**Name : Akash Babu Misal**

**PRN: 21520005**

**Class:** Final Year (Computer Science and Engineering)

**Course Name: Cryptography and Network Security**  **Lab**

**Assignment No – 4**

Aim - Implementation of Vigenère Cipher

Theory –

**Vigenère Cipher Overview:**

The Vigenère Cipher is a polyalphabetic substitution cipher that improves upon the Caesar Cipher by using a keyword to determine different shift values for different positions in the plaintext. It involves repeatedly applying Caesar Cipher shifts based on the letters in the keyword.

**Part-A: Encryption**

In this part of the experiment, we will implement the Vigenère Cipher encryption process. The encryption process involves the following steps:

Key Setup: The user provides a keyword, which is used to create a repeating key. The keyword is repeated to match the length of the plaintext.

**Input**: The user provides a plaintext message to be encrypted.

**Text Preparation**: The plaintext message is processed to remove spaces and converted to uppercase.

**Encryption**: For each letter in the plaintext, we perform the following steps:

Determine the shift value based on the corresponding letter in the repeating keyword. Apply the Caesar Cipher shift to the letter using the shift value. Replace the original letter with the shifted letter.

**Output**: The encrypted message is produced, which is the ciphertext with varying shifts based on the keyword.

**Part-B: Decryption**

In this part of the experiment, we will implement the Vigenère Cipher decryption process. The decryption process is the reverse of encryption and involves the following steps:

**Input**: The user provides the ciphertext and the keyword used for encryption.

**Text Preparation:** The ciphertext is processed to remove spaces and converted to uppercase.

**Decryption**: For each letter in the ciphertext, we perform the following steps:

Determine the shift value based on the corresponding letter in the repeating keyword. Apply the reverse Caesar Cipher shift to the letter using the negative shift value. Replace the original letter in the ciphertext with the decrypted letter.

**Output**: The decrypted message is produced, which should match the original plaintext message.

**Code**:

#include <bits/stdc++.h>

using namespace std;

string format(string &str) {

    stringstream res;

    for (auto &ch : str) {

        if (ch != ' ') {

            res << (char)tolower(ch);

        }

    }

    return res.str();

}

string encrypt(string &plain, string &key) {

    stringstream cipher;

    for (int i = 0; i < plain.size(); i++) {

        int val = plain[i] - 'a' + key[i % (key.size())] - 'a';

        cipher << (char)('a' + (val % 26));

    }

    return cipher.str();

}

string decrypt(string &cipher, string &key) {

    stringstream plain;

    for (int i = 0; i < cipher.size(); i++) {

        int val = cipher[i] - 'a' - (key[i % (key.size())] - 'a');

        plain << (char)('a' + (val + 26) % 26);

    }

    return plain.str();

}

int main() {

    int choice;

    cout << "1. Encrypt\n2. Decrypt\nEnter your choice: ";

    cin >> choice;

    cin.get();

    if (choice == 1) {

        string plain, key;

        cout << "\nEnter plain text: ";

        getline(cin, plain);

        plain = format(plain);

        cout << "\nEnter key: ";

        getline(cin, key);

        string cipher = encrypt(plain, key);

        cout << "\nEncrypted text is : " << cipher << endl;

    } else if (choice == 2) {

        string cipher, key;

        cout << "\nEnter cipher text: ";

        getline(cin, cipher);

        cipher = format(cipher);

        cout << "\nEnter key: ";

        getline(cin, key);

        string plain = decrypt(cipher, key);

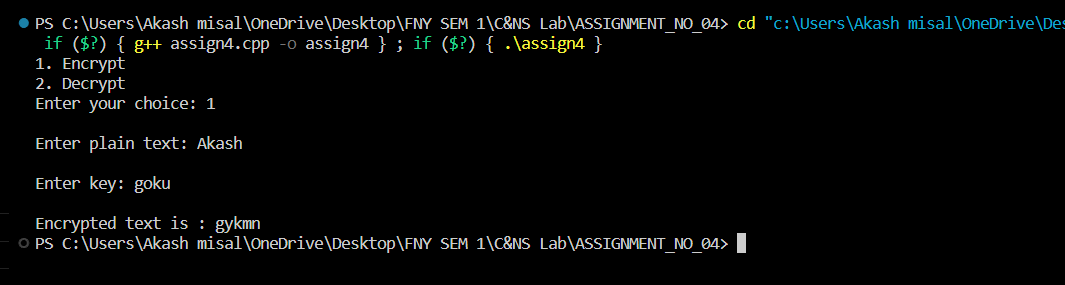
        cout << "\nDecrypted text is : " << plain << endl;

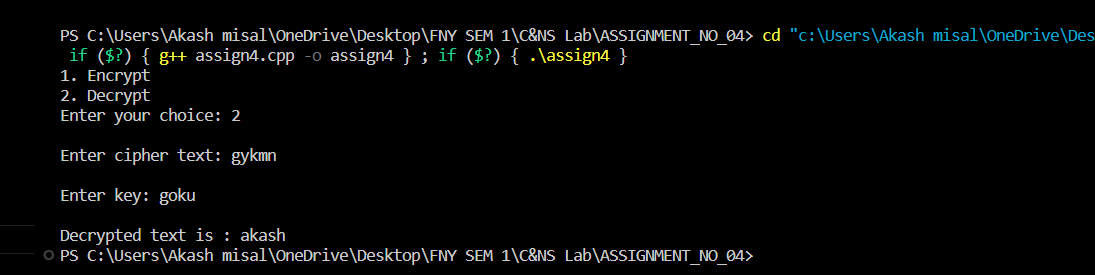
    }

    return 0;

}

**Output**:





**Conclusion**:

The Vigenère Cipher is a more advanced encryption technique that offers improved security compared to simple ciphers like the Caesar Cipher. This experiment allows us to understand both the encryption and decryption processes of the Vigenère Cipher and highlights the importance of the keyword in creating a variable shift for each character in the plaintext. Proper implementation and key management are crucial for maintaining the confidentiality of the message.