Université Bordeaux 1 — **MHT633 – Arithmétique et Cryptologie**
Mathématiques — Année 2008–2009

Partiel du Lundi 16 mars 2009 (Correction)

Exercice 1 – [Chiffrement affine]

1) A est un ensemble fini, donc une application de A dans A est bijective si et seulement si elle est injective, ou encore si et seulement si elle est surjective. Pour que e_K soit inversible, il faut par exemple que e_K soit surjective, donc que $aA + b = A$ ce qui équivaut encore à $aA = A$. Mais alors il existe $x \in A$ tel que $ax = 1$ ce qui prouve que a est inversible.

Réciproquement, si a est inversible, alors $x \mapsto ax$ est une injection de A dans A, elle est donc bijective et inversible. La condition nécessaire et suffisante cherchée est donc

$$a \in A^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}\,.$$

2) On est amené à résoudre dans $A = \mathbb{Z}/26\mathbb{Z}$ le système

$$\left\{\begin{array}{rcl} 20a + b & = & 14 \\ 13a + b & = & 17. \end{array}\right.$$

Par différence on trouve $7a = 23$. Il faut calculer l'inverse de 7 dans A. L'algorithme d'Euclide étendu conduit à la relation de Bezout

$$7 \times 15 - 26 \times 4 = 1.$$

On en déduit que l'inverse de 7 est 15, ce qui donne $a = 15 \times 23 = 7$. En réinjectant cette valeur dans l'une des deux équations initiales on obtient $b = 4$. La réponse est donc $(a, b) = (7, 4)$.

3) On est conduit à résoudre dans A l'équation $7x+4 = n$, avec $n \in \{6, 9, 4, 18, 7\}$. Par multiplication par l'inverse de 7 qui est 15, on obtient $x+8 = 15n$, ou encore $x = 15n - 8$, et l'on obtient $x = 4$, 23, 0, 2, 19. On en déduit le clair « EXACT ».

Exercice 2 – [Hill affine]

1) Posons $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ et $B = (x, y)$. On est conduit à résoudre le système suivant, à inconnues dans A :

$$\left\{\begin{array}{rcll} 18a + 8c + x & = & 25 & (1) \\ 18b + 8d + y & = & 0 & (2) \\ 12a + 15c + x & = & 4 & (3) \\ 12b + 15d + y & = & 25 & (4) \\ 11a + 4c + x & = & 16 & (5) \\ 11b + 4d + y & = & 16 & (6) \end{array}\right. .$$

Par différences, (1)−(3), (3)−(5), puis (2)−(4), (4)−(6), donnent respectivement

$$\left\{\begin{array}{rcll} 6a + 19c & = & 21 & (1') \\ a + 11c & = & 14 & (2') \end{array}\right. , \qquad \left\{\begin{array}{rcll} 6b + 19d & = & 1 & (3') \\ b + 11d & = & 9 & (4') \end{array}\right. .$$

En calculant $6 \times (2') - (1')$, on en déduit $21c = 11$, ou encore $-5c = 11$. L'inverse de -5 dans A est 5, et on obtient $c = 5 \times 11 = 3$ puis, par $(2')$, $a = 7$; De même, on obtient $(b, d) = (6, 5)$. En reportant dans (1) et (2), on trouve $(x, y) = (5, 8)$. La clé est donc

$$K = \left(\begin{pmatrix} 7 & 6 \\ 3 & 5 \end{pmatrix}, (5, 8) \right).$$

2) On cherche $(u, v) \in A^2$ tel que $(3, 12) = (u, v)M + B$, ou encore

$$\begin{cases} 3 &= 7u + 3v + 5 \quad (7) \\ 12 &= 6u + 5v + 8 \quad (8) \end{cases}$$

En effectuant $5 \times (7) - 3 \times (8)$, on obtient $5 = 17u + 1$ d'où $17u = 4$. L'inverse de 17 dans A est 23, d'où on tire $u = 14$.

En reportant dans (7) cela donne $3v = 4$. L'inverse de 3 dans A est 9 et l'on a finalement $v = 10$. On a donc $(u, v) = (14, 10)$ et le clair recherché est « OK ».[1]

Exercice 3 – [Pohlig-Hellman]

1) On veut que l'équation $m^e = 1$ n'ait pas d'autre solution que $m = 1$. Puisque m est forcément non nul, et que $(\mathbb{Z}/29\mathbb{Z})^*$ est cyclique, d'ordre 28, m est de la forme α^k pour une racine primitive α (un élément d'ordre 28). L'équation $m^e = 1$ devient $ke \equiv 0 \pmod{28}$, qui n'a pas d'autre solution que $k = 0$ ssi e est inversible modulo 28. On obtient $e \in \{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}$.

2) On cherche e tel que

$$2^e = 14 \bmod 29.$$

Les puissances successives de 2 dans $\mathbb{Z}/29\mathbb{Z}$ sont $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 3$, $2^6 = 6$, $2^7 = 12$, $2^8 = 24$, $2^9 = 19$, $2^{10} = 9$, $2^{11} = 18$, $2^{12} = 7$, $2^{13} = 14$.

Si on y rajoute l'équation $2^{14} = 28$, ce calcul montre que 2 est racine primitive modulo 29. En effet si ce n'était pas le cas, 2 serait d'ordre $\leqslant 14$ mais aucune des puissances 2^i ne vaut 1, pour $1 \leqslant i \leqslant 14$. On en déduit l'unique solution $e = 13$.

3) La lettre 0 $(= A)$ ne permet pas de retrouver e (on a $0^e = 0$ pour tout e). On peut donc supposer qu'une lettre convenable est dans $(\mathbb{Z}/29\mathbb{Z})^*$, donc de la forme α^x, pour α une racine primitive d'ordre 28 (2 par exemple, d'après la première question). Elle se code en un élément non nul, disons α^y, tel que $\alpha^{ex} = \alpha^y$, soit $ex \equiv y \pmod{28}$. Ceci permet de retrouver e si et seulement si x est inversible modulo 28. Par la fin de la première question, les 2^x convenables sont

$$2, 8, 3, 19, 18, 14, 27, 21, 26, 10, 11, 15,$$

correspondant aux lettres $C, I, D, T, S, O, V, K, L, P$. Noter qu'aucune lettre ne correspond à 26 et 27.

[1] Autre méthode : la fonction de déchiffrement est $X \mapsto (X - B)M^{-1}$; on applique la formule

$$M^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

On trouve $ad - bc = 17$, dont l'inverse dans $(\mathbb{Z}/26Z)^*$ est 23 ; soit $M^{-1} = \left(\begin{smallmatrix} 11 & 18 \\ 9 & 5 \end{smallmatrix}\right)$. On obtient le même résultat.