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

Corrigé de l'examen du 7 Avril 2008

Exercice 1 : Dans le chiffrement de Vigenère, on commence par répéter la clé pour obtenir une chaîne ayant la même longueur que le texte à chiffrer, puis on chiffre chaque lettre à l'aide du chiffrement par décalage correspond à la lettre de la clé associée en utilisant le carré de Vigenère.

Clé	A	L	G	O	R	I	T	H	M	E
Texte clair	c	e	m	o	d	e	d	e	c	h
Texte chiffré	C	P	S	C	U	M	W	L	O	L

Clé	A	L	G	O	R	I	T	H	M	E
Texte clair	i	f	f	r	e	m	e	n	t	n
Texte chiffé	I	Q	L	F	V	U	X	U	F	R

Clé	A	L	G	O	R	I	T	H	M	
Texte clair	e	s	t	p	a	s	s	u	r	
Texte chiffré	E	D	Z	D	R	A	L	B	D	

Le chiffrement est donné ici par : CPSCUMWLOLIQLFVUXUFREDZDRALBD

Exercice 2 : 1. On obtient le système :

$$\begin{cases} x \equiv 3 & \mod 4 \\ x \equiv 2 & \mod 5 \\ x \equiv 5 & \mod 6 \end{cases}$$

Pour la deuxième équation, puisqu'il manque 3 hommes sur une rangée de 5, il en reste donc 2. De même, quand il manque 1 homme sur une rangée de 6, il en reste 5 sur cette rangée.

2. Soit $M = m_1 \times m_2 \times \ldots \times m_k$ où les m_i sont des entiers deux à deux premiers entre eux. On considère le système de congruences :

$$\begin{cases} x \equiv a_1 & \mod m_1 \\ x \equiv a_2 & \mod m_2 \\ \quad \vdots & \\ x \equiv a_k & \mod m_k \end{cases}$$

Alors il existe une unique solution de ce système modulo M. Elle est donnée par $\sum_{i=1}^{k} a_i M_i y_i \mod M$ où $M_i = \frac{M}{m_i}$ et $y_i = M_i^{-1} \mod m_i$.

3. On applique le théorème des restes chinois à ce système. On a $m_1 = 2$, $m_2 = 3$ (m_1 et m_2 sont premiers entre eux), donc $M = 6$ et $M_1 = 3$, $M_2 = 2$. On obtient alors $y_1 = 1$ et $y_2 = 2$. l'unique solution modulo 6 du système est $5 \mod 6$ et on a bien l'équivalence demandée.
4. Puisque $x \equiv 1 \mod 2$ et $x \equiv 2 \mod 3 \Leftrightarrow x \equiv 5 \mod 6$, le système (1) et le système (2) sont équivalents.
5. On voit facilement que $x \equiv 1 \mod 2$ et $x \equiv 3 \mod 4 \Leftrightarrow x \equiv 3 \mod 4$. Ceci montre que les sytèmes (2) et (3) sont équivalents.
6. Pour résoudre le système (3), on utilise à nouveau le théorème des restes chinois. On pose $m_1 = 3$, $m_2 = 4$ et $m_3 = 5$. m_1, m_2, m_3 sont deux à deux premiers entre eux. On a $M = 60$, $M_1 = 20$, $M_2 = 15$ et $M_3 = 12$. Alors $y_1 = 20^{-1} \mod 3 = 2^{-1} \mod 3 = 2$, $y_2 = 15^{-1} \mod 4 = 3^{-1} = 3$ et $y_3^{-1} = 12^{-1} \mod 5 = 2^{-1} \mod 5 = 3$. L'unique solution modulo 60 est donnée par : $2\times20\times2+3\times15\times3+2\times12\times3 = 287$. On a donc comme solution $47 \mod 60$ pour le système (3). Puisque les systèmes (1) et (3) sont équivalents et que la compagnie comporte entre 100 et 150 hommes, on a $X = 107$.
7. On ne pouvait pas utiliser le théorème des restes chinois directement pour résoudre ce système (1) car 2 et 4 ne sont pas premiers entre eux.

Exercice 3 : 1. On a $32 = 2^5$, donc $\varphi(32) = 2^5 - 2^4 = 16$. $\varphi(32)$ représente le nombre d'éléments inversibles de $\mathbb{Z}/32\mathbb{Z}$.

2. Il y a donc 16 éléments inversibles dans $\mathbb{Z}/32\mathbb{Z}$. Un élément de $\mathbb{Z}/32\mathbb{Z}$ est inversible, si et seulement si, il est premier avec 32. On obtient les nombres suivants : 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31.

3. Pour calculer l'inverse de 15 dans $\mathbb{Z}/32\mathbb{Z}$, on utilise l'algorithme d'Euclide :
$32 = 2 \times 15 + 2$ donc $2 = 1 \times 32 - 2 \times 15$
$15 = 2 \times 7 + 1$ donc $1 = 15 - 7 \times 2 = 15 - 7(1 \times 32 - 2 \times 15)$
D'où $1 = 15 \times 15 - 7 \times 32$. On réduit modulo 32. Ceci donne $15 \times 15 = 1 \mod 32$ et donc l'inverse de 15 dans $\mathbb{Z}/32\mathbb{Z}$ est 15.

Exercice 4 : 1. On a $p - 1 \equiv 1 \mod 3$ et $q - 1 \equiv 1 \mod 3$, ce qui donne $(p-1)(q-1) \equiv 1 \mod 3$, donc $2(p-1)(q-1) \equiv 2 \mod 3$ et $2(p-1)(q-1) + 1 \equiv 0 \mod 3$.

2. $k = \varphi(pq) = (p-1)(q-1)$ car p et q sont premiers. D'après la question précédente, e est bien défini. On a $3e = 2(p-1)(q-1) + 1$, donc $3e \equiv 1 \mod (p-1)(q-1)$ et donc l'inverse de e dans $\mathbb{Z}/k\mathbb{Z}$ est 3.

3. (a) On a $n = 187 = 11 \times 17$. Ce qui donne $p = 11$ et $q = 17$. D'après la question précédente, l'inverse de 3 modulo $\varphi(n) = (p-1)(q-1)$ est $e = \frac{2(p-1)(q-1)+1}{3} = 107$. D'après la définition du RSA, on en déduit que la clé secrète de Bob est (11,17,107).

   (b) On a $C \equiv M^3 \mod n$ et donc $M \equiv C^{107} \mod n$. On va donc calculer $C^{107} \mod n = 9^{107} \mod 187$ à l'aide de l'algorithme d'exponentiation rapide. En base 2, on a $107 = (1101011)$.

i	b_i	Etapes du calcul
6	1	$1^2 \times 9$
5	1	$9^2 \times 9 = 729 = 168 \mod 187$
4	0	$168^2 = 28224 = 174 \mod 187$
3	1	$174^2 \times 9 = 272484 = 25 \mod 187$
2	0	$25^2 = 625 \mod 187$
1	1	$64^2 \times 9 = 36864 = 25 \mod 187$
0	1	$25^2 \times 9 = 5635 = 15 \mod 187$

On obtient finalement $M = 15$.