TD 4 - Cryptographie

Exercice 1. (Chiffre de César)
Le chiffre de César consiste à décaler les lettres constituant le message d'un indice fixe. La clé est donnée par la lettre qui remplacerai la lettre A. Par exemple si cette clé est F, on considère le tableau suivant :

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

Et on code le message SALSIFIE en XFQXNKNJ.

1. Coder le message C'EST PAS FAUX avec la clé K (on pourra utiliser le carré de Vigenère en annexe).
2. Decoder le message VMDMZ OWVVI OQDM GWC CX sachant qu'il a été codé avec la clé I.
3. On représente les lettres comme des éléments de $\mathbb{Z}/26\mathbb{Z}$ (A $= 0$, B $= 1, \ldots$). Si la clé est une lettre associée à $i \in \mathbb{Z}/26\mathbb{Z}$, quelle opération sur un élément de $\mathbb{Z}/26\mathbb{Z}$ correspond au cryptage de la lettre associée ? Même question pour le décryptage ?

Une variante : le chiffrement affine. Plutôt que d'effectuer une translation sur les lettres, on leur applique une transformation affine. La clé est donnée par deux entiers a, b, et le cryptage envoie la lettre d'indice $i \in \mathbb{Z}/26\mathbb{Z}$ sur la lettre d'indice $ai + b \in \mathbb{Z}/26\mathbb{Z}$.

4. Sous quelle(s) condition(s) le chiffrement affine est-il décodable ? Sous cette condition, écrire une méthode de décodage.
5. Décoder le message G'DX INAEB DB GNB, qui a été codé avec la clé $a = 9, b = 3$:

Un problème : L'analyse fréquentielle. Ces chiffrements consistent simplement en une permutation des lettres. En particulier, la fréquence des lettres est conservée : la lettre la plus fréquence code probablement une lettre fréquente en français.

6. Les lettres les plus fréquentes en français sont respectivement le E et le A. Le texte suivant a été codé par un chiffre affine. Déterminer la clé de codage.

AZRDVQ AZL S'DJCZ , D S'WZJMZ PJ CSDQBWVK SD BDRODXQZ,
UZ ODMKVMDV. IPVL-KJ, UZ LDVL NJZ KJ R'DKKZQAL.
U'VMDV ODM SD YPMZK, U'VMDV ODM SD RPQKDXQZ.
UZ QZ OJVL AZRZJMZM SPVQ AZ KPV OSJL SPQXKZROL.

Exercice 2. (Chiffre de Vigenère)
Pour éviter l'analyse fréquentielle, on considère des chiffrements polyalphabétiques : une même lettre n'est pas toujours codée par la même autre lettre. Le chiffre de Vigenère est un exemple : c'est comme un chiffre de César, mais où la clef de codage changerait à chaque lettre du message.

Considérons le message LES CITES D'OR avec la clef PWIYSHWIXMJ. On code la première lettre comme un chiffre de César avec la lettre P, la deuxième lettre comme un chiffre de César avec la lettre W et ainsi de suite, On obtient

L	E	S		C	I	T	E	S		D'	O	R
A	A	A		A	A	A	A	A		A	A	A

Si la clé est plus courte que le message, on la répète pour faire coincider les longueur comme dans l'exemple suivant :

I	L		E	T	A	I	T		U	N	E		F	O	I	S
C	L		E	F	C	L	E		F	C	L		E	F	C	L

1. Coder le message SYNAPTOSOME avec la clé RAT.
2. Quelle clé faut il prendre pour que le chiffrement de Vigenère redonne un chiffre de César ?
3. Soit un texte de n lettres. On pose $n_{\mathtt{A}}, \ldots, n_{\mathtt{Z}}$ le nombre d'occurrences respectives de chaque lettre de l'alphabet dans ce texte. On définit l'***indice de coïncidence*** du texte comme la probabilité que deux lettres tirées au hasard (avec remise) soient égales. Dans un texte en français, l'indice de coïncidence est de 0.075 environ.

a) Montrer que l'indice de coïncidence est donné par

$$IC = \sum_{l=\mathtt{A}}^{\mathtt{Z}} \frac{n_l^2}{n^2}$$

b) Calculer l'indice de coïncidence d'un texte totalement aléatoire.

c) Montrer qu'un chiffrement par permutation des lettres ne change pas l'indice de coïncidence.

d) Montrer que choisir un sous-texte aléatoirement dans un texte en français (suffisamment long) ne change pas son indice de coïncidence.

e) Soit un texte clair "$x_0x_1\dots x_n$", codé en un texte crypté "$y_0y_1\dots y_n$" par un chiffrement de Vigenère avec une clef de longueur $k < n$. Montrer que le texte "$x_0x_kx_{2k}\dots$ est codé en "$y_0y_ky_{2k}\dots$" par un chiffre de César.

En particulier, l'indice de coïncidence de $y_0y_k\dots$ est le même que celui de $x_0x_k\dots$, qui et lui-même celui du français. On peut donc, face à un texte crypté, chercher un entier k qui donne un sous-texte avec un indice de coïncidence proche du français : on peut ainsi déterminer la longueur de la clé, si elle est inférieure à la longueur du texte.

Exercice 3. (Chiffre de Hill)
Soit M une matrice dans $\mathcal{M}_p(\mathbb{Z}/26\mathbb{Z})$. Un mot de longueur p est une suite de lettre, que l'on peut voir comme un vecteur v de $\mathbb{Z}/26\mathbb{Z}$ de longueur p. On peut alors coder le mot v par le mot Mv. (Pour un mot de longueur supérieure à p, on peut bien-sûr découper le mot en mots de longueur p).

1. Sous quelle(s) condition(s) sur la matrice M peut on décoder le message ?
2. On prend $p = 2$ à partir d'ici, et on considère la matrice

$$M := \begin{pmatrix} 3 & -5 \\ 5 & 8 \end{pmatrix}$$

Montrer qu'elle respecte la(les) condition(s) de la question précédente.

3. Coder le message `HORTILLONNAGES` avec la matrice M.
4. Décoder le message `XOEMLO PV VJHDYK`, sachant qu'il a été encodé par la matrice M.
5. Le message `CRYPTO` est encodé en `MPODXM` par une matrice $N \in \mathcal{M}_2(\mathbb{Z}/26\mathbb{Z})$. Calculer la matrice N.

Exercice 4. (Un dernier exemple de chiffrement de Hill) Considérons la matrice

$$M := \begin{pmatrix} 0 & 3 \\ 9 & 0 \end{pmatrix} \in \mathcal{M}(\mathbb{Z}/26\mathbb{Z})$$

1. Calculer le déterminant de M et son inverse.
2. Coder le message `RAMIFICATION` avec la matrice M. Décoder le message `ACQVCUMUNNCK`.

De nos jours, on ne crypte plus du texte : tout est fait par ordinateur, on est donc plus intéressés à crypter des entiers (les bits qui représenterons le texte).

Exercice 5. (RSA)
Soit n un entier, on définit $\varphi(n)$ comme le cardinal de l'ensemble des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

1. Si $n = p$ est premier, montrer que $\varphi(n) = n - 1$.
2. Montrer que, si $n = pq$ est un produit de deux nombres premiers, on a $\varphi(n) = \varphi(p)\varphi(q)$.
3. Montrer que pour tout entier $k \in \mathbb{Z}$, premier avec n on a $k^{\varphi(n)} \equiv 1[n]$.
4. On suppose maintenant que $n = pq$ est produit de deux nombres premiers distincts. Soient c et d deux entiers tels que $cd \equiv 1[\varphi(n)]$. Montrer que $t^{cd} \equiv t[n]$ (on distinguera le cas $t \wedge n = 1$ et $t \wedge n \neq 1$).

Supposons que n et c soient connus (clé publique). Tout le monde peut alors coder un message $t \in \mathbb{Z}$ en appliquant la fonction $t \mapsto t^c \in \mathbb{Z}/n\mathbb{Z}$.

5. Expliquer comment on décode le message.
6. Expliquer en quoi ce système de cryptage est difficile à attaquer.
7. Peut-on coder sans risque tous les message $t \in \mathbb{Z}$?

Exercice 6. (Exponentiation rapide) On a vu que pour utiliser la méthode RSA, il faut calculer des puissances dans $\mathbb{Z}/n\mathbb{Z}$. L'exponentiation rapide est un algorithme efficace dans ce but.

1. a) Rappeler le principe de l'écriture en binaire (en base 2) d'un nombre entier.
   b) Convertir 77 en binaire.
   c) Convertir 11110111011 en base décimale.
2. Soient b et e deux entiers, montrer que b^e s'écrit comme un produit de nombres de la forme b^{2^i}. Il suffit alors de savoir calculer $b^{2^i} = (b^{2^{i-1}})^2$
3. Calculer 6^{77} modulo 50, calculer 5^{22} modulo 23.

Exercice 7. On considère le cryptage RSA associé aux valeurs $p = 53$, $q = 11$ et $c = 3$.

1. a) Calculer la valeur publique associée n.
   b) Calculer $\varphi(n)$.
   c) Calculer la valeur d de la clé privée.
2. On considère le message composé des 4 entiers suivant : 010, 052, 215, 211. Crypter ce message avec la clé publique (n, c).

Exercice 8. Dans le cryptage RSA, supposons que n soit produit de deux nombres premiers p et q proches (on suppose $p > q$). On pose

$$t := \frac{p+q}{2} \quad \text{et} \quad s := \frac{p-q}{2}$$

1. Montrer que s est un entier "petit" et que $n = t^2 - s^2$.
2. On considère l'algorithme suivant
   (a) $t := \lceil \sqrt{n} \rceil$
   (b) $z := t^2 - n$.
   (c) Tant que z n'est pas un carré, faire $t := t + 1$ et $z := t^2 - n$.
   (d) Retourner $p := t + \sqrt{z}$ et $q := t - \sqrt{z}$.
   Montrer que les valeurs p et q sont bien telles que $pq = n$.
3. Utiliser la méthode ci-dessus pour retrouver la clé secrète d correspondante à la clé publique $(n = 899, c = 17)$.

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

Carré de Vigenère