Name: Nikita Shivchandra Khot

PRN No: 2020BTECS00041

Assignment No 4

Aim: To Study and implementation of Vigenere Cipher Technique

Theory: It is a classical symmetric-key encryption method that improves upon Caesar Cipher by using a keyword to shift letters in a more complex pattern.

Encryption: Convert plaintext message to numbers, typically using the A=0, B=1, C=2, ... Z=25 mapping. Convert the repeating keyword to numbers using the same mapping. Add the corresponding numbers of the message and the keyword (mod 26) to get the ciphertext. Mod 26 means that if the result is greater than or equal to 26, you subtract 26 until it's less than 26.
Decryption: To decrypt, you use the same keyword. Subtract the keyword's numbers from the ciphertext numbers (mod 26) to obtain the original plaintext.

Code:

```
#include<bits/stdc++.h>
using namespace std;
string generateKey(string str, string key)
{
    int x = str.size();
    for (int i = 0; ; i++)
    {
        if (x == i)
            i = 0;
        if (key.size() == str.size())
            break;
        key.push_back(key[i]);
    }
    return key;
}
string encrypt(string str, string key)
{
    string cipher_text;
    for (int i = 0; i < str.size(); i++)
    {
        char x = (str[i] + key[i]) % 26;
        x += 'A';
        cipher_text.push_back(x);
    }
    return cipher_text;
}
```

```
string decrypt(string cipher_text, string key)
{
    string text;
    for (int i = 0 ; i < cipher_text.size(); i++)
    {
        char x = (cipher_text[i] - key[i] + 26) % 26;
        x += 'A';
        text.push_back(x);
    }
    return text;
}
int main()
{
    string str = "GOODMORNINGALL";
    string keyword = "MONARCHY";

    string key = generateKey(str, keyword);
    string cipher_text = encrypt(str, key);

    cout << "\n(Encrypted)Cipher Text: " << cipher_text << "\n";
    cout << "\n(Decrypted)Plain Text: " << decrypt(cipher_text, key);

    return 0;
}
```

Output:

```
71 + 77 = 148  (18)  S
79 + 79 = 158  (2)  C
79 + 78 = 157  (1)  B
68 + 65 = 133  (3)  D
77 + 82 = 159  (3)  D
79 + 67 = 146  (16)  Q
82 + 72 = 154  (24)  Y
78 + 89 = 167  (11)  L
73 + 77 = 150  (20)  U
78 + 79 = 157  (1)  B
71 + 78 = 149  (19)  T
65 + 65 = 130  (0)  A
76 + 82 = 158  (2)  C
76 + 67 = 143  (13)  N

(Encrypted)Cipher Text: SCBDDQYLUBTACN

(Decrypted)Plain Text: GOODMORNINGALL
```

Logic:

Encryption

The plaintext(P) and key(K) are added modulo 26.

$E_i = (P_i + K_i) \bmod 26$

Decryption

$D_i = (E_i - K_i) \bmod 26$

Limitations:

Vigenère Cipher is more secure than the Caesar Cipher because it introduces variability in the letter shifting based on the keyword. However, it's not as strong as modern encryption techniques like AES or RSA. Vigenère ciphers can still be cracked with sufficient computational power and analysis, especially if keyword is short or easily guessable.