info223 : Science informatique
TD 6 : chiffrement par substitution

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

Exercice 1 : chiffrement par rotation

Question 1. Le code de César est une méthode de chiffrement par rotation de l'alphabet. Dans la version utilisée par Jules César, un décalage de trois lettres vers la droite était effectué pour coder.

Construisez une table indiquant le codage de chaque lettre de l'alphabet latin.

Décodez le message "`YHQL, YLGL, YLFL`".

Codez le message "`JE SUIS VENU, J'AI VU, J'AI VAINCU`".

Question 2. Si on se limite à l'alphabet latin, combien de possibilités de rotation y a-t-il ? Et avec un alphabet de taille n ?

Question 3. Quel est l'avantage du chiffrement par rotation de 13 lettres ?

Exercice 2 : substitution monoalphabétique

Question 1. De manière générale on peut utiliser une substitution de l'alphabet pour chiffrer un texte (la rotation en est un cas particulier). On considère maintenant la substitution suivante :

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
C	F	Z	J	L	A	K	N	Q	V	G	O	B	T	Y	D	R	X	H	I	M	W	P	S	U	E

Décodez le message "`O'QTAY Z'LHI KLTQCO`".

Codez le message "`JE SUIS BATMAN`".

Question 2. Si on se limite à l'alphabet latin, combien de possibilités de permutations y a-t-il ? Et avec un alphabet de taille n ?

Question 3. Comment peut-on généraliser le chiffrement par substitution (et donc par rotation) à l'ensemble des caractères ASCII ?

Exercice 3 : code de Vigenère et cryptanalyse

Question 1. Le code de Vigenère repose sur le même principe que le code de César, mais les lettres ne sont pas toutes décalées de la même manière. Par exemple, avec la clé `BLA` les trois premier caractères du textes seront décalés de 2, 12 et 1 lettre respectivement, car :

- `B` est la 2ème lettre de l'alphabet,
- `L` est la 12ème lettre de l'alphabet,
- `A` est la 1ère lettre de l'alphabet.

On répète ensuite les mêmes décalages pour les caractères suivants : 2, 12, 1, 2, 12, 1, 2, 12, etc.

Décodez le message "`TBJXC CLGN`" en utilisant la clé "`JAWS`".

Codez le message "`BLAISE DE VIGENERE `" en utilisant la clé "`CODE`".

Question 2. Pour deux textes de même taille, l'indice de coïncidence est le pourcentage des positions pour lesquelles les deux textes ont une lettre identique. Quel est l'indice de coïncidence attendu pour deux chaines aléatoires ?

Question 3. Entre deux textes quelconques *en français*, l'indice de coïncidence moyen est de $7,46\%$. Comment peut-on expliquer ce résultat ?

Question 4. Quelle est la valeur attendue de l'indice de coïncidence pour deux textes en français qui on été codés avec la même clé ?

Quelle est la valeur attendue de l'indice de coïncidence pour deux textes en français qui on été codés avec la même clé, mais qui ne sont pas "alignés"? (Par exemple car on ne connait pas les premiers caractères d'un des textes.)

Question 5. Étant donné un texte crypté avec le code de Vigenère, comment peut-on retrouver la taille de la clé en utilisant l'indice de coïncidence ?

Question 6. Proposez des outils pour craquer un texte crypté par permutation monoalphabétique.

Quels outils peut-on réutiliser pour craquer un texte crypté avec le code de Vigenère *lorsqu'on connait la taille de la clé* ?

Question 7. Proposez une méthode de cryptanalyse complète pour un texte crypté avec le code de Vigenère.