INFO002 : cryptologie
TD 1 : cryptologie historique

Pierre Hyvernat
Laboratoire de mathématiques de l'université de Savoie
bâtiment Chablais, bureau 17, poste : 94 22
email : Pierre.Hyvernat@univ-smb.fr
www : http://www.lama.univ-smb.fr/~hyvernat/

```
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
1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
```

Exercice 1 : code de César et substitutions monoalphabétiques

Question 1. Décryptez le texte suivant, chiffré avec un chiffre de César (décalage) :

`XFQZY`

Question 2. Quelle est la particularité du "chiffrement" `ROT13` (décalage de 13 lettres) ?

Question 3. Vous interceptez une réponses chiffrée par substitution monoalphabétique. La question (décryptée auparavant) était

`avez vous besoin de renfort ?`

La réponse est

`VST`

Pouvez-vous décrypter cette réponse ?

Question 4. La question était cette fois

`a qu'elle heure decollez vous ?`

Pouvez-vous décrypter les réponses suivantes ?
- réponse 1 : `MIELHTKTIHTV`
- réponse 2 : `SGNECJZC`

Question 5. Combien de clés y a t'il pour un chiffrement par décalage ?

Comment programmeriez-vous le décryptage automatique d'un texte chiffré par décalage ?

Question 6. Combien de clés y a t'il pour un chiffrement par substitution monoalphabétique ?

Comment programmeriez-vous le décryptage "intéractif" d'un texte chiffré par substitution monoalphabétique ?

Comment programmeriez-vous le décryptage "automatique" d'un texte chiffré par substitution monoalphabétique ?

Exercice 2 : Système monôme-binôme ("straddling checkeboard")

Pour ce système, on écrit l'alphabet désordonné sur 3 lignes de 10 colonnes, *en laissant 2 cases vides sur la première ligne*. On peut ajouter 2 symboles sur la dernière ligne...

Par exemple, pour

```
    0  1  2  3  4  5  6  7  8  9
    c  r  y  -  p  t  o  g  -  a
3   h  i  e  b  d  f  j  k  l  m
8   n  q  s  u  v  w  x  z  .  ␣
```

Les symboles de la première ligne sont codés par leur numéro de colonne, ceux de la deuxième ligne, par `3` (indice de la première case vide) puis leur numéro de colonne, ceux de la troisième ligne, par `8` (indice de la seconde case vide) puis leur numéro de colonne.

Par exemple :
- `p` est chiffré par `4`
- `i` est chiffré par `31`
- `q` est chiffré par `81`

Question 1. Déchiffrez le message

`83803 28632 39438 32823 13943 83288`

Question 2. Combien de choix possibles y a t'il pour les "trous" de la première ligne ?
Proposez une méthode de décryptage pour ce système.

Exercice 3 : auto-clé

Les chiffrements "autoclaves" utilisent le message clair comme (partie de la) clé !
Si le message clair est donné par $m_1 m_2 m_3 \ldots$, et la clé k, on obtient le chiffrement

$$\begin{cases} M_1 = (m_1 + k) \bmod 26 \\ M_i = (m_i + m_{i-1}) \bmod 26 \quad \text{si } i > 1 \end{cases}$$

Question 1. Décrypter le message

`PACUB ZWCPD RTSWG GYNYW`

Question 2. Quelle amélioration proposez vous pour rendre la cryptanalyse plus complexe ?

Question 3. À votre avis, pourquoi ce genre de chiffre n'a t'il jamais été vraiment utilisé ?

Exercice 4 : chiffrement par permutation de colonnes

Pour ce système, on écrit le texte clair dans un rectangle, qu'on réécrit ensuite en colonnes :

		`vive`		
`vive la crypto`	donne	`lacr`	qui devient donc	`VLYIAPVCTERO`
		`ypto`		

Question 1. Décryptez les messages suivants (la numérotation ne fait pas partie du message).

```
012345678901234567890123
TSDCIHNIUPIOFLHSTFTEIAICR
```

et

```
012345678901234567890123456789012345678
YSIYBOOSABUFOSIMINTTANEHSYDEEAATARYLHSAS
```

Question 2. Proposez une manière de chiffrer un texte qui ne "rentre pas exactement" dans le rectangle choisi.

Question 3. Comme le montrent les exemples, ce système n'est vraiment pas sûr. Une amélioration consiste à permuter les colonnes avant de les lire pour complexifier le décryptage manuel.
Proposez une manière mnémotechnique pour se souvenir à la fois du nombre de colonnes *et* de la permutation finale.

Exercice 5 : divers

Question 1. Décrivez un mécanisme qui permettrait d'empêcher l'analyse de trafic sur un canal de communication.