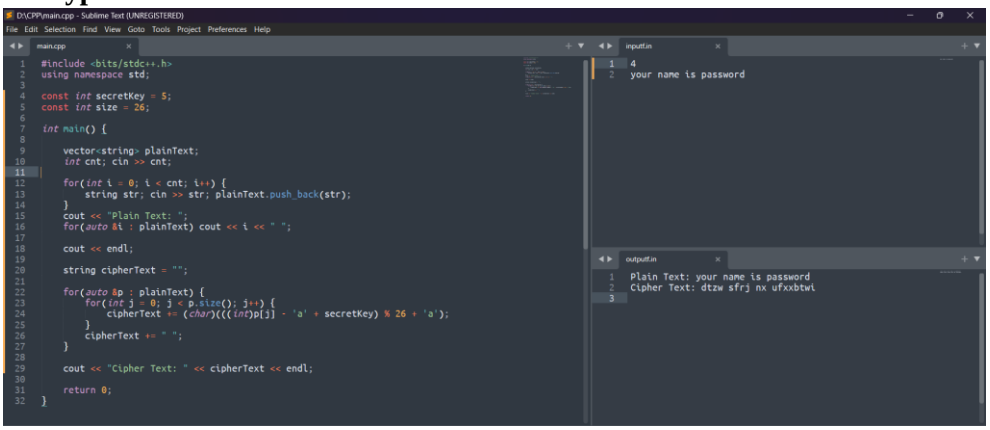
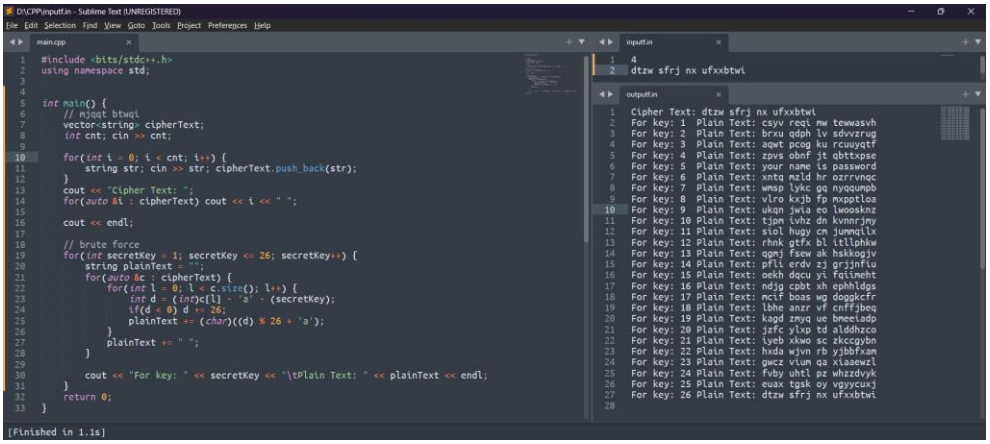
| | |
|---|---|
| **NAME** | Harsh Mukesh Jain |
| **UID** | 2021300048 |
| **DATE** | 21 - 08 - 2024 |

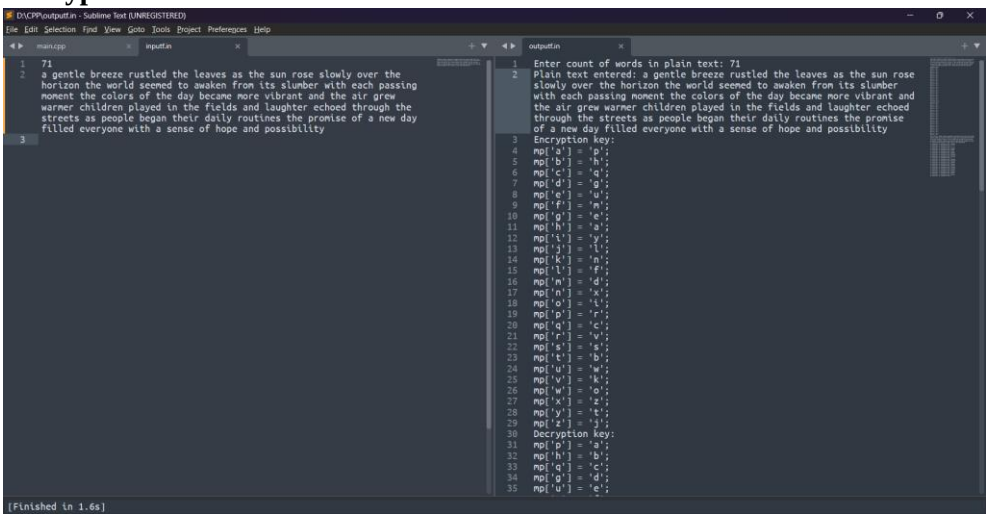
| **Experiment 1** | |
|---|---|
| **AIM:** | Implement different substitution techniques. |
| **PROBLEM DEFINITION:** | To implement all substitution encryption techniques namely Caesar Ciphers, Monoalphabetic Cipers, Playfair Cipher, Hill Cipher and Polyalphabetic Ciphers. Then, perform ethical hacking on all substitution encryption techniques. |
| **THEORY:** | **Caesar Cipher**<br>The Caesar cipher is one of the simplest and oldest encryption techniques. It is a type of substitution cipher where each letter in the plaintext is shifted a certain number of places down or up the alphabet. For example, with a shift of 3, 'A' would be replaced by 'D', 'B' would become 'E', and so on. The key in a Caesar cipher is the number of positions each letter is shifted. Despite its simplicity, the Caesar cipher is not secure against modern cryptographic attacks.<br>**Monoalphabetic Cipher**<br>A monoalphabetic cipher is a substitution cipher where each letter in the plaintext is replaced by another letter from the alphabet. Unlike the Caesar cipher, which uses a fixed shift, a monoalphabetic cipher can use a more complex substitution pattern. Each letter in the plaintext is consistently replaced by the same letter in the ciphertext. This type of cipher is more secure than the Caesar cipher but is still vulnerable to frequency analysis.<br>**Playfair Cipher**<br>The Playfair cipher is a digraph substitution cipher that encrypts pairs of letters (digraphs) instead of single letters. It uses a 5x5 matrix (for a 26-letter alphabet, 'I' and 'J' are often combined) filled with a keyword and then the remaining letters of the alphabet. The encryption process involves replacing each pair of letters in the plaintext with another pair according to specific |

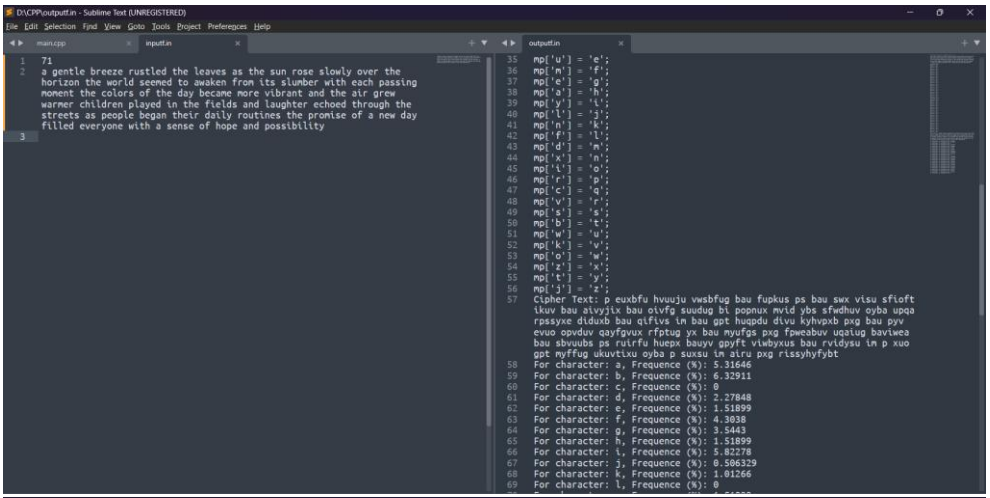
| | |
|---|---|
| | rules based on their positions in the matrix. The Playfair cipher is more secure than simple substitution ciphers but is still vulnerable to cryptanalysis.<br><br>**Hill Cipher**<br><br>The Hill cipher is a polygraphic substitution cipher that operates on blocks of letters rather than individual letters. It uses a matrix (usually 2x2 or 3x3) to encrypt the plaintext. Each block of letters is treated as a vector and multiplied by the encryption matrix modulo 26. The resulting vector is the ciphertext. The Hill cipher is more complex than simple substitution ciphers and provides better security, but it is still vulnerable to known-plaintext attacks.<br><br>**Polyalphabetic Cipher (Vigenère Cipher)**<br><br>The Vigenère cipher is a method of encrypting alphabetic text by using a simple form of polyalphabetic substitution. It uses a keyword to determine the shift for each letter in the plaintext. For example, if the keyword is "LEMON" and the plaintext is "ATTACKATDAWN", the first letter 'A' is shifted by 'L' (11 positions), the second letter 'T' is shifted by 'E' (4 positions), and so on. The Vigenère cipher is more secure than monoalphabetic ciphers because it uses multiple substitution alphabets, making frequency analysis more difficult. |
| **RESULT:** | **1. Caesar Cipher**<br><br>**Encryption:**<br>  <br><br><br>**Decryption:** |



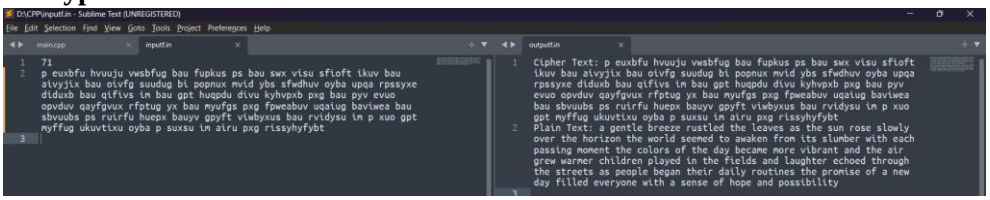

## 2. Monoalphabetic Substitution

## Encryption:

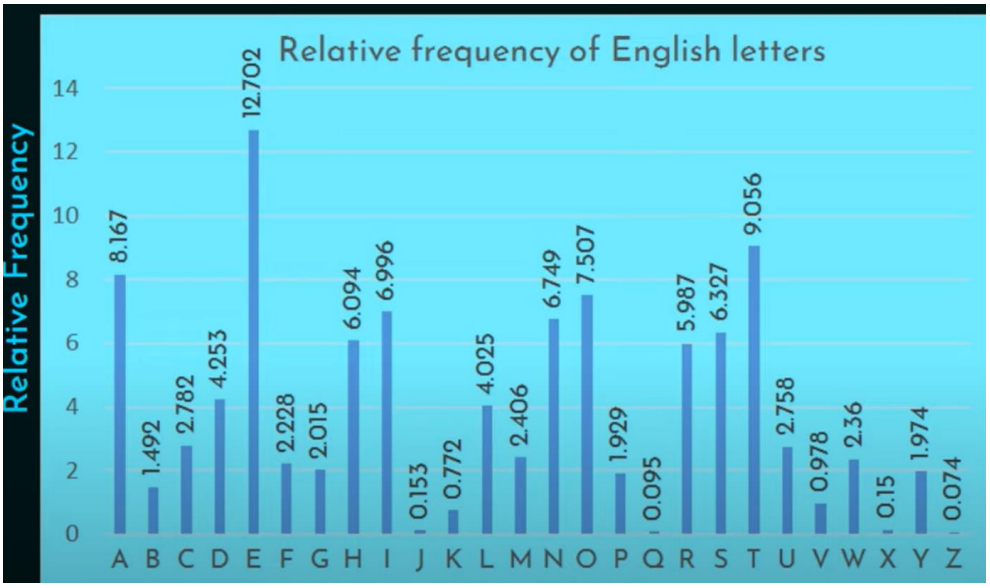


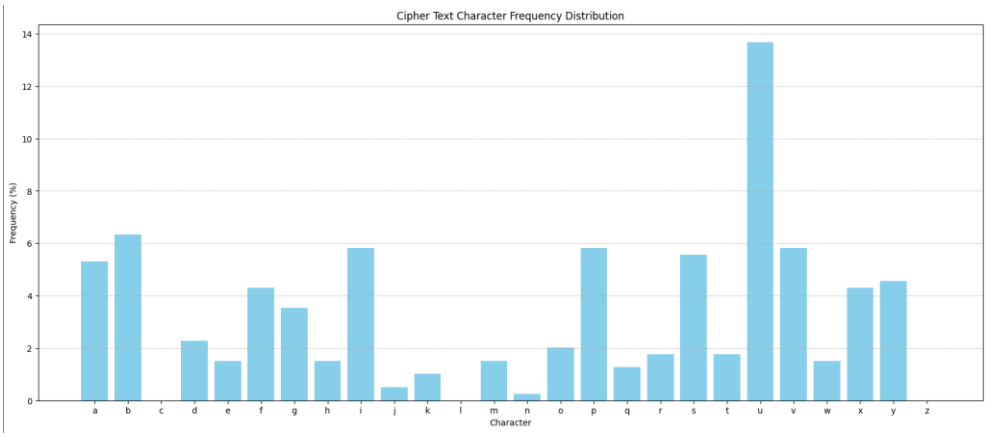



## Decryption:



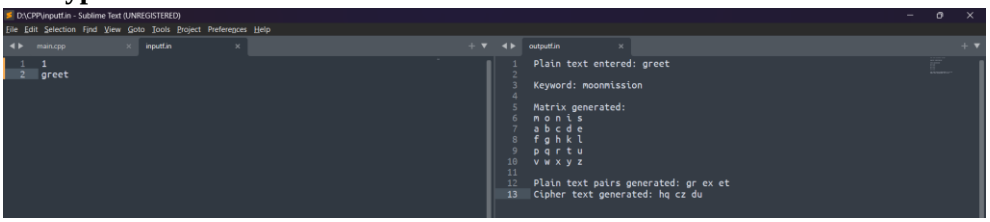

## Cryptanalysis:



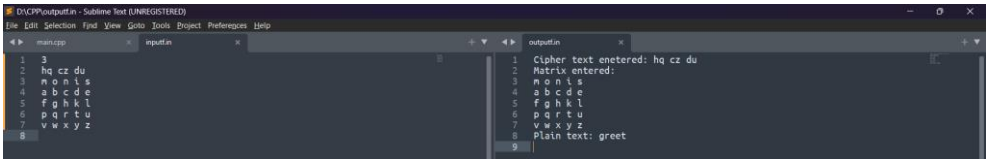



## 3. Playfair Cipher

### Encryption:

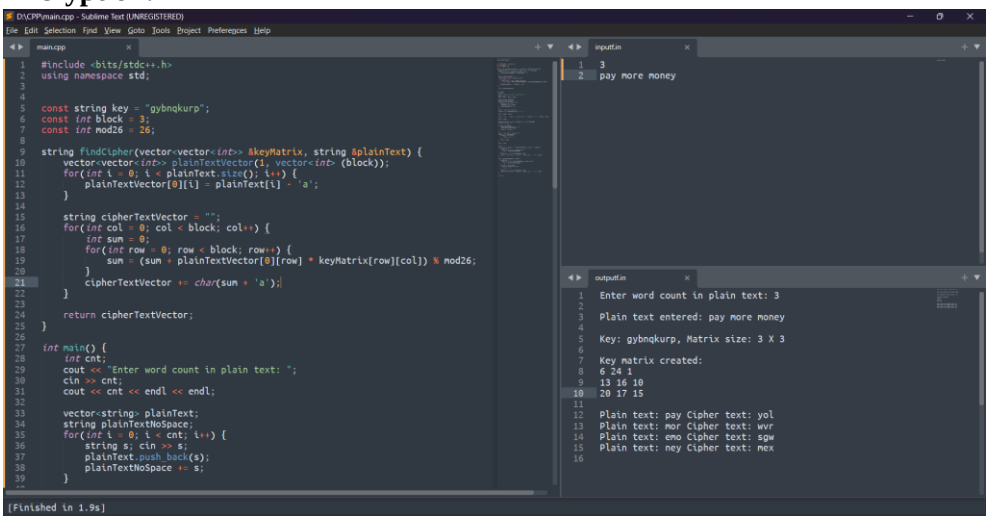



### Decryption:

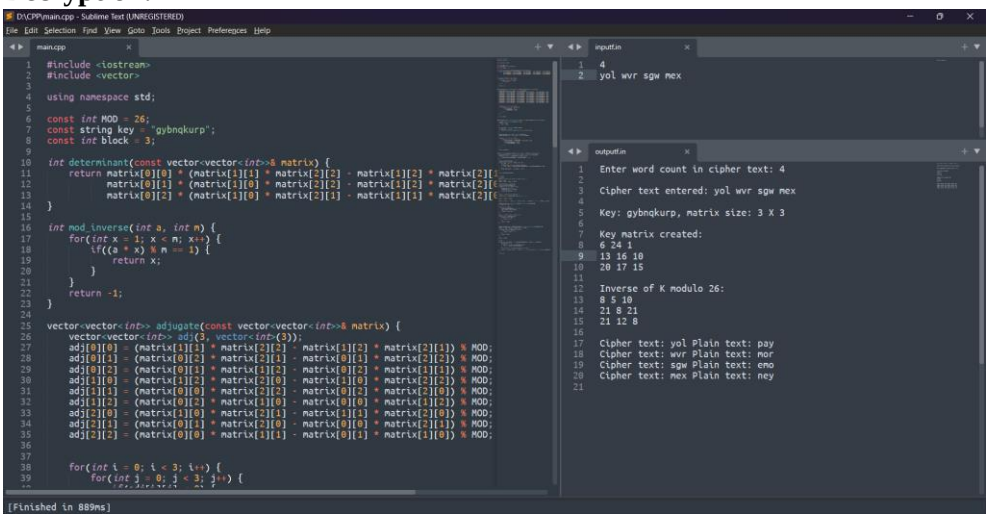



## 4. Hill Cipher

### Encryption:

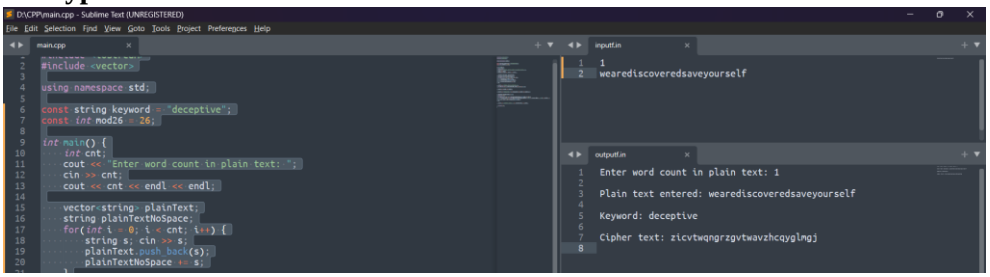


**Decryption:**

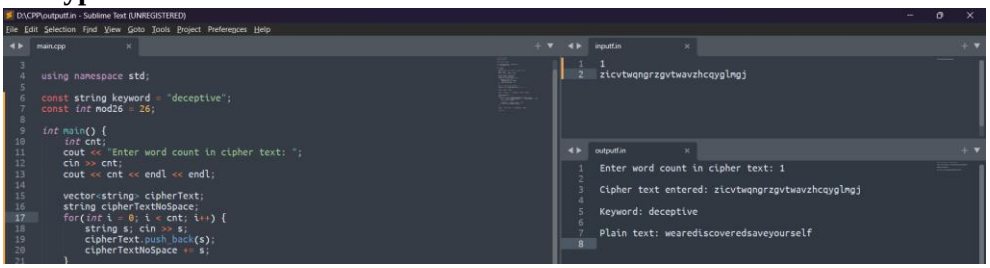



## 5. Polyalphabetic Cipher

**Encryption:**




**Decryption:**




**CONCLUSION:**

Through this experiment, I explored and implemented various substitution encryption techniques, including Caesar cipher, Monoalphabetic cipher, Playfair cipher, Hill cipher, and Polyalphabetic (Vigenère) cipher. This hands-on experience provided a comprehensive understanding of how these algorithms function and how they can be applied to convert plaintext into ciphertext and vice versa.