Roll No: 09
Name: Shreya Bagade
Date: 28/07/2023

LAB ASSIGNMENT NO:02

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

Lab Outcome Attained: Illustrate symmetric cryptography by implementingclassical ciphers.

Theory:

➢ How Vigenere cipher works?

The Vigenere cipher is a classical encryption technique that employs a simple form of polyalphabetic substitution to encrypt messages. Here's how it works:

1. Key Setup: Both the sender and receiver agree upon a keyword or phrase, known as the "key." The key is repeated to match the length of the message to be encrypted, for example, "KEY". So, if the message is "HELLO", the repeated key would be "KEYKE".
2. Mapping Letters to Numbers: Assign each letter of the key and the message a numerical value according to their position in the alphabet (e.g., A=0, B=1, ..., Z=25).
3. Encryption Process:
    - For each letter in the message, find the corresponding letter in the key.
    - Add the numerical values of the message letter and key letter.
    - Take the result modulo 26 to get the encrypted letter's numerical value.
    - Convert the numerical value back to a letter based on the alphabet mapping.
    - Example- So, for message “HELLO”, take the first letter of the message ("H") and the corresponding letter from the key ("K"). Add their numerical values (7 + 10 = 17).

      Convert the result (17) back to a letter (R).

      Repeat this process for each letter in the message.

Message: H E L L O

Key: K E Y K E

Encrypted: R G V T W

4. Decryption Process:
    - Similar to encryption, for each letter in the encrypted message, find the corresponding letter in the key.
    - Subtract the numerical value of the key letter from the encrypted message letter.
    - If the result is negative, add 26 to it to get a positive value.
    - Convert the result modulo 26 to get the decrypted letter's numerical value.
    - Convert the numerical value back to a letter based on the alphabet mapping.
    - Example: Take the first letter of the encrypted message ("R") and the corresponding letter from the key ("K").

      Subtract the numerical value of the key letter (10) from the encrypted letter's numerical value (17).

      Since 17 - 10 = 7, convert the result (7) back to a letter (H).

      Repeat this process for each letter in the encrypted message.

      Encrypted: R G V T W

      Key: K E Y K E

      Decrypted: H E L L O

- **<u>Explain in brief how Kasiski Test is used to break the vigenere cipher</u>?**

The Kasiski test is a method used to break the Vigenère cipher by exploiting repeated patterns in the encrypted text. Here's how it works in brief:

1. Identifying Repeated Patterns: When a Vigenère cipher is used with a repeating keyword, the same sequence of key letters will be used to encrypt identical parts of the plaintext. This can lead to repeated

patterns in the encrypted text.

2. Finding Key Length Guesses: The Kasiski test involves finding repeated sequences of letters in the encrypted text. By measuring the distance between these repetitions, one can make educated guesses about the length of the repeating keyword.
3. Calculating Probable Key Length: Calculate the greatest common divisor (GCD) of the distances between repeated sequences. This GCD could provide an estimate of the length of the keyword.
4. Dividing the Cipher Text: Divide the encrypted text into sections, each with a length equal to the guessed keyword length. This separates the text encrypted with the same letter of the keyword.
5. Frequency Analysis: Treat each section as if it's encrypted using a simple Caesar cipher. Analyze the frequency distribution of letters in each section to determine the likely shift used for each section.
6. Recovering the Keyword: After determining the shifts for each section, the shifts can be used to reconstruct parts of the keyword. Combining these parts can lead to partial or full recovery of the keyword.
7. Decrypting the Message: With the keyword known, the Vigenère cipher can be decrypted using the same process as encryption but in reverse. The keyword's letters are subtracted from the corresponding letters in the encrypted message.

- **How Playfair cipher works?**

The Playfair cipher is a substitution cipher that uses a 5x5 matrix of letters to encrypt digraphs (pairs of two letters) from the plaintext. Here's a brief explanation of how it works, along with an example:

Encryption Process: -

Key Setup: Choose a keyword and remove duplicate letters, then fill in the remaining letters of the alphabet to create a 5x5 matrix (Playfair square). For example, using the keyword "KEYWORD".

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

Roll No: 09
Name: Shreya Bagade
Date: 28/07/2023

Message Preparation: Divide the plaintext into digraphs (pairs of two letters), and handle special cases (e.g., repeated letters in a digraph). If a digraph has an odd number of letters, add a filler letter (e.g., 'X').

Encrypting Digraphs:
For each digraph:

1. If the letters are in the same row, replace them with the letters to their right (cyclically).
2. If the letters are in the same column, replace them with the letters below them (cyclically).
3. If the letters are in different rows and columns, take the letters at the intersection of their respective rows.

Example:
Message: "HELLO"
Key: "KEYWORD"

Playfair Square:
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
Digraphs: "HE", "LX", "LO"
Encrypted Digraphs: "BY", "MX", "LP"

Decryption Process:

Key Setup: Use the same keyword to recreate the Playfair square.
Decrypting Digraphs:
For each encrypted digraph:
If the letters are in the same row, replace them with the letters to their left (cyclically).
If the letters are in the same column, replace them with the letters above them (cyclically).
If the letters are in different rows and columns, take the letters at the

intersection of their respective rows.
Example (Decryption):

Encrypted Digraphs: "BY", "MX", "LP"
Decrypted Digraphs: "HE", "LX", "LO"

- **How cryptanalysis of Playfair can be done?**

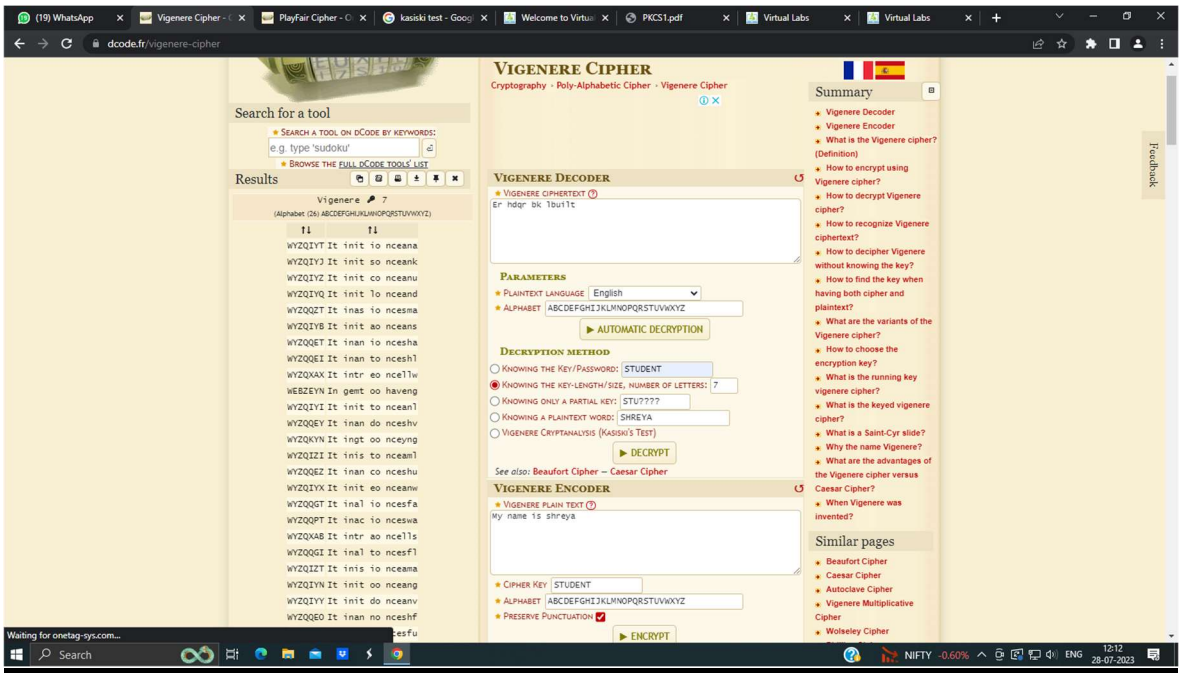
Cryptanalysis of the Playfair cipher involves attempting to break the encryption scheme to reveal the original plaintext without knowing the key. Here's a brief overview of some common techniques used to cryptanalyze the Playfair cipher:

1. Frequency Analysis: Since Playfair operates on digraphs (pairs of letters), the frequency analysis becomes more complex. However, repeated digraphs or common English digraphs can still provide hints about the key. For example, if a specific digraph appears frequently in the ciphertext, it could correspond to a common English digraph, helping to identify potential substitutions.
2. Known-Plaintext Attack: If an attacker has access to some plaintext-ciphertext pairs encrypted using the same key, they can analyze the pairs to discover patterns in the key. This could lead to partial or full recovery of the key and the ability to decrypt other messages.
3. Brute Force Attack: The Playfair cipher key space is relatively small compared to modern encryption methods, making brute force attacks feasible. An attacker could systematically try all possible keys and evaluate the decrypted text for meaningful patterns.
4. Digraph Analysis: Examining the encrypted text for repeated digraphs or common digraphs can provide insights into the structure of the Playfair matrix. For instance, repeated encrypted digraphs might indicate that the same plaintext digraph was encrypted twice using different keys, allowing the attacker to deduce the key.
5. Known Key Length Attack: If the attacker knows the length of the keyword, they can focus on finding the actual keyword itself. By analyzing the frequencies of letters in the ciphertext, they might identify common words or digraphs encrypted with the same key.
6. Short Message Vulnerability: The Playfair cipher's security is

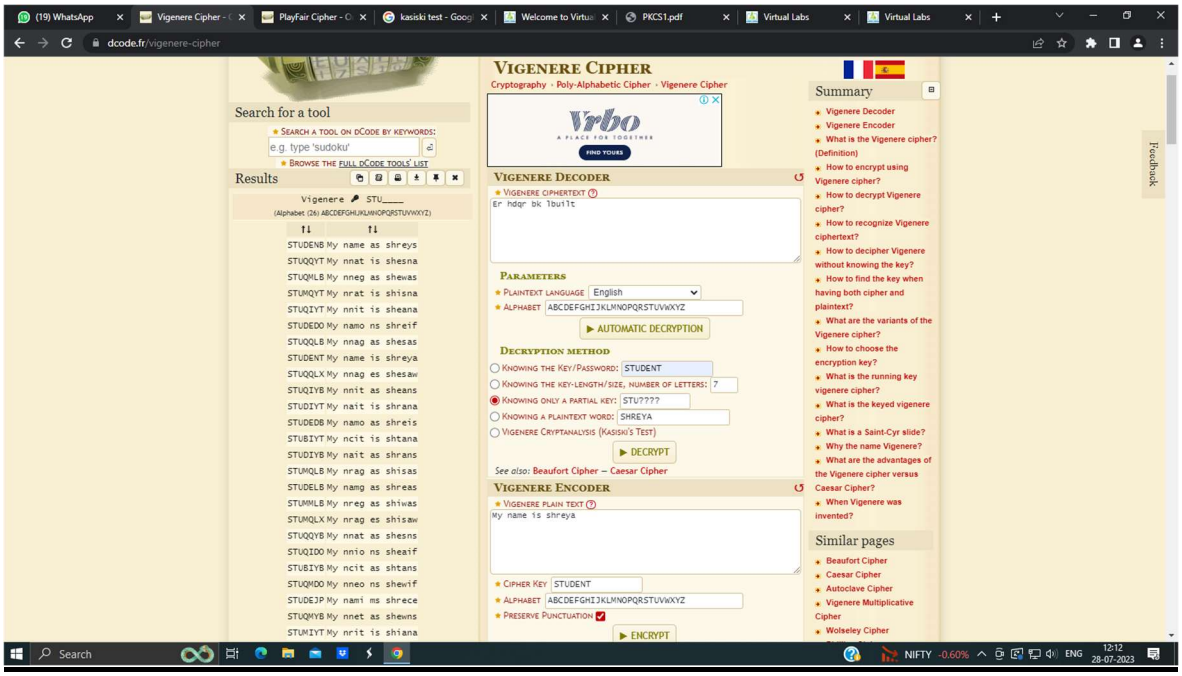
weakened when used to encrypt very short messages. With fewer digraphs, the attacker's task of analyzing patterns and frequencies becomes easier.

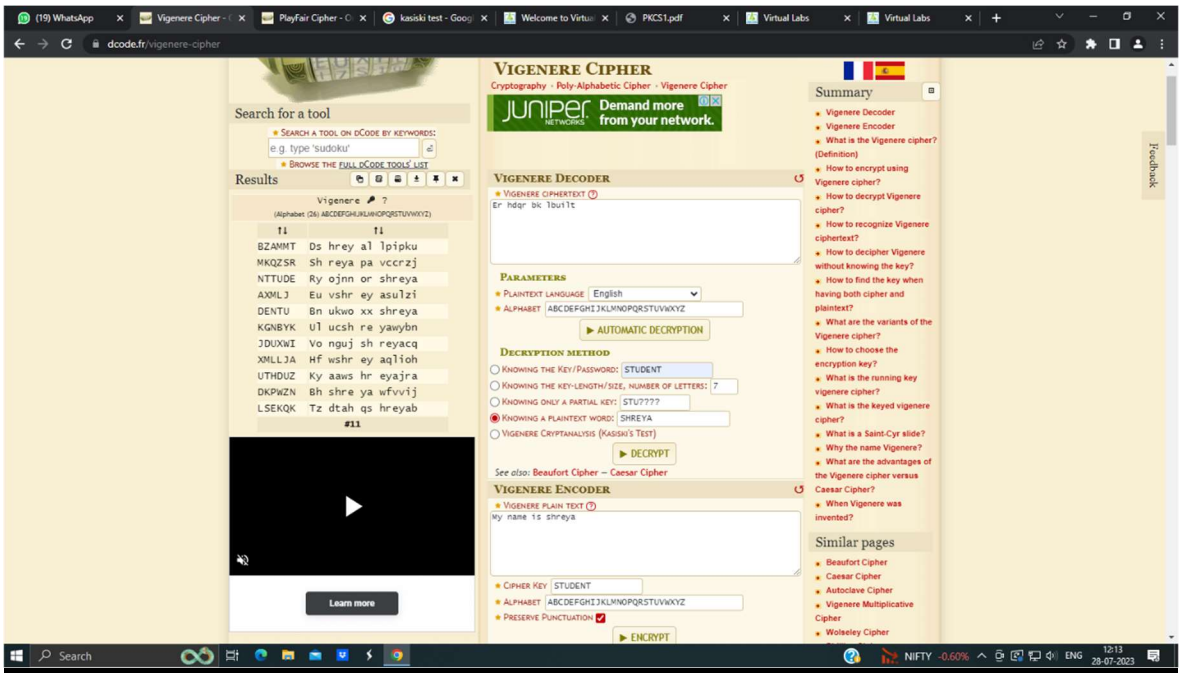
7. Key Enumeration: By trying all possible keywords and creating corresponding Playfair matrices, the attacker could compare the decrypted text with known English words or phrases to identify the correct key.

Output Screenshots:

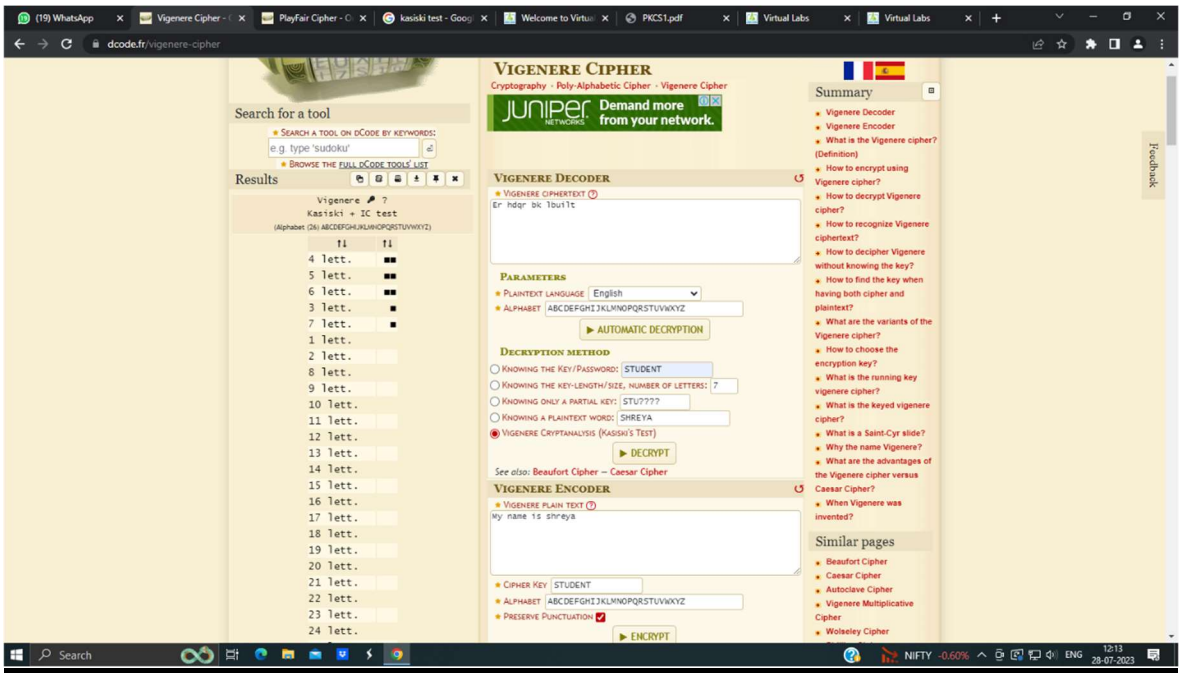


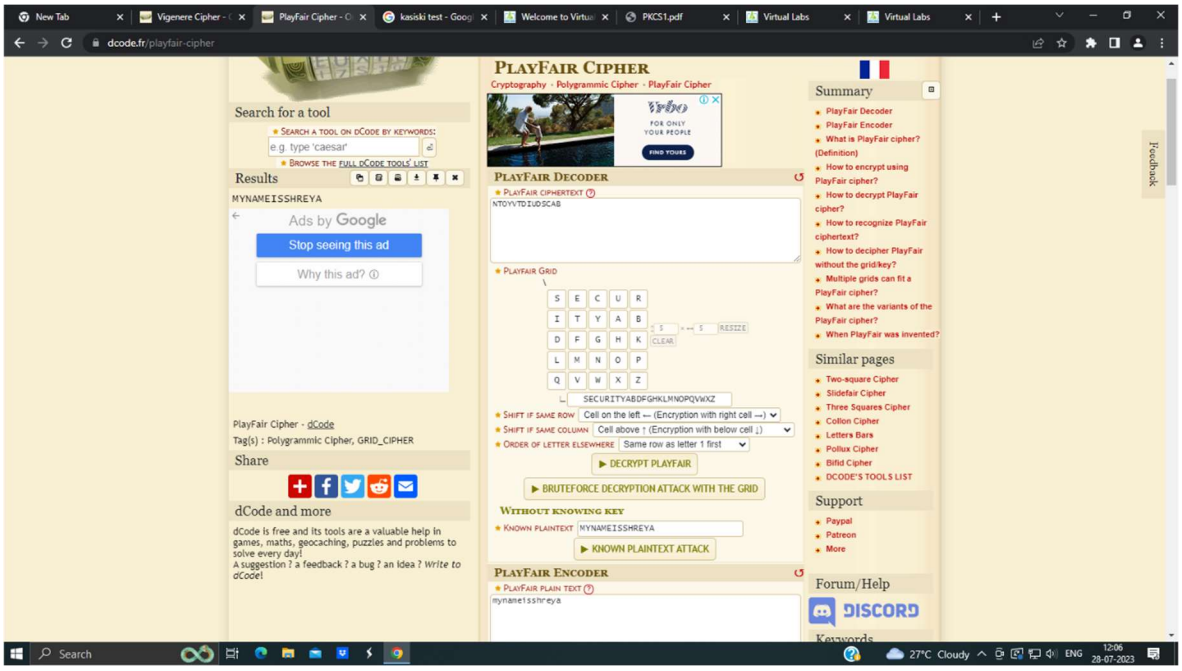
Roll No: 09
Name: Shreya Bagade
Date: 28/07/2023



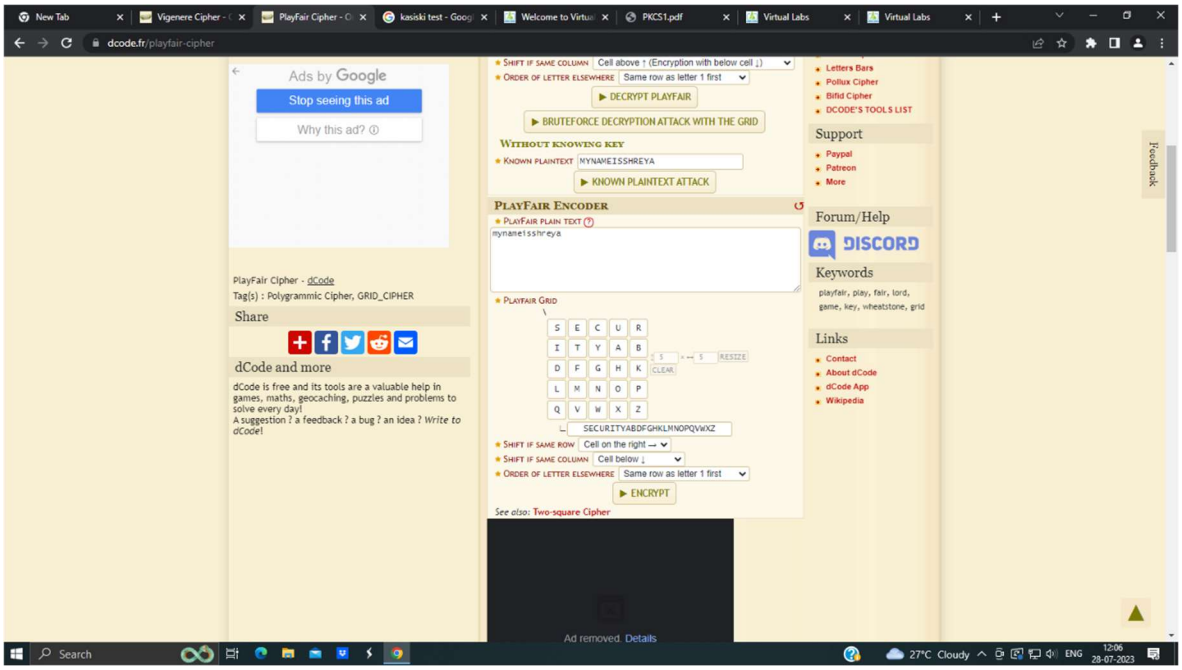


Roll No: 09
Name: Shreya Bagade
Date: 28/07/2023





Roll No: 09
Name: Shreya Bagade
Date: 28/07/2023



Conclusion: We learnt about Vigenere cipher and Playfair cipher and their fundamentals in terms of security. The Vigenere cipher demonstrated its ability to enhance security through polyalphabetic substitution, resisting simple frequency analysis.On the other hand, the Playfair cipher showcased the effectiveness of digraph substitution in introducing complexity and adding security layers to encryption.