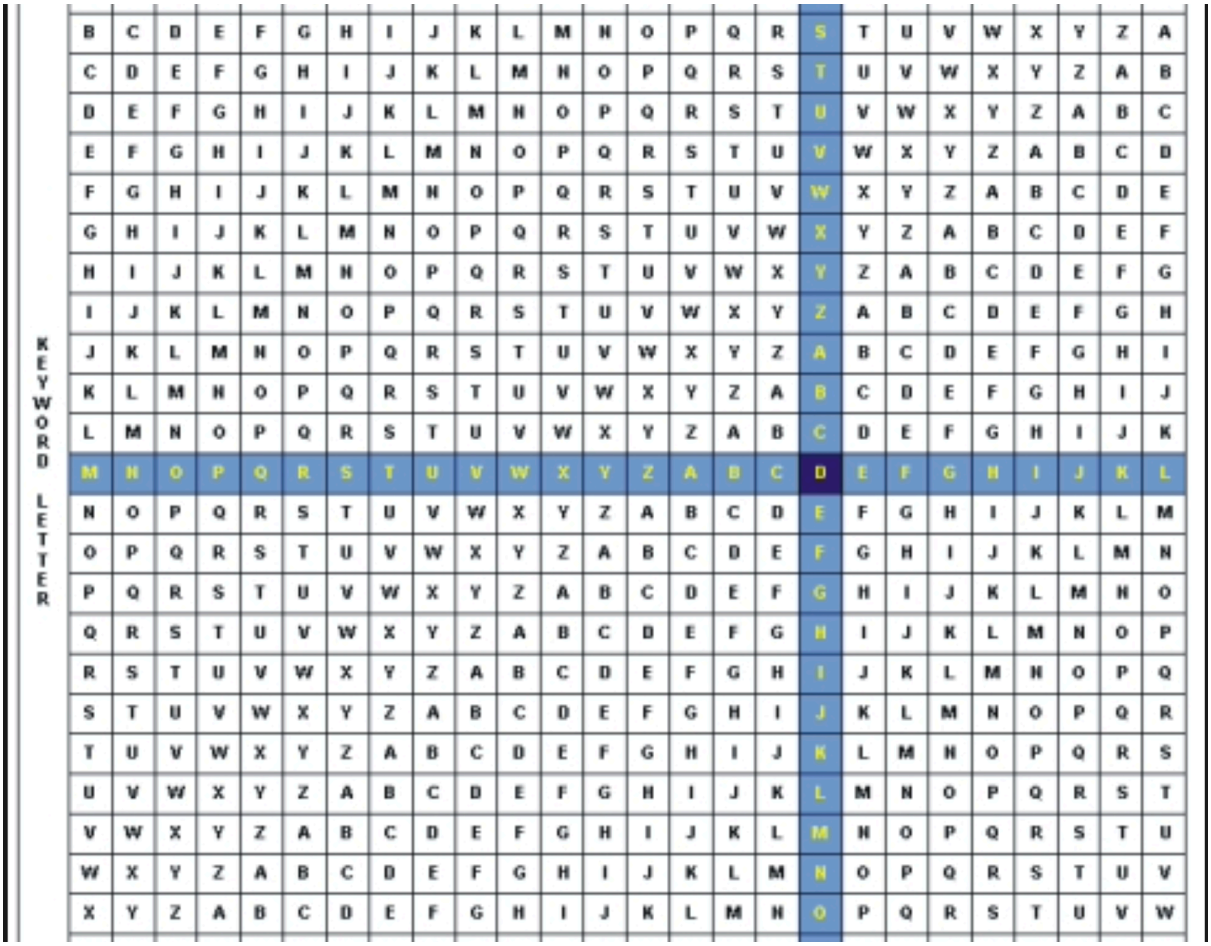
KAMEL Tarek
ABDALLAOUI Mohamed
Encadré par : Pr JOUHARI Houda

TP: Cryptosystème de Vigenère



Objectif:

Le but de ce TP est de programmer les fonctions de chiffrement et déchiffrement du cryptosystème de Vigenère puis d'effectuer une attaque à force brute sur un texte chiffré.

Chiffrement de Vigenère :

I. Demander à l'utilisateur de taper le message clair Plaintext et le mot- clé Keyword;

```
//Demander à l'utilistaeur d'entrer le texte chiffré
cout << "Entrer le texte clair : " << endl;
string plainText;
getline(cin, plainText);
```

II. Créer une fonction «Chiffrer» qui prend en entrée ces deux chaines de caractères Plaintext et Keyword et qui retourne la chaine de caractère Ciphertext.

```
//Fonction de chiffrement
string chiffrer(string plainText, string key)
{
return cipherText;
}
```

1. Transformer le texte en une chaine de caractère en majuscule tout en supprimant les espaces ;

```
//Transformer le texte clair en majuscule
for(int i=0; i<plainText.size(); i++)
{
    plainText[i] = toupper(plainText[i]);
}
```

2. Transformer le mot-clé en une chaine de caractère en majuscule ;

```
//Transformer la clé en majuscule
for(int i=0; i<key.size(); i++)
{
    key[i] = toupper(key[i]);
}
```

3. Faire associer un nombre entier à chaque lettre de l'alphabet : convertir le
message et la clé en nombres. Pour cela, vous aurez besoin de définir la variable :

```
int alphabet[26] = {'A','B', 'C', 'D', 'E', 'F', 'G', 'H', 'I',
'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U',
'V', 'W', 'X', 'Y', 'Z'};
```

4. Calculer la function de chiffrement modulos 26 :

```
//Appliquer le chiffrement
for(int i=0; i<plainText.size(); i++)
{
    cipherArray[i] = (plainTextArray[i] + keyArray[i%key.size()])%26;
}
```

5. Copier le contenu du tableau de caractères en une chaine de caractère : Le chiffré.

```
//Tableau de correspondance de la clé
for(int i=0; i<key.size(); i++)
{
    keyArray[i] = key[i] - 'A';
}
```

```
//Tableau de correspondance du texte clair
for(int i=0; i<plainText.size(); i++)
{
    plainTextArray[i] = plainText[i] - 'A';
}
```

Pour notre cas :

Cas 2 : Demander à l'utilisateur d'entrer la longueur de la clé utilisée.

Voici nos résultats :

```
Entrer le texte clair :
Ceci est une phrase de test
Entrer la clé
ABCD
cipher text is: CFELETVXNFRKRBUHDFVHSU
mohamedabdallaoui@Mohameds-MBP TP1_CS %
```