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

Examen du Lundi 11 mai 2009, 8:30 – 10:00 (Correction)

Exercice 1 –
Soient p, q deux grands nombres premiers distincts et $N = pq$. On pose $\mathcal{M} = \mathcal{C} = \mathbb{Z}/N\mathbb{Z}$. $\mathcal{K}$ est l'ensemble des triplets (N, e, d), où $ed \equiv 1 \pmod{\varphi(N)}$; ici $\varphi(N)$ est l'indicatrice d'Euler et vaut $(p-1)(q-1)$.

Pour une clé $K \in \mathcal{K}$ on définit les fonctions de chiffrement

$$\begin{aligned} e_K : \mathcal{M} &\to \mathcal{C} \\ m &\mapsto m^e, \end{aligned}$$

et de déchiffrement

$$\begin{aligned} d_K : \mathcal{C} &\to \mathcal{M} \\ m &\mapsto m^d. \end{aligned}$$

Exercice 2 – Comme dans la méthode de Dixon, on a $N \mid (12534-1)(12534+1)$ et on peut espérer factoriser N en calculant $\operatorname{pgcd}(N, 12534 \pm 1)$. C'est bien le cas, fournissant les facteurs 109 et 151.

Exercice 3 –

1) Puisque $\operatorname{pgcd}(p, q) = 1$ (d'après la définition de RSA), le Lemme Chinois donne l'isomorphisme d'anneaux $\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$; il suffit donc de vérifier que $x \equiv y^d \pmod{p}$ et $x \equiv y^d \pmod{q}$ pour avoir la congruence voulue modulo N. On se contente de montrer la congruence mod p, l'autre étant analogue.

On a $x \equiv M_p q x_p \pmod{p} \equiv x_p \pmod{p}$; il faut donc démontrer que $y^d \equiv y^{d_p} \pmod{p}$. Par division euclidienne $d = k(p-1) + d_p$ pour un certain entier k, soit $y^d = y^{k(p-1)} y^{d_p}$; si $y \not\equiv 0 \pmod{p}$, le petit théorème de Fermat dit que $y^{p-1} \equiv 1 \pmod{p}$ et le résultat suit.

Il ne nous reste plus que le cas dégénéré $y \equiv 0 \pmod{p}$ à traiter, et on aimerait que la congruence $y^d \equiv y^{d_p} \pmod{p}$ se réduise à $0 \equiv 0 \pmod{p}$, ce qui sera vrai si $d \neq 0$ et $d_p \neq 0$. On va voir que c'est effectivement le cas si $p \neq 2$:

- On sait que $d \neq 0$, sinon le déchiffrement renverrait 1 quel que soit le chiffré ! Plus formellement, celà suit de la propriété $\operatorname{pgcd}(d, \varphi(N)) = 1$ des clés RSA, qui empêche $d = 0$ sinon ce pgcd serait $\varphi(N) > 1$.
- De même, on a $\operatorname{pgcd}(d, (p-1)(q-1)) = 1$, ce qui implique $\operatorname{pgcd}(d, p-1) = \operatorname{pgcd}(d_p, p-1) = 1$. Donc $d_p \neq 0$ *sauf* si $p - 1 = 1$, soit $p = 2$.

On vérifie directement que l'identité proposée est fausse si $p = 2$ ou $q = 2$ et $y \equiv 0 \pmod{2}$ (à cause de la définition $0^0 = 1 \neq 0$). Ce cas est exclus par les propriétés attendues du système : $N = pq$ doit être difficile à factoriser.

2)

a) La difficulté à factoriser un entier est liée à la taille de son plus petit facteur premier : c'est évident pour la méthode naïve par division successive, ce n'est pas vrai si on utilise la méthode de Dixon (mais c'est vrai pour beaucoup d'autres algorithmes

modernes, par exemple la méthode des courbes elliptiques). On a admis en cours qu'un « entier RSA » était difficile à factoriser pour cette raison.

b) D'après la question précédente, p et q sont de l'ordre de $N^{1/2}$ (ils sont du même ordre de grandeur et leur produit est N), donc leur taille ($\approx \log(N^{1/2})$) est la moitié de celle de N.

L'entier d est défini modulo $\varphi(N)$, qui est de l'ordre de N ; les entiers d_p et d_q sont définis modulo $p-1$ et $q-1$, qui sont de l'ordre de $N^{1/2}$.

Ceci n'implique pas *nécessairement* que d_p et d_q sont de taille deux fois plus faible que d, mais c'est déjà le cas si d est choisi proche de N. De façon générale, un entier modulo M tiré uniformément au hasard (donc pris dans $[0, M-1]$) est de taille proche de celle de M avec forte probabilité.

c) À part les initialisations et le recollement par Lemme Chinois, le coût des calculs est celui de l'exponentiation $y \mapsto y^d$ d'une part, et des 2 exponentiations $y \mapsto y^{d_p}$, $y \mapsto y^{d_q}$ d'autre part.

Le calcul $y \mapsto y^{d_p}$ effectue des multiplications et divisions portant sur des opérandes de taille 2 fois plus faible (taille de p au lieu de taille de N), soit un gain d'un facteur 4. L'exposant est lui aussi de taille 2 fois plus faible, soit un gain d'un facteur 8 au total.

Le raisonnement est le même pour le calcul modulo q ; comme on doit effectuer deux exponentiations (mod p et mod q) au lieu d'une seule (mod N), le gain total est donc d'un facteur 4.

Exercice 4 –

1) T n'a pas de racine — car $T(0) = T(1) = 1$ — et n'est pas divisible par l'unique polynôme irréductible de degré 2 sur $\mathbb{F}_2$, à savoir $X^2 + X + 1$; il est donc irréductible.

2) $\mathbb{F}$ est de cardinal $2^{\deg T} = 16$, donc G est de cardinal 15 : on enlève 0.

3) On retourne (c_1, c_2) avec $c_1 = X^3$ et $c_2 = (X^2+1)(X^2)^3 \equiv X^3 + 1 \pmod{T}$.

4) Il faut calculer $(X^3 + X + 1)(X^2 + 1)^{-1}$ dans $\mathbb{F}$. Par l'algorithme d'Euclide étendu, on obtient $(X^2 + 1)^{-1} \equiv X^3 + X + 1 \pmod{T}$; le clair est donc

$$(X^3 + X + 1)^2 \equiv X^3 + 1 \pmod{T}.$$