Name: Aman Singh
Batch : T23 Roll no :128

Experiment No 2

Aim : Implementation and analysis of Cryptanalysis or decoding of polyalphabetic ciphers:

Playfair, Vigenere cipher.

Lab Outcome :

LO1 : Illustrate symmetric cryptography by implementing classical ciphers.

Theory :

1. How vigenere cipher works (with eg)?

The Vigenère cipher is a classical encryption technique that builds upon the simple Caesar cipher by introducing a keyword that determines the shifting pattern for each letter. This method of encryption offers a more robust form of security compared to the monoalphabetic substitution techniques.

How the Vigenère Cipher Works:

1. Choosing a Keyword:
Start by selecting a keyword, which can be any word or phrase. For instance, consider using the keyword "KEY" for this explanation.

2. Matching the Keyword Length:
Repeat the keyword to match the length of the plaintext you want to encrypt. If the plaintext is longer than the keyword, the keyword will be repeated as needed. Let's say we want to encrypt the word "HELLO."

3. Converting to Numerical Values:
Convert both the keyword and the plaintext into numerical values based on their positions in the alphabet. A=0, B=1, C=2, and so on. For our example, "HELLO" becomes 7 4 11 11 14.

4. Shifting with the Keyword:
Starting with the first letter of the keyword and the corresponding letter in the plaintext, add their numerical values together (mod 26) to get the encrypted letter. In our case:
- Letter "H" (numerical value 7) + Letter "K" (numerical value 10) = 17, which corresponds to the letter "R."
Continue this process for each letter, cycling through the keyword as necessary.

5. Converting Back to Letters:

Name: Aman Singh
Batch : T23 Roll no :128

Convert the numerical values of the encrypted letters back to their corresponding letters in the alphabet. The encrypted version of "HELLO" with the keyword "KEY" is "RIFNP."

Example:

- Plaintext: HELLO
- Keyword: KEY
- Numerical Values: 7 4 11 11 14
- Shifted Values: (7 + 10) (4 + 4) (11 + 24) (11 + 4) (14 + 10)
- Encrypted Values: 17 8 9 15 24
- Encrypted Text: RIOPI

Advantages and Weaknesses:

The Vigenère cipher's main advantage lies in its utilization of a keyword, introducing variability and making frequency analysis less effective. It can also handle more characters without becoming overly predictable. However, its security can still be compromised if the keyword is short or easily guessed.

2. Kasiski Test: Breaking the Vigenère Cipher:

The Kasiski Test is a cryptanalysis technique used to decipher the Vigenère cipher by determining the length of the keyword used for encryption. This method exploits the patterns that emerge when the same keyword segment encrypts multiple occurrences of the same plaintext segment, resulting in repeated ciphertext segments. By identifying the distances between these repetitions, cryptanalysts can deduce potential keyword lengths and subsequently break the encryption.

Steps of the Kasiski Test:

1. Identifying Repeated Ciphertext Segments:
Begin by examining the ciphertext for recurring segments. Due to the nature of the Vigenère cipher, if the same keyword segment is used to encrypt the same plaintext segment, the resulting ciphertext segments will match.

2. Calculating Distances:
Once you've identified the repeated ciphertext segments, calculate the distances between them in terms of the number of letters. These distances often correlate to multiples of the keyword length.

3. Finding Common Factors:

Name: Aman Singh
Batch : T23 Roll no :128

Look for common factors among the distances you've calculated. If the same keyword length was used multiple times, it would result in similar distances. By identifying common factors, you narrow down the possible lengths of the keyword.

4. Testing Potential Keyword Lengths:
With the potential keyword lengths in mind, you can begin testing them to see if they reveal any patterns. If a guessed keyword length is correct, it would result in a repeating pattern in the decrypted text, indicating that you're on the right track.

5. Deciphering the Text:
Once you've determined the keyword length, you can begin deciphering the text as if it's a set of simple Caesar ciphers. Divide the ciphertext into columns based on the keyword length, and decrypt each column using frequency analysis.

Example:

Let's say we have the following repeated segments in the ciphertext:
```
Ciphertext: GATKIVWLGGXKD
Segments: GAT KIVWLGG XKD
Distances: 4 7
```
The distances between the repeated segments are 4 and 7. The common factor between these distances is 1, suggesting that the keyword length could be 1 or a factor of the key length.

3. How Playfair Cipher works?

The Playfair cipher is a digraph substitution cipher that enhances security by encrypting pairs of letters rather than individual ones. This technique uses a key matrix, often a 5x5 grid, to transform plaintext letters into ciphertext digraphs. While it might seem intricate, understanding its operation can provide insights into its encryption process.

How Playfair Cipher Works:

1. Key Matrix Creation:
Begin by creating a key matrix, typically a 5x5 grid, containing unique letters. For example, consider the keyword "KEYWORD" and construct the matrix:

```
K E Y W O
R D A B C
F G H I L
M N P Q S
```

Name: Aman Singh
Batch : T23 Roll no :128

T U V X Z
```

2. Handling Repeated Letters and Missing Letters:
Since the key matrix requires distinct letters, some letters may be omitted, often a combination like "I" and "J." When encrypting, treat these as the same letter.

3. Breaking the Plaintext into Digraphs:
Divide the plaintext into pairs of letters (digraphs). For instance, "HELLO" becomes "HE" and "LL" with an added filler letter if needed. If the plaintext has an odd number of letters, append an extra letter (like "X") at the end.

4. Applying the Rules:
For each digraph:
- If both letters are in the same row, replace them with the letters to their right (looping to the leftmost if at the end).
- If both letters are in the same column, replace them with the letters below (looping to the top if at the bottom).
- If neither of the above conditions holds, form a rectangle with the two letters and replace each letter with the opposite corner's letter.

Example of Playfair Encryption:

- Key Matrix:
```
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
```
- Plaintext: "HELLO" - Digraphs: "HE" and "LL" - Encryption Steps:
- "HE" forms a rectangle. Replace "H" with "L" and "E" with "O" to get "LO."
- "LL" is in the same row. Replace "L" with "M" and "L" with "N" to get "MN."
- Ciphertext: "LOMN"

Advantages and Limitations:

The Playfair cipher offers better security than simple substitution ciphers. Breaking it requires more complex techniques like frequency analysis of digraphs. The use of a key matrix introduces an additional layer of complexity, making cryptanalysis more intricate.
```

Name: Aman Singh
Batch : T23 Roll no :128

4. Cryptanalysis of the Playfair Cipher .

Cryptanalysis is the art of deciphering encrypted messages without the key. The Playfair cipher, a digraph substitution technique, may seem secure, but it's not immune to skilled cryptanalysts. Breaking the Playfair cipher involves exploiting its weaknesses and patterns to reveal the original message.

Cryptanalysis Steps for Playfair Cipher:

1. Frequency Analysis:
Even though Playfair encrypts digraphs, frequency analysis still works. In English, certain letter pairs are more common than others. Analyze the frequency distribution of digraphs in the ciphertext and compare them with known frequencies in English. High-frequency digraphs in the ciphertext could correspond to common letter pairs in the plaintext.

2. Identifying Patterns:
Look for repeated digraphs or sequences in the ciphertext. These can reveal underlying patterns that correspond to specific plaintext words or phrases. Patterns might emerge due to repeated sections of the original message.

3. Exploiting Known Plaintext:
If you have a portion of the original plaintext (a known plaintext), you can use it to your advantage. Encrypt the known plaintext with different parts of the key matrix to see if the ciphertext matches portions of the encrypted message. This might give you insights into the key matrix's structure.

4. Brute Force Attack:
If the key matrix is not very large or complex, a brute force attack might be feasible. Generate all possible key matrices and use each one to decrypt the ciphertext. Compare the decrypted results with English words or phrases to determine the correct key matrix.

5. Trial and Error with Keyword Variations:
If you have a hint about the keyword, try variations of the keyword to see if they yield meaningful plaintext. Small changes to the keyword can drastically alter the key matrix, affecting the decryption outcome.

6. Choosing an Optimal Key Length:
The length of the keyword affects the key matrix's size. If you can deduce the keyword length, you can narrow down the potential key matrices to test.

7. Breaking the Key Matrix:
If you have enough ciphertext, you might be able to identify repeated or near-repeated digraphs. This could indicate that the same key matrix sections are encrypting different parts of the

message. By analyzing these overlapping sections, you might be able to reverse-engineer parts of the key matrix.

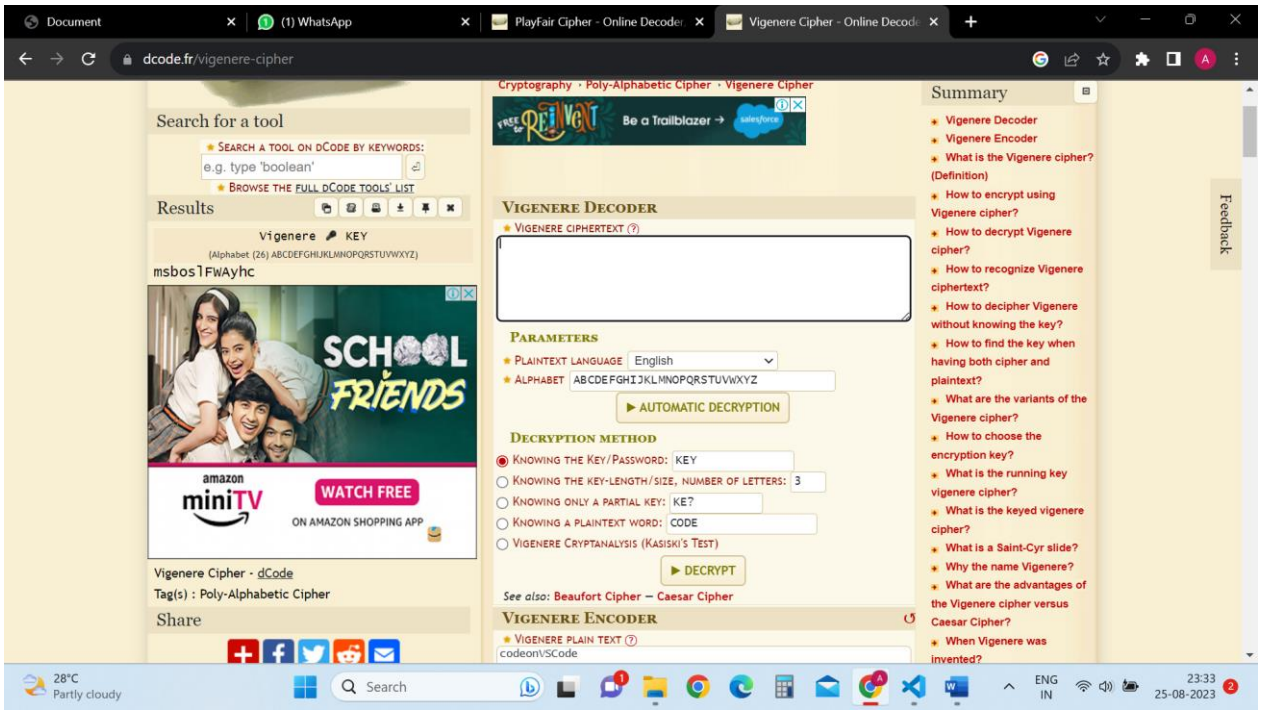
Example:

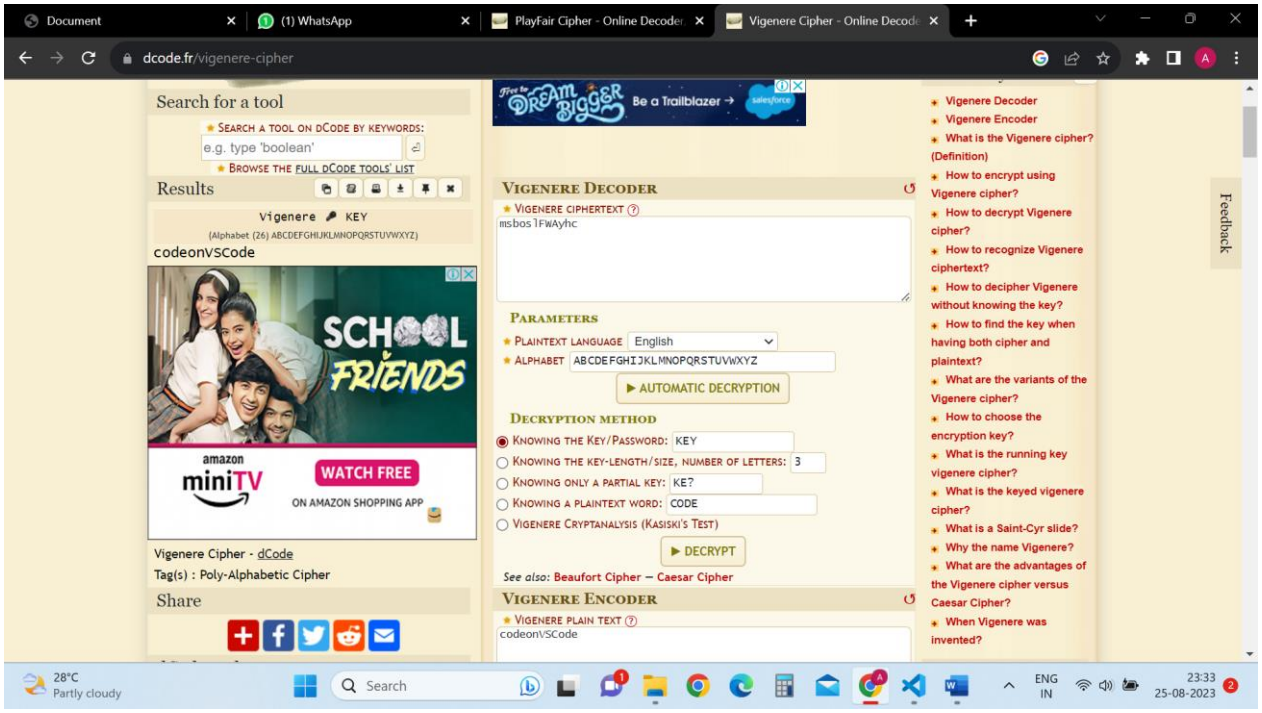
Suppose you have the ciphertext "SRIOAKDLA." Analyzing the frequency of digraphs, you notice that "SR" is repeated. If "SR" corresponds to "TH" in English, you've made progress in deciphering the message.

Output:

1. **Vigenere Cipher:**

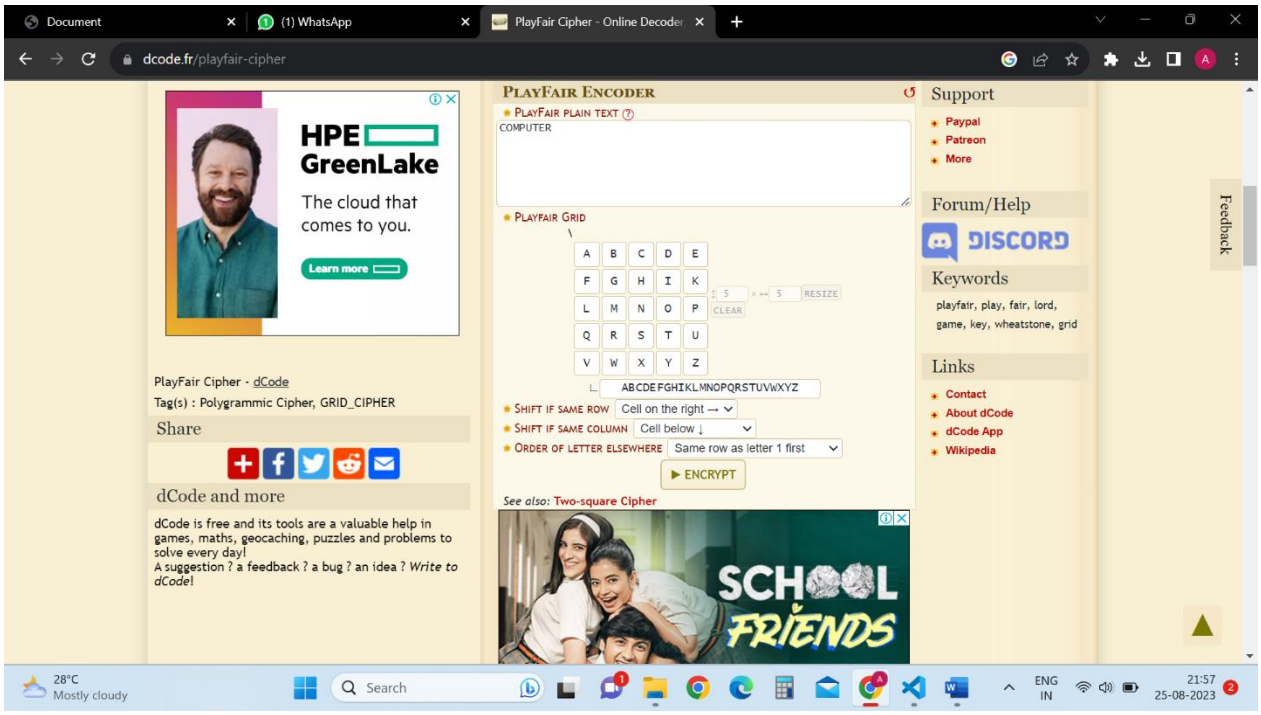
Name: Aman Singh
Batch : T23 Roll no :128

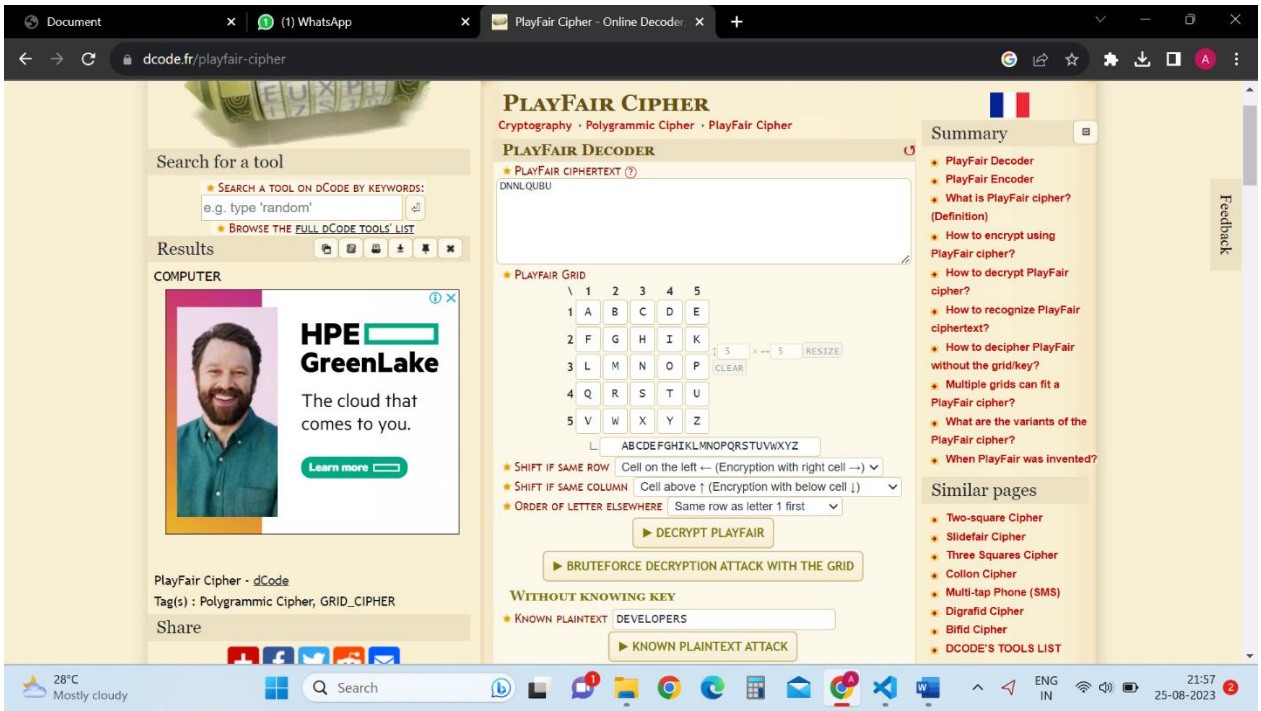




Name: Aman Singh
Batch : T23 Roll no :128

2. Playfair Cipher:





Name: Aman Singh
Batch : T23 Roll no :128

Conclusion:

Implemented and learned about Vigenère and Playfair Ciphers, explored the intricate steps of digital key generation and verification, successfully generated and verified digital signatures using software tools, and delved into the practical application of the RSA encryption scheme.