

Cryptography and Network Security

Name: Piyush Mhaske
PRN : 2019BTECS00089

Batch: B3

Assignment 4

Objective:

Vigenere Cipher

Theory:

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.

- The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Cipher.
- At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
- The alphabet used at each point depends on a repeating keyword.

Code:

```
//code by :- Piyush Mhaske
#include <bits/stdc++.h>
#define ll long long
#define ul unsigned long long
#define pb emplace_back
#define po pop_back
#define vi vector<ll>
#define vii vector<vector<ll>>
using namespace std;
void file(){
    ios_base::sync_with_stdio(false);
    cin.tie(NULL);}
ll M = 1e9 + 7;
string Vignere(string PlainText, string key){
    vector<vector<char>> table(26);
```

```

vector<char> temp(26);
string ans;
for(int i=0;i<26;i++){
    int count=0;
    for(int j=i;count<26;j=(j+1)%26,count++){
        temp[count] = 'a' + j;
    }
    table[i] = temp;
}

for(auto x:table){
    for(auto y:x){
        cout<<y;
    }
    cout<<"-----\n";
}

int n = key.size();
int m = PlainText.size();
int num = m/n;
int rem = m%n;

while(--num){
    key+=key;
}

key += key.substr(0,rem);
cout<<key;

for(int i=0;i<PlainText.size();i++){
    ans+= table[PlainText[i]-'a'][key[i]-'a'];
}
return ans;
}
int main()
{
    file();






    string PlainText, CipherText, key;
    cin>>PlainText>>key;






    CipherText = Vignere(PlainText, key);
    cout<<CipherText<<"\n";

    return 0;
}

```

Output:

```
^ Testcase 1 Passed 30ms    
Input:   
thisisthekey  
assignment  
Expected Output:   
tzaaofflrdeq  
Received Output:   
tzaaofflrdeq
```

```
^ Testcase 2 Passed 31ms    
Input:   
remotelocation  
geology  
Expected Output:   
xiazhkjugoewul  
Received Output:   
xiazhkjugoewul
```

Conclusion:

Vigenere cipher is repeating nature of it's keys. If a cryptanalyst correctly guesses the key's length, the cipher text can be treated as interwoven Caesar Cipher, which can easily be broken individually.