Enseignement Libre
Introduction à la Cryptographie
2008/2009

UNIVERSITÉ de Cergy-Pontoise

Corrigé de l'examen du 27 Avril 2009

Exercice 1 : 1. Dans le chiffrement par décalage, il y a 25 clés possibles qui correspondent au décalage pour chaque lettre (on ne considère pas le décalage par 0 qui ne modifie pas le message).

2. Dans le chiffrement affine, la clé est donnée par le couple (a, b) et l'on fait la tranformation $ax+b$, mod 26 où a et b sont éléments de $\mathbb{Z}/26\mathbb{Z}$. De plus on doit avoir a premier avec 26. Or $26 = 13\times 2$, donc $\varphi(26) = (13-1)(2-1) = 12$. Il y a donc 12 possibilités pour a et 26 pour b, ce qui donne 312, mais il faut enlever le couple $(1, 0)$ avec lequel on n'a aucun chiffrement. Il y a donc 311 clés.

3. Dans le chiffrement par substitution, on applique une permutation des 26 lettres de l'alphabet, ce qui donne 26 ! possibilités ; on enlève l'application identique qui ne modifie pas le message de départ. Cela fait donc 26 ! -1 clés.

Exercice 2 : Soit un entier N que l'on écrit en base 10 sous la forme : $N = \sum_{i=0}^{k} a_k 10^k$ où $a_k \in \{0, 1, \ldots, 8, 9\}$. Pour $k \in \mathbb{N}^*$, on a $10^k \equiv 1 \mod 9$. Or N est divisible par 9, si et seulement si, $N \equiv 0 \mod 9$ c'est à dire si et seulement si $\sum_{i=0}^{k} a_k 10^k \equiv 0 \mod 9$. D'après ce qui précède, on a $\sum_{i=0}^{k} a_k 10^k \equiv \sum_{i=0}^{k} a_k \mod 9$. On obtient bien le critère recherché.

Exercice 3 : Pour un régiment donné, on note X le nombre de soldats du régiment. Les conditions que l'on doit vérifier permettent d'écrire le système de congruences suivant :

$$\begin{cases} x \equiv 6 \mod 7 \\ x \equiv 10 \mod 11 \\ x \equiv 12 \mod 13 \end{cases}$$

puisque l'on a un homme en moins sur la dernière rangée. On résoud ensuite ce système de congruences à l'aide du théorème des restes chinois. Posons $m_1 = 7$, $m_2 = 11$ et $m_3 = 13$. Les m_i sont deux à deux premiers entre eux. On peut donc appliquer le théorème. Soit $M = m_1 \times m_2 \times m_3 = 1001$. On a alors $M_1 = M/m_1 = 143$, $M_2 = M/m_2 = 91$ et $M_3 = M/m_3 = 77$. On calcule ensuite $y_1 = M_1^{-1} \mod 7 = 5$, $y_2 = M_2^{-1} \mod 11 = 4$ et $y_3 = M_3^{-1} \mod 13 = 12$. On obtient ensuite une unique solution du système modulo 1001. Cette solution est donnée par $6\times 143\times 5 + 10\times 91\times 4 + 12\times 77\times 12 = 19018 \mod 1001$. Puisque $19018 \equiv 1000 \mod 1001$, ceci montre que la méthode proposée permet de vérifier que le régiment est complet. Remarque : Vérifier uniquement que 1000 est solution su système ne suffit pas. La résolution du système permet de montrer l'unicicté de la solution modulo 1001 et donc que le régiment est complet puisque pour les autres possibilités, il faut ajouter des multiples de 1001.

Exercice 4 : 1. On a $35 = 7 \times 5$, $n = 35$ est bien le produit de 2 nombres premiers. De plus, $\varphi(n) = 6 \times 4 = 24$. Puisque 5 est permier avec 24, on peut prendre 5 comme exposant public et $(35, 5)$ est une clé publique valide pour le RSA. Pour obtenir l'exposant privé, on calcule $5^{-1} \mod 24$ et on obtient 5. La clé privée associée est donnée par $(5, 7, 5)$.

2. Montrons comment est décodée la lettre I. Dans le tableau, I correspond au chiffre 12. La clé privée étant $(5, 7, 5)$, il faut calculer $12^5 \mod 35$. On peut utiliser l'algorithme d'exponontiation rapide. En base 2, on a $5 = (1, 0, 1)$. On fait donc le calcul suivant :

i	c_i	Etapes du calcul
2	1	$1^2 \times 12 = 12 \mod 35$
1	0	$12^2 = 144 = 4 \mod 35$
0	1	$4^2 \times 12 = 192 = 17 \mod 35$

On obtient donc 17 qui correspond à la lettre L. On continue ainsi avec les autres lettres. On a les correspondances suivantes :

I	$\rightarrow$	12	$\rightarrow$	17 $\rightarrow$	L
A	$\rightarrow$	1	$\rightarrow$	1 $\rightarrow$	A
M	$\rightarrow$	18	$\rightarrow$	23 $\rightarrow$	P
E	$\rightarrow$	6	$\rightarrow$	6 $\rightarrow$	L
U	$\rightarrow$	31	$\rightarrow$	26 $\rightarrow$	R
S	$\rightarrow$	27	$\rightarrow$	27 $\rightarrow$	S
B	$\rightarrow$	2	$\rightarrow$	32 $\rightarrow$	V
Q	$\rightarrow$	24	$\rightarrow$	19 $\rightarrow$	N
X	$\rightarrow$	33	$\rightarrow$	3 $\rightarrow$	C
L	$\rightarrow$	17	$\rightarrow$	12 $\rightarrow$	I

Le texte clair est : la persévérance paie.

3. Cete manière d'utiliser la correspondance entre les lettres et le chiffres et d'appliquer le RSA lettre par lettre affaiblit le système de chiffrement car un attaquant peut mettre en mémoire le chiffrement de chaque lettre grâce à la clé publique et regarder les valeurs transmises. Il n'a pas besoin de connaître la clé.

Exercice 5 : 1. On a $N = 17 \times 23 = 391$, puis $\varphi(N) = (P-1)(Q-1) = 352$.

2. On a $pgcd(11, 352) = 11$. Donc $E = 11$ n'est pas premier avec 352. Il ne peut pas être pris comme exposant public de signature. On a aussi $pgcd(13, 352) = 1$. Donc $E = 13$ peut être choisi comme exposant public de signature. De plus, $532 = 13 \times 27 + 1$, d'où $1 = 352 - 27 \times 13$. Si on réduit modulo 352, puisque l'exposant secret pour la signature est l'inverse de 13 modulo 352, on obtient $D = -27 \mod 352 = 325$. La clé secrète de signature est $(17, 23, 325)$ et la clé publique est $(391, 13)$.

3. Alice calcule d'abord $100^{325} \mod 391$. En base 2, on a $325 = 2^8 + 2^6 + 2^2 + 1$. On utilise ensuite l'algorithme d'exponentiation rapide :

i	c_i	Etapes du calcul
8	1	$1^2 \times = 100 \mod 391$
7	0	$100^2 = 10000 = 225 \mod 391$
6	1	$225^2 \times 100 = 223 \mod 391$
5	0	$223^2 = 72 \mod 391$
4	0	$72^2 = 101 \mod 391$
3	0	$101^2 = 35 \mod 391$
2	1	$35^2 \times 100 = 117 \mod 391$
1	0	$117^2 = 4 \mod 391$
0	1	$4^2 \times 100 = 36 \mod 391$

La signature de 100 est donc 36. Alice envoie à Bob le couple $(100, 36)$.

4. Bob prend la clé publique de signature d'Alice. Il calcule $36^{13} \mod 391$ et vérifie qu'il obtient bien 100.