Université de Cergy-Pontoise **2006-2007**
Introduction à la cryprographie **UE libre**

Corrigé de l'examen du 23 Avril 2007

Exercice 1 : 1. Le chifrement affine est défini par la fonction :

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{Z}/26\mathbb{Z} = & \rightarrow & Z/26\mathbb{Z} \\ x & \rightarrow & a.x+b \end{array} \right.$$

où a et b sont des constantes. On a donc $\varphi(x) = a.x + b \mod 26$.

2. L'opération de déchiffrement est possible si a est inversible dans $\mathbb{Z}/26\mathbb{Z}$ c'est à dire si a est premier avec 26.

3.

Texte clair	R	E	N	D	E	Z	V	O	U	S	A	U	M	E	T	R	O
Texte clair dans $\mathbb{Z}/26\mathbb{Z}$	17	4	13	3	4	25	21	14	20	18	0	20	12	4	19	17	14
Texte chiffré dans $\mathbb{Z}/26\mathbb{Z}$	4	17	18	14	17	2	16	21	13	7	5	13	15	17	10	4	21
Texte chiffré	E	R	S	O	R	C	Q	V	N	H	F	N	P	R	K	E	V

Exercice 2 : On obtient le système :

$$\left\{ \begin{array}{lll} x = & 0 & \mod 11 \\ x = & 5 & \mod 9 \\ x = & 8 & \mod 13 \end{array} \right.$$

On utlise alors le théorème des restes chinois avec $m_1 = 11$, $m_2 = 9$, $m_3 = 13$. D'où $M = m_1 \cdot m_2 \cdot m_3 = 1287$. On obtient alors $M_1 = \frac{M}{m_1} = 117$, $M_2 = \frac{M}{m_2} = 143$ et $M_3 = \frac{M}{m_3} = 99$. On a alors $y_1 = M_1^{-1} \mod 11 = 7^{-1} \mod 11 = 8$, puis $y_2 = M_2^{-1} \mod 9 = 8^{-1} \mod 9 = 8$ et $y_3 = M_3^{-1} \mod 13 = 8^{-1} \mod 13 = 5$. On sait que l'on a une unique solution $\mod M$, donnée par $X = 0 \times 117 \times 8 + 5 \times 143 \times 8 + 8 \times 99 \times 5 \mod 1287$. D'où $X = 9680 \mod 1287$. de plus, X est compris entre 1000 et 3000. On obtient : $X = 1958$.

Exercice 3 : 1. En base 2, on a : $103 = 1100111$

2. $143 = 13 \times 11$. On pose $p = 13$ et $q = 11$, p et q sont premiers.
3. $\varphi(143) = (p-1)(q-1) = 12 \times 10 = 120$. L'indicateur d'Euler donne le nombre d'éléments inversibles modulo 143. Il y a donc $143 - 120 = 23$ élements compris entre 0 et 142 qui ne sont pas inversibles modulo 143.
4. Théorème d'Euler-Fermat : Soit n un entier, si x est premier avec n, alors $x^{\varphi(n)} = 1 \mod n$. Donc pour x premier avec 143, $x^{\varphi(143)} = 1 \mod 143$, c'est à dire $x^{120} = 1 \mod 143$.
5. En utilisant l'algorithme d'Euclide étendu, on obtient $103^{-1} \mod 120 = 7$.
6. En utilisant l'algorithme d'exponentiation rapide, on obtient $27^{103} \mod 143 = 92$.
7. Dans le RSA, si x est le message clair et $(n = 143, e = 7)$ est la clé publique, le message chiffré est $y = x^7 \mod 143$. Ici, on a alors $y = x^7 \mod 143 = 27$. Alice qui connait la décomposition de n en facteurs premiers possède donc la clé secrète $(p = 13, q = 11, d)$ où d est la clé de déchiffrement et est donnée par $d = e^{-1} \mod (p-1)(q-1)$. Ici, on obtient $d = 7^{-1} \mod 120$. D'après la question 5, on a $d = 103$. On retrouve alors le texte clair en calculant $y^{103} \mod 143$ c'est à dire $27^{103} \mod 143$. D'après la question 6, le texte clair est donc 92.