TD 2 Cybersécurité

1 Clés secrètes

Un chiffré a été intercepté issu du chiffrement suivant:

```
def efface(c):
    return c.replace(' ','')
def chiffre(s,k):
    def h(x):
        return chr(((ord(x)-ord('a')+k)%26)+ord('a'))
    return "".join(list(map(h,list(efface(s)))))
```

Le chiffré intercepté est en français (sans espaces) et sa distribution des fréquences est donné Fig. 1:

`ultactdfynstqqcpopnpdlcazfcqltcpdtxawp`

(1) Comment les lettres sont-elles codées?

(2) Quelles sont les hypothèses pour en faire la cryptanalyse?

(3) Quel est l'espace des clés?

(4) Faites-en la cryptanalyse par force brute en le programmant.

(5) Quelle(s) autre(s) cryptanalyse pourrait-on faire?

(6) Est-ce plus simple si vous savez que la première lettre du clair est un `j`?

2 Chiffre de Feistel

Un **chiffre de Feistel** de taille de bloc $2n$ à r tours est défini par :

$$g : \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^n \times \{0,1\}^n$$

$$X, Y, Z \mapsto (Y, F(Y,Z) \oplus X)$$

g fonction de $2n \times m$ bits dans $2n$ bits et $\oplus$ XOR sur n bits.

(1) Montrer qu'en inversant l'ordre d'utilisation des clés de tour dans un chiffre de Feistel, on peut utiliser le même algorithme pour déchiffrer que celui utilisé pour chiffrer. On se limitera à un chiffre de Feistel à 2 tours dont la valeur de $m = n$.

(2) Peut-on utiliser le chiffre précédent pour construire un chiffre de Feistel?

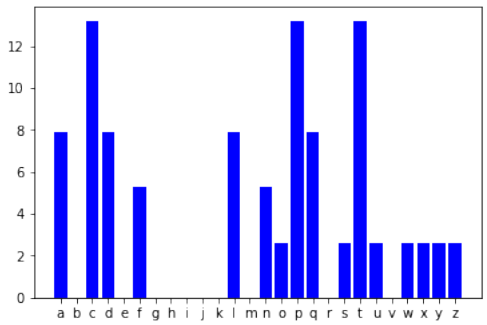

Figure 1: Analyse des fréquences du chiffré

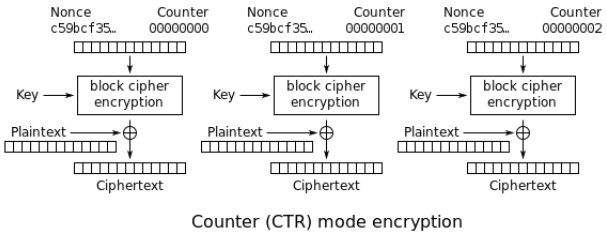

Figure 2: Mode CTR

3 Un protocole cryptographique

On considère le protocole suivant:

(1) $A \rightarrow B : \{K\}_{pkA}$

(2) $A \leftarrow B : \{\{K\}_{pkA}\}_{pkB}$

(3) $A \rightarrow B : \{\{\{K\}_{pkA}\}_{pkB}\}_{skA}$

(1) Quelle est l'information partagée par A et B pour que ce protocole fonctionne ?

(2) Quelles sont les informations conservées secrètes par chaque partie ?

(3) Décrire et expliquer le fonctionnement de ce protocole.

(4) Quelles propriétés de sécurité sont assurées?

(5) Comment B peut-il récupérer K à l'issue de la 3e étape?

(6) Pourrait-on échanger le rôle des clés secrètes et des clés publiques?

4 Modes de chiffrement

Il est conseillé de chainer le chiffrement de blocs de clair. Un des mécanismes conseillés est celui du mode CTR décrit dans la Fig. 2:

(1) Décrivez comment mettre en place le mode CTR avec le chiffre qu'on a obtenu à la question 2.2.