

Barret Alexandre - Mizoules Vincent

Compte rendu - TP5

Usage

Pour lancer notre programme :

```
make && ./tp5
```

Pour nettoyer le projet

```
make clean  
make clear
```

Il est possible de désactiver l'affichage des informations de debug en commentant/décommentant le `define` présent au début du programme.

Réponses aux questions

1) Fonctions de chiffrement et déchiffrement par substitution

polyalphabétique de Vigenère.

Les méthodes `encrypt()` et `decrypt()` de la classe `Vigenere` réalisent le chiffrement et déchiffrement par substitution polyalphabétique de Vigenère.

(cf `main_cipher.cpp`)

2) Fonction de décryptage du chiffrement de Vigenère via l'indice de coïncidence et d'un test de χ^2

La méthode `analyze()` de la classe `VigenereCryptanalysis` réalise le décryptage du chiffrement de Vigenère via l'indice de coïncidence et d'un test de χ^2 .

(cf `main_cryptanalysis.cpp`)

Le principe de cette fonction est le suivant :

```
// calcul de la taille de la clé
On initialise les variables
Tant que la taille de la clé n'est pas suffisante pour avoir un IC correct
|   Pour chaque lettres de l'alphabet
|   |   Calculs...
|   FinPour
|   Calcul l'IC
FinTantQue
```

```
// recherche de la clé
```

```
Pour chaque lettres de la clé
```

```
|   Pour chaques lettres de l'alphabet
```

```
|   |   Calcul du chi2 partiel
```

```
|   FinPour
```

```
|   On garde le chi2 minimal et la lettre assiciée
```

```
FinPour
```

```
On déchiffre le message
```