

Cryptography and Network Security

Name: Piyush Mhaske
PRN : 2019BTECS00089

Batch: B3

Assignment 5

Objective: Columnar Transposition

Theory:

The Columnar Transposition Cipher is a form of transposition cipher just like Rail Fence Cipher. Columnar Transposition involves writing the plaintext out in rows, and then reading the ciphertext off in columns one by one.

Code:

```
//code by :- Piyush Mhaske
#include <bits/stdc++.h>
#define ll long long
#define ull unsigned long long
#define pb emplace_back
#define 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 Columnar(string PlainText, string key){
    string ans;
    unordered_map<char, vector<char>> mp;
    int j=0;
    int m = key.size();
    for(int i=0; i<PlainText.size(); i++){
        mp[key[j]].push_back(PlainText[i]);
        j = (j+1)%m;
    }

    for(int i=0; i<26; i++){
        if(mp.count('a'+i)){
            for(auto x:mp['a'+i]){
```

```

        ans+=x;
    }
}



return ans;

}
int main()
{
    file();
    string PlainText, CipherText, key;
    cin>>PlainText>>key;

    CipherText = Columnar(PlainText, key);
    cout<<CipherText<<"\n";
    return 0;
}

```

Output:

^ **Testcase 1 Passed** 32ms  

Input: [Copy](#)

```
thisisthekey
assignment
```

Expected Output: [Copy](#)

```
tehistsehiyk
```

Received Output: [Copy](#)

```
tehistsehiyk
```

```
^ Testcase 2 Passed 29ms
Input: success consistency
Expected Output: secucss
Received Output: secucss
```

Conclusion:

Easy to Crack the message can be predicted if it is small.