Université de Cergy-Pontoise **2007-2008**
Introduction à la cryprographie **UE libre**

Examen du 7 Avril 2008

Exercice 1 : On donne le carré de Vigenère :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	VWXYZ
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	VWXYZ
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	WXYZA
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	XYZAB
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	YZABC
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	ZABCD
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	ABCDE
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	BCDEF
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	CDEFG
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	DEFGH
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	EFGHI
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	FGHIJ
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	GHIJK
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	HIJKL
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	IJKLM
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	JKLMN
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	KLMNO
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	LMNOP
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	MNOPQ
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	NOPQR
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	OPQRS
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	PQRST
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	QRSTU
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	RSTUV
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	STUVW
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	TUVWX
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	UVWXY

A l'aide du mot-clé "ALGORITHME", et en expliquant le procédé, chiffrer, à l'aide du chiffrement de Vigenère, le texte suivant : “cemodedechiffrementnestpassur”

Exercice 2 : L'adjudant-chef a un problème. S'il fait défiler ses hommes par rang de 4, il n'a que 3 hommes sur le dernier rang, s'il les fait défiler par 5, il lui manque 3 hommes sur le dernier rang et s'il les fait défiler par 6, il lui manque un homme sur le dernier rang. La compagnie comporte entre 100 et 150 hommes. On note X le nombre d'hommes dans la compagnie.

1. Ecrire un sytème (1) de congruences vérifié par X.
2. Enoncer le Théorème des restes chinois.
3. Résoudre le système de congruences :
$$\begin{cases} x & \equiv 1 & \mod 2 \\ x & \equiv 2 & \mod 3 \end{cases}$$
En déduire que
$$x \equiv 1 \mod 2 \quad \text{et} \quad x \equiv 2 \mod 3 \Leftrightarrow x \equiv 5 \mod 6$$
4. Montrer que le système (1) est équivalent au système (2) :
$$(2) \begin{cases} x & \equiv 1 & \mod 2 \\ x & \equiv 2 & \mod 3 \\ x & \equiv 3 & \mod 4 \\ x & \equiv 2 & \mod 5 \end{cases}$$
et que le système (2) est équivalent au système (3) :
$$(3) \begin{cases} x & \equiv 2 & \mod 3 \\ x & \equiv 3 & \mod 4 \\ x & \equiv 2 & \mod 5 \end{cases}$$

5. Résoudre le système (3). En déduire la valeur de X.
6. Pourquoi ne pouvait-on pas utiliser le théorème des restes chinois pour résoudre le système (1) ?

Exercice 3 : On note φ l'indicatrice d'Euler.

1. Calculer $\varphi(32)$. Que représente $\varphi(32)$?
2. A quelle condition un élément de $\mathbb{Z}/32\mathbb{Z}$ est-il inversible ? Donner les éléments inversibles de $\mathbb{Z}/32\mathbb{Z}$.
3. Calculer l'inverse de 15 dans $\mathbb{Z}/32\mathbb{Z}$.

Exercice 4 : Soient p et q deux nombres premiers tels que

$$p \equiv 2 \mod 3 \quad q \equiv 2 \mod 3$$

1. Montrer que $2(p-1)(q-1)+1 \equiv 0 \mod 3$.
2. On pose $k = \varphi(pq)$. Calculer l'inverse dans $\mathbb{Z}/k\mathbb{Z}$ de $e = \frac{2(p-1)(q-1)+1}{3}$.
3. Alice et Bob communiquent en utilisant l'algorithme RSA. La clé publique de Bob est $(187, 3)$.
   (a) Quelle est clé secrète de Bob ?
   (b) Alice veut transmettre le message M à Bob. Bob reçoit 9. Quel était le message M envoyé par Alice ?