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

Examen du Lundi 11 mai 2009, 8:30 – 10:00
Durée 1h30. Documents interdits.

Exercice 1 – Définir le procédé de chiffrement RSA, et indiquer comment il se déchiffre. Indiquer en particulier les ensembles $\mathcal{M}$ (messages), $\mathcal{C}$ (chiffrés), $\mathcal{K}$ (clés), ainsi que pour, une clé $K = (N, e, d) \in \mathcal{K}$, les fonctions de chiffrement e_K et de déchiffrement d_K.
Indiquer aussi les relations que doivent vérifier N, e, d.

Exercice 2 – Soit $N = 16459$. En remarquant que $12534^2 \equiv 1^2 \pmod{N}$, factoriser N par un calcul de pgcd.

Exercice 3 – Pour accélérer le déchiffrement RSA on utilise le théorème des restes chinois. Supposons que $d_K(y) = y^d$ et $N = pq$; on définit $d_p = d \pmod{p-1}$, $d_q = d \pmod{q-1}$, $M_p = q^{-1} \pmod{p}$ et $M_q = p^{-1} \pmod{q}$; puis on effectue les opérations suivantes :

$$x_p \leftarrow y^{d_p} \pmod{p}, \quad x_q \leftarrow y^{d_q} \pmod{q}, \quad x \leftarrow M_p q x_p + M_q p x_q \pmod{N}.$$

1) Montrer que $x = y^d \pmod{N}$.

2) On rappelle que la taille d'un entier est le nombre de bits de sa décomposition en base 2. On suppose que multiplications et divisions s'exécutent en temps quadratique (c'est-à-dire que doubler la taille des opérandes conduit à un calcul 4 fois plus lent) et on rappelle que le calcul de y^d nécessite un nombre de multiplications en $O(\log d)$ (c'est-à dire qu'un exposant de taille double nécessite deux fois plus de multiplications).

a) Expliquer pourquoi dans le cadre de RSA, il est raisonnable de supposer que p et q sont de même taille.

b) Expliquer pourquoi on peut s'attendre à ce que la taille de d_p et d_q soit deux fois plus faible que la taille de d.

c) Justifier pourquoi la méthode de calcul ci-dessus est essentiellement 4 fois plus rapide que la méthode directe, qui ne ferait que des calculs modulo N.

Exercice 4 – On rappelle le principe du chiffrement ElGamal dans le groupe multiplicatif G : la clé publique est $g, h \in G$, la clé privée est un $x \in \mathbb{Z}$ tel que que $h = g^x$.

Chiffrement: soit $m \in G$ le message à chiffrer

(1) On tire $k \in \mathbb{Z}/\left|G\right|\mathbb{Z}$, puis on calcule $c_1 = g^k$.
(2) On calcule $c_2 = mh^k$.
(3) On retourne (c_1, c_2).

Déchiffrement: soit (c_1, c_2) le texte chiffré, le clair s'obtient par la formule $m := c_2 c_1^{-x}$. (On suppose la clé privée x connue !)

1) Soit $T(X) = X^4 + X + 1 \in \mathbb{F}_2[X]$. Montrer que T est irréductible.

On note $\mathbb{F}$ le corps fini $\mathbb{F}_2[X]/(T)$ et on choisit pour la suite $G = \mathbb{F}^*$.

2) Quel est le cardinal du groupe G.

3) On connaît $g = X$, $h = X^2$ et on tire $k = 3$. Chiffrer le message $X^2 + 1 \bmod T$.

4) Déchiffrer le message $(X^2 + 1 \bmod T, X^3 + X + 1 \bmod T)$ si $x = 1$.