CS302 Information Security and Cryptography

Assignment - 3

U20CS135

Implement,

1. Encryption and decryption using Hill cipher.

2. Encryption and decryption using Vigenere cipher.

1.

Code

```
#include <bits/stdc++.h>
using namespace std;


void getKeyMatrix(string key, int keyMatrix[][3])
{
   int k = 0;
   for (int i = 0; i < 3; i++)
   {
       for (int j = 0; j < 3; j++)
       {
           keyMatrix[i][j] = (key[k]) % 65;
           k++;
       }
   }
}
```

```
void encrypt(int cipherMatrix[][1],
             int keyMatrix[][3],
             int messageVector[][1])
{
   int x, i, j;
   for (i = 0; i < 3; i++)
   {
       for (j = 0; j < 1; j++)
       {
           cipherMatrix[i][j] = 0;

           for (x = 0; x < 3; x++)
           {
               cipherMatrix[i][j] +=
                   keyMatrix[i][x] * messageVector[x][j];
           }

           cipherMatrix[i][j] = cipherMatrix[i][j] % 26;
       }
   }
}



void HillCipher(string message, string key)
{

   int keyMatrix[3][3];
   getKeyMatrix(key, keyMatrix);

   int messageVector[3][1];



   for (int i = 0; i < 3; i++)
       messageVector[i][0] = (message[i]) % 65;

   int cipherMatrix[3][1];
```

```
    encrypt(cipherMatrix, keyMatrix, messageVector);

    string CipherText;


    for (int i = 0; i < 3; i++)
        CipherText += cipherMatrix[i][0] + 65;


    cout << " Ciphertext:" << CipherText;
}


int main()
{

    string message;
    cin>>message;


    string key;
    cin>>key;

    HillCipher(message, key);
    cout<<endl;

    return 0;
}
```

```
node_sm@temple:~/Desktop/CourseWork/ict/Assignment 3$ ./hill
shivam
mishra
 Ciphertext:OTA
```

2.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 cipherText(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 originalText(string cipher_text, string key)
{
    string orig_text;

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

        char x = (cipher_text[i] - key[i] + 26) %26;


        x += 'A';
        orig_text.push_back(x);
    }
    return orig_text;
}


int main()
{
    string str;
    string keyword;
    cin>>str;
    cin>>keyword;
    string key = generateKey(str, keyword);
    string cipher_text = cipherText(str, key);

    cout << "Ciphertext : "
        << cipher_text << "\n";

    cout << "Original/Decrypted Text : "
        << originalText(cipher_text, key);
```

```
    return 0;
}
```

```
node_sm@temple:~/Desktop/CourseWork/ict/Assignment 3$ ./vig
shivam
mishra
Ciphertext : QBMODY
```

SUBMITTED BY: U20CS135

Shivam Mishra