption in the Vigenere Cipher. To match the length of the plaintext message, the keyword is repeated. The shift value for each letter in the keyword is then calculated for each corresponding letter in the plaintext.

To encrypt a message, each letter of the plaintext is shifted by the corresponding letter in the keyword. Here the plaintext is divided into group of n characters each where n is length of key used for encryption . For Eg:-

Plaintext :- hello world

Key:- vig

Plain text will be divided as follows and mapped with key given accordingly :- (in group of 3)

Hel low orl d

Vig vig vig v

Then **(p+c)%26** formula is applied and letter corresponding to it is encoded character

Where , **p:- number corresponding to character in plain text starting from zero , c:-number corresponding to character present in key starting from zero**

So applying above text we get **cipher text** as:- **cmrgwcjzry**

Explain in brief how Kasiki test is used to break vigenere cipher?

A cryptanalysis technique for cracking the Vigenere cipher is the Kasiski test. It operates by scanning the ciphertext for repeating character patterns. If a character sequence is found to be repeated, the interval between the sequence's occurrences is most likely to be a multiple of the keyword's length.

Consider the case where the ciphertext comprises the letters "ABCABC". The interval between each occurrence of the sequence will be 3, 6, 9, 12, etc. if the keyword is 3 characters long. The gap between each occurrence of the sequence will be 4, 8, 12, 16, etc.

By finding the distances between repeated sequences in the ciphertext, the cryptanalyst can narrow down the possible values of the keyword length. Once the keyword length is known, the cryptanalyst can then use other methods to break the cipher.

Here is an example of how the Kasiski test can be used to break a Vigenere cipher:

Ciphertext:

ABCDEFGH

HIJKLMNOPQRSTUVWXYZ

The ciphertext's repetitive sequence is the first thing the cryptanalyst discovers. The letters "ABC" are repeated twice in this instance. The sequence's occurrences are separated by 12 steps.

The cryptanalyst can determine that the keyword length is three because the spacing between the sequence's repetitions is a multiple of three. The cryptanalyst can then employ additional techniques, like frequency analysis, to decipher the message.

The Kasiski test is a simple but effective method for breaking the Vigenère cipher. It is not foolproof, but it can be used to break ciphers that have been encrypted with short keywords.

How Playfair Cipher works ? (with eg)

The Playfair cipher is a symmetric encryption method that encrypts and decrypts communications using a 5x5 square letter-keyed matrix. Charles Wheatstone created it in 1854, and Lord Playfair later made it well-known. The primary goal of the Playfair cipher is to convert digraphs (pairs of letters) from plaintext into ciphertext using the encryption methods described below:

1)Before encrypting plain text if two consecutive letters in plaintext are same then insert bogus character ‘x’ in between them

2)If both characters in pair are in same row replace them by immediate right character from same row

3)f two characters in pair appear in same column replace them with immediate bottom character

4)If above two cases are not satisfied replace them by character in same row but in column of other character

Eg:-

Suppose we want to encrypt the message "HELLO" using the keyword "KEYWORD" (without repeating letters, and 'J' is combined with 'I').

Keyed Matrix Setup:

K E Y W O

R D A B C

F G H I L

M N P Q S

T U V X Z

The plaintext "HELLO" is divided into digraphs: "HE" and "LLO".

Encryption Rules:

"HE": H and E are in the same row, so we replace H with the letter to its right (E) and E with the letter to its right (F).

"LLO": L and O form a rectangle, so we replace L with the letter at the opposite corner of the rectangle (M) and O with the letter at the opposite corner of the rectangle (N).

Ciphertext:

The encrypted message is "FE MN NM."

To decrypt the ciphertext, the recipient would use the same keyed matrix and apply the decryption rules in reverse.

How cryptanalysis on playfair cipher can be done ?

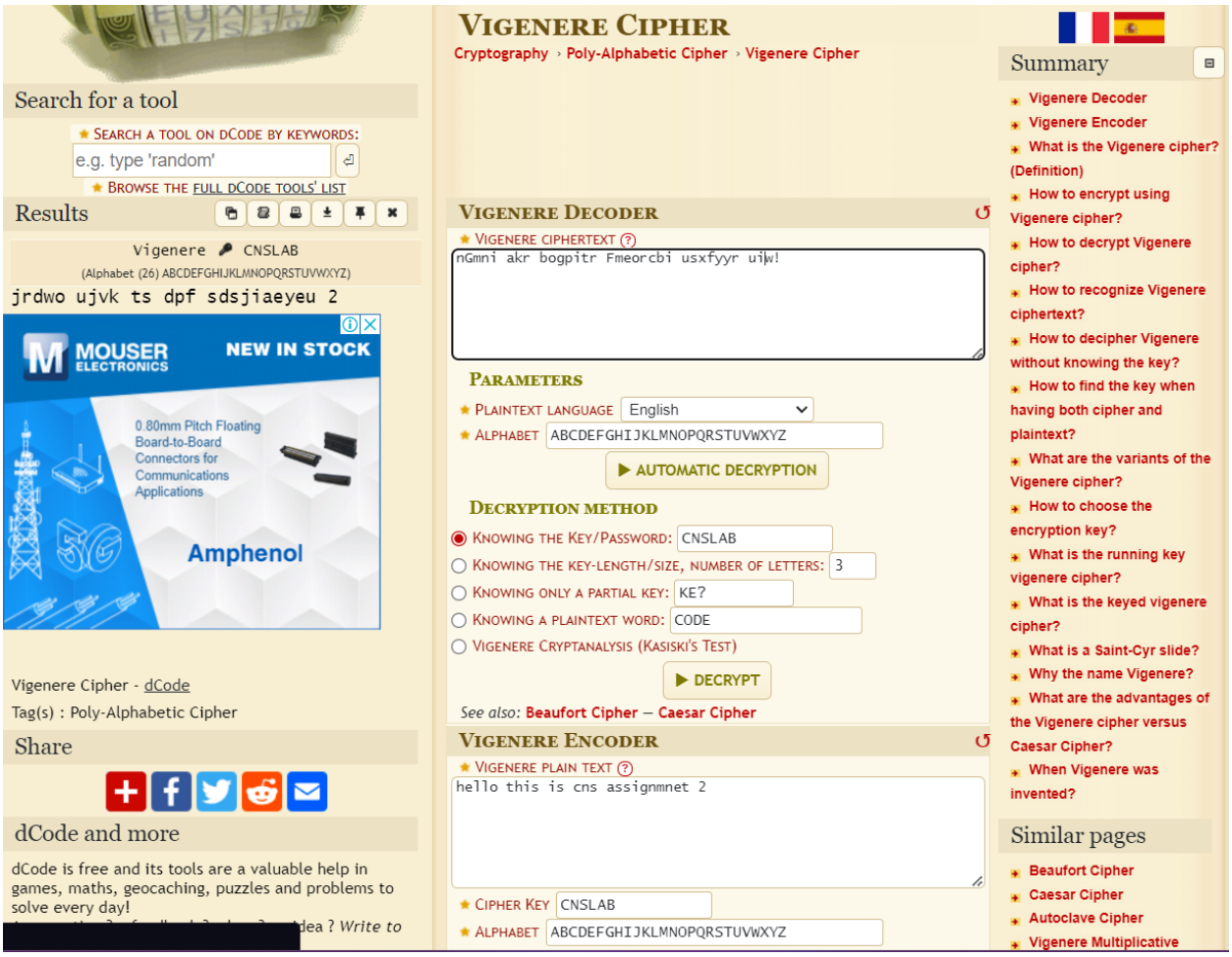
Cryptanalysis on the Playfair cipher involves attempting to break the encryption without knowing the key or the plaintext-ciphertext pair. Most common way is using **frequency analysis**

Cryptanalysts can perform frequency analysis on the ciphertext to identify patterns in the letter distribution. In English text, certain letters appear more frequently than others (e.g., 'E' is the most common letter). By analyzing the frequency of letters in the ciphertext, they can make

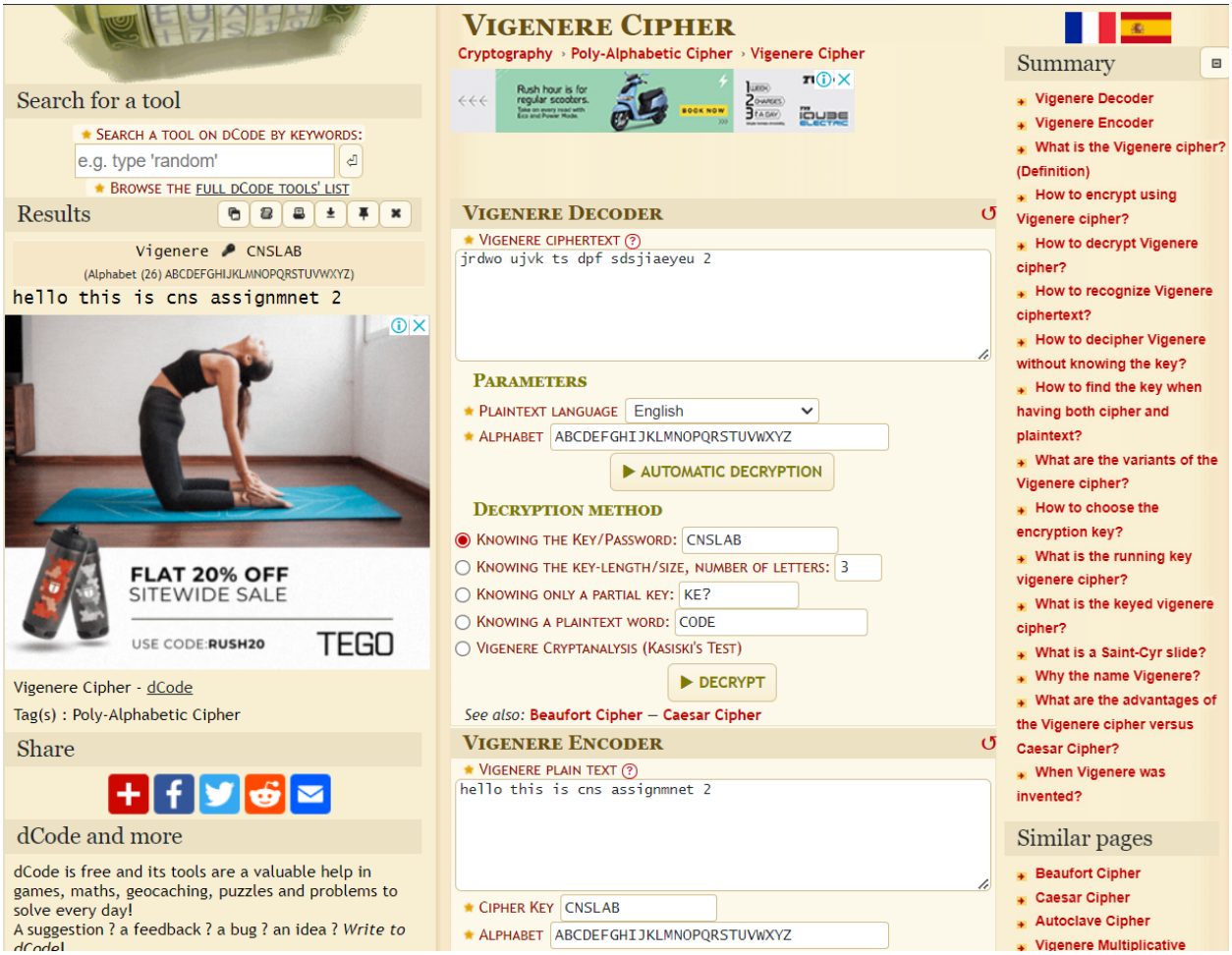
educated guesses about which letters might correspond to common letters in the English language.

Output Screenshot:-

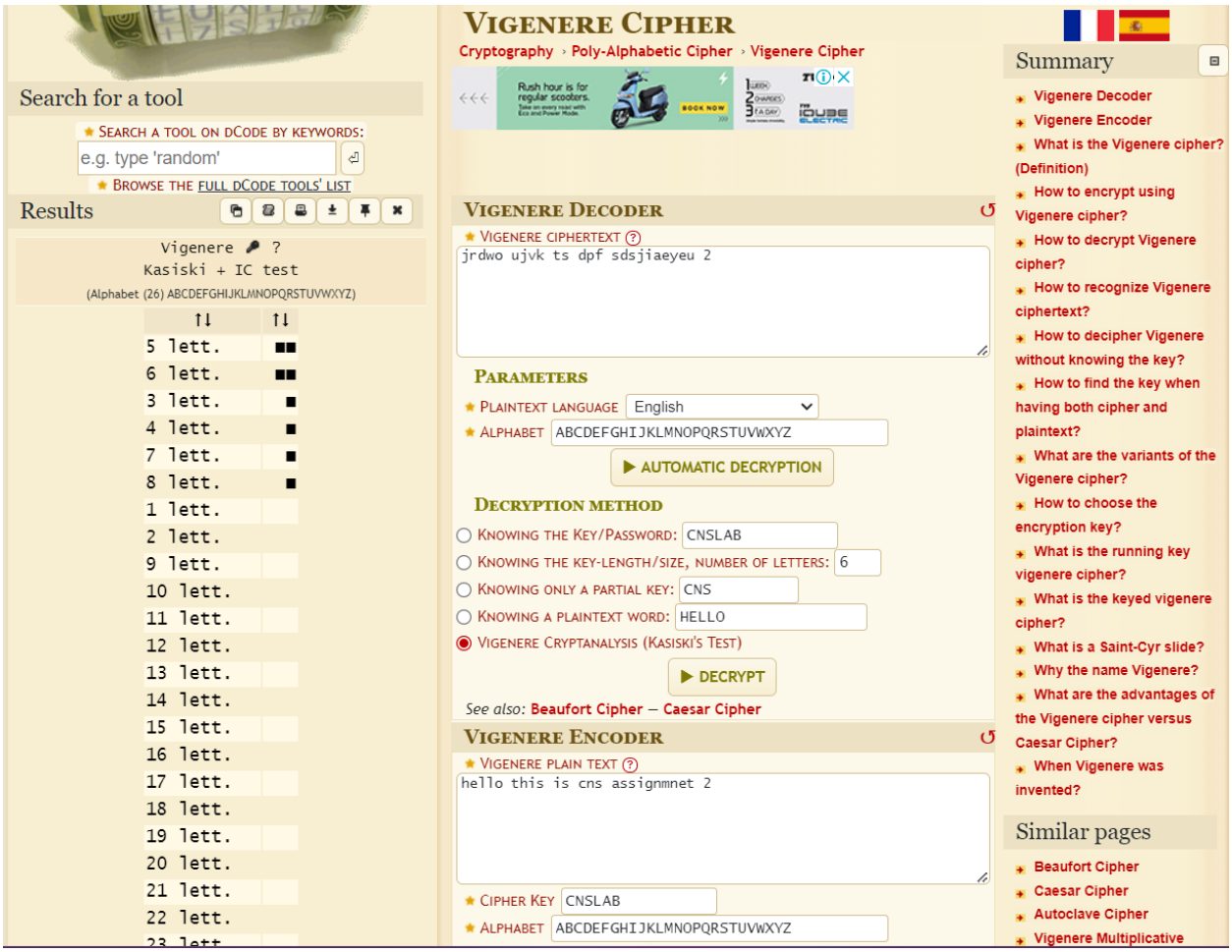
1)Vigenere cipher - encode plain text



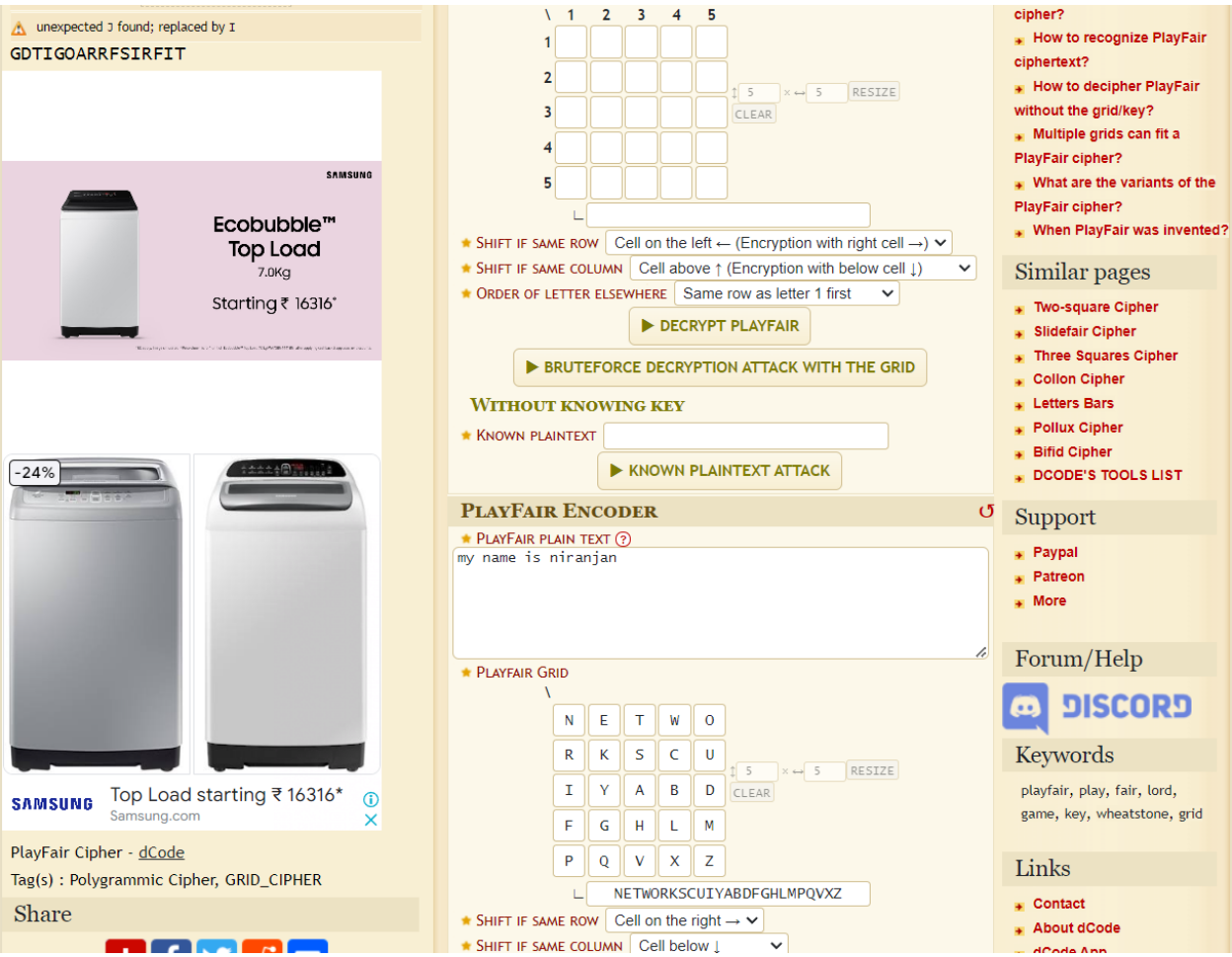
2)Vigenere cipher - decode cipher text



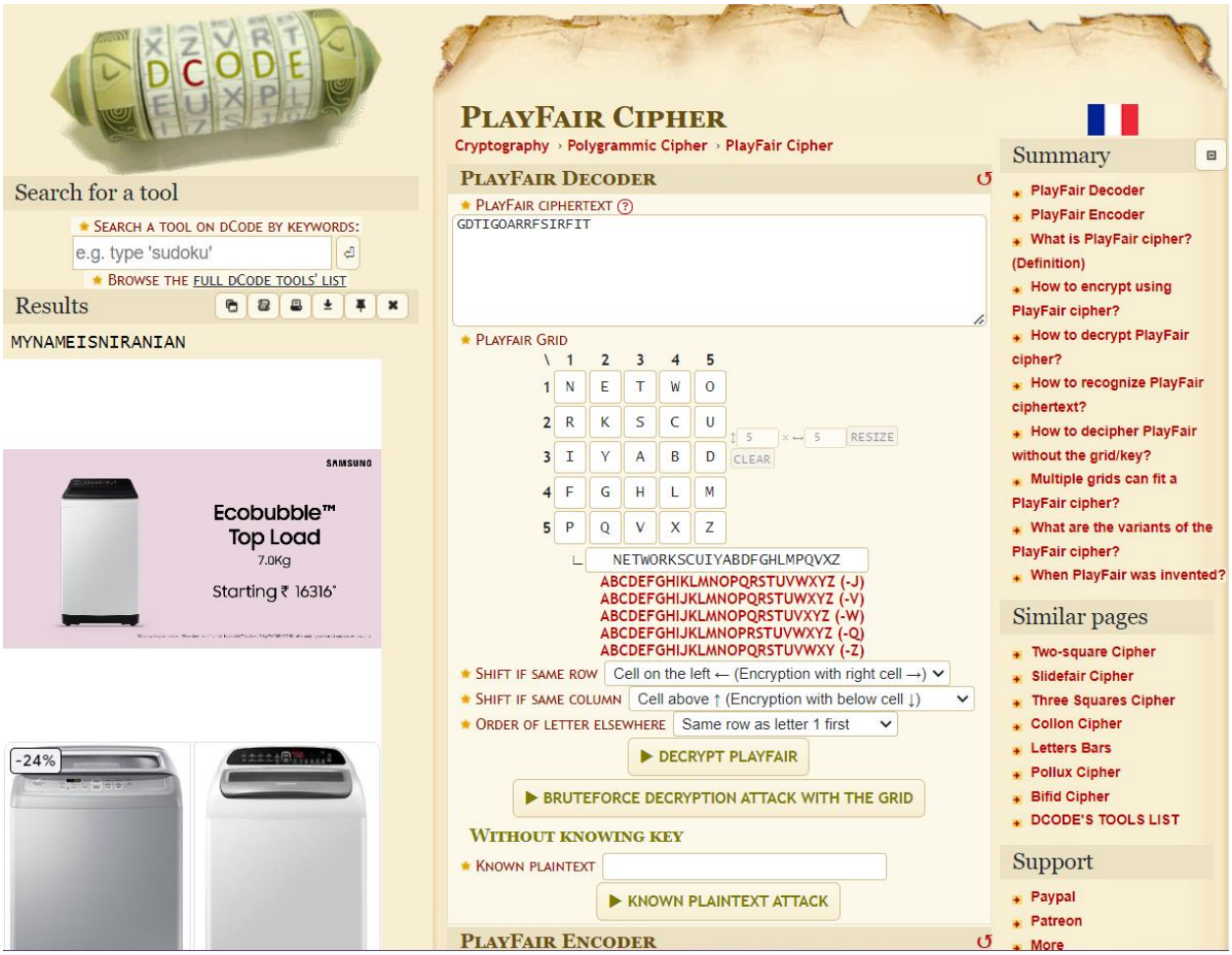
3)Vigenere Cipher - Kasiki test



4)Playfair cipher (key - networksecurity) - encode



5)Playfair cipher - decode



Conclusion:-

Successfully implemented cryptanalysis of vigenere cipher as well as playfair cipher and also encoded plain text , learnt in detail about cryptanalysis ,encoding in vigenere , playfair cipher