Université de Perpignan C. Negre

TD 1 Cryptographie

Exercice 1. 1. En utilisant la correspondance

$$\text{Alphabet} \longrightarrow \mathbb{Z}_{26} = \{0, \ldots, 25\}$$

Numériser le texte ci-dessous (du moins une partie)

Des chercheurs tentent de visualiser des raisonnements mathematiques dans les emotions comme la honte ou la compassion.

2. Chiffrer le message précédent avec une méthode par décalage de clef 7.

3. Chiffrer le message avec une méthode par substitution en utilisant la clef $k : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ définie par

$$k(\lambda) = \begin{cases} \lambda + 1 & \text{si } \lambda \neq 7 \text{ et } 25 \\ 0 & \text{si } \lambda = 7, \\ 8 & \text{si } \lambda = 25. \end{cases}$$

Donner la fonction réciproque de k.

4. Chiffrer le message avec une méthode de Vigenère de clef $k = (2, 19)$.

Exercice 2. Surchiffrer consiste à chiffrer plusieurs avec éventuellement des méthodes différentes

$$M \longrightarrow C_1 \longrightarrow C_2 \longrightarrow \cdots \longrightarrow C_n$$

A quel type de une méthode de chiffrement correspond le surchiffrement avec,

- d'abord, une méthode de Vigenère de longueur 3
- et ensuite une méthode de Vigenère de longueur 2

Que dire de la longueur de la clef? Qu'en déduisez- vous dans le cas général du surchiffrement avec deux méthodes de Vigenère.

Exercice 3. (Attaque à message clair chiffré). On considère le message clair suivant

M=cet insecte constitue une espece endemique c est e.

- Le message suivant est un chiffré par substitution du message M précédent. Donner tout ou partie de la clef utilisée.

kapexoakpakyxopepqaqxaaozakaaxlawemqakaopa

- Le message suivant est un chiffré du message M avec une méthode de Vigenère, donner la clef utilisée.

tywremhlkyfxemwrkohdeyhbgyfnvhgndctdvwhbky

Les exercices qui suivent pourront être fait en utilisant les programmes/fichiers situés dans les archives `substitution.tar` et `vigenere.tar` sur la page

`http://perso.univ-perp.fr/christophe.negre/Enseignements/Cryptographie/Master1/`

Exercice 4. (Cryptanalyse par analyse de fréquence)
On considère le message chiffré avec une méthode de substitution.

bqzrllrrlxjltxjprgrvervzrrttrrvldrvlrlerrlriqtjrwqvzxuqwzprixrzovjzzrbr
llrdrljlryjhverzqkcerbqzrllrrlxjlkxjherrlctrkrrttrxuxjlderzprgvjlxwzqwt
vjrwrvlpqwwrxdrjwrzjxzrzhexwpzfrvxrwyqwbrzpxwzvwrzqelrpqkcerdeqyqwprrlx
jrwlderzovrrlrjwlzxyqebrpxuqjedtrvertrzbqjwzprzxcqvbgrxuxjrwlbrllrbqvec
rprtxwhqjzzrgxcjlvrttrovqwqczreurbgrstrzbqwpxkwrzrlbgrstrzkxtxprzprzrzd
rerzzrzkxjwzrlxjrwlbqkkrzxkrertxuxjlprujwrdrepvrzprwhrtverztryrvovjtrbt
xjexjlrwbrkqkrwlyxjzxjlzxjttjetrzxwhtrzprzrzqzrlerwpxjlzxkxjhervexyyerv
zrkrwlujzjctrbqkkrrttrhertqlxjllqviqvezrttrxuxjldejztgxcjlvprprzreerezr
zprvxhrwqvxtvwbqwlertxvlerlqvlzqwurlrkrwlwrlxjlovvwgxjttqwovjrvlyxjldjl
jrtrlrrlovjyxjzxjlgqeervetgjurerttrwxuxjlzverttrovrprtxlqjtrleqvrrdxzvw
bgjyyqwprtxjwrqwuqfxjlzxdrxvxrltxrltqwfpjzljwhvxjldxelqvlprzlxbgrzctrvr
zqvwqjerzovjjwpjovxjrwltrzrwpeqjlzqvtxlgrwxepjretxuxjllqvbgrrzrzixkcrzw
vrzrlxjrwleqvhrzrlhertrztrbervxprzrzbtxujbvtrzrlxjlxyxjerdtrverelqvlrtx
drezqwwrprbrllrrwyxwlzqwxttverzqwxlljlvprtrzqwprzxuqjxzrzjwlreuxttrzrwl
ervwkqlrltxvlerzqwerhxepzqwzjtrwbrzqwkqjwperhrzlrrxdejkxjrwlrllexpvjzxj
rwlvwrzrvtrjprrtxbexjwlrtxbexjwlrrlxjlerdxwpvrzverttrrttrrwrlxjldqvexjw
zjpjerbqvurelrtxbexjwlrexkrwxjlzrzbqvprzbqwlerzrzgxwbgrzerljexjlzrzlxtq
wzzqvzzrzivdrztvjyxjzxjllrwjetrkqjwzprdtxbrdqzzjctrwrtvjtxjzzxjlprzqvyy
trovrtrwrbrzzxjerrlrlxjlprurwvrbrovqwdqveexjlxddrtrezqwgxcjlvprprbqedzz
xwzuxejxljqwdqzzjctrovrpxvhkrwlrejtfxuxjlxvyqwpprzxdevwrttrvwbqjwrlqwwr
qvrlxjltxlreerve

1. Sachant que les lettres sont substituées par paire (par exemple a est substitué avec h, et h est substitué par a) quel est le nombre de clef de chiffrement de ce type.
2. Donner le tableau des fréquences des lettres, et des fréquences des bigrammes les plus fréquents.
3. En déduire la clef de chiffrement et le message clair correspondant.

Exercice 5. (Cryptanalyse par analyse de fréquence) On considère le message chiffré suivant avec une méthode de Vigenère.

yitufcivcoraqneuwhndqmgqtsnvnxrvxapcwwnygayao
rcbycvvgraraibdrvxrpyapjdhjwctgcxrzamxulgzewdcwwrevwr
bfoaxrehmvbttvmotryyxyemqywnkilpeberyrapnegzibanzhjfg
zibzhxeaorawhxowpndgzewdcwwrevwrbttvmotryyxycmvvfgmpn
dymxccrahdxrawjrrijryqmpncrvhapvvmwertprrvjpnlhksdcfl
ibdvmgupfliwzzjvnfkacberuibnegtcztzeysvyyndbvxnerumbl
hxsrygliywhaiwaycwypenilevwrwpfliywhaiwaycwjdgcgrphf

1. Pour les périodes $m = 3, 4, 5, 6$, calculer les indices de coincidence des sous-messages. En déduire la longueur de la clef.

2. Décomposer le message en sous-messages, et déterminer la clef de chiffrement en effectuant une série d'attaques par analyse de fréquences.

Exercice 6 (Enigma)**.** Nous allons établir ici une propriété qui permet de déterminer l'ordre des rotors dans Enigma. Cette approche fut proposée par Gillogly en 1995.

1. Montrer que l'indice de coïncidence du texte obtenu après le premier passage dans le tableau de connexions est identique à celui du texte clair.

2. En supposant que la fréquence de chaque lettre dans le chiffré produit par la machine Enigma soit uniforme, calculer la proportion de lettre modifiées par le tableau de connections à la fin du processus de chiffrement.

3. Nonton g_i, $i \in \{0, 1, \ldots, 25\}$, le nombre moyen d'occurrences d'une lettre i dans le texte obtenu en déchiffrant le le message chiffré avec la bonne configuration de rotors mais un tableau de connexions sans fiche. Montrer que, sous l'hypothèse de la question 2, on a

$$g_i = \frac{n}{13}\left(\frac{6}{26} + 7f_i\right) \text{ pour } i \in \{0, 1, \ldots, 25\}$$

   où f_i est la fréquence de la lettre i dans le texte clair, et n est le nombre de lettre du message.

4. En déduire l'indice de coincidence du texte obtenu en fonction de l'indice de coïncidence I_1 du texte clair original et de I_0 d'un texte avec des lettre apparaissant avec une fréquence uniforme. Calculer sa valeur en supposant que le texte clair original à l'indice de coïncidence de la langue française est de 0.078.

5. Monter une attaque basée sur ces résultats.