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

FEUILLE D'EXERCICES n° 7
Cryptographie asymétrique (3)

Exercice 1 – [Crible quadratique]
On désire factoriser un entier impair N, en utilisant une variante de l'algorithme de Dixon :

(1) On choisit une base de facteurs $\mathcal{B} = \{-1, p_1, \ldots, p_k\}$ où les p_i sont premiers.

(2) Pour chaque $j \in \mathbb{N}$, on pose $t = \pm j$, $x_t = \left\lfloor \sqrt{N} \right\rfloor + t$ et on calcule $y_t = x_t^2 - N$ jusqu'à ce qu'on trouve $k+2$ tels nombres se décomposant entièrement sur $\mathcal{B}$. Pour chaque tel t on a $y_t = \pm \prod_{i=1}^{k} p_i^{a_{i,t}}$, et l'on forme le $(k+1)$-uplet $(v_{0,t}, v_{1,t}, \ldots, v_{k,t})$ où $v_{0,t} = 0$ si $y_t > 0$, $v_{0,t} = 1$ si $y_t < 0$ et $v_{i,t} = a_{i,t} \bmod 2$ si $i \geqslant 1$.

(3) On cherche un sous-ensemble S des valeurs de t obtenues précédemment tel que pour tout $i = 0, 1, \ldots, k$, on ait $\sum_{t \in S} v_{i,t} \equiv 0 \bmod 2$. Alors si $x = \prod_{t \in S} x_t$ et $y^2 = \prod_{t \in S} y_t$ on a $x^2 \equiv y^2 \bmod N$; si de plus $x \not\equiv \pm y \bmod N$, alors $(x \pm y, N)$ fournit un facteur non trivial de N.

1) Pourquoi peut-on exclure de $\mathcal{B}$ les p tels que N ne soit pas résidu quadratique modulo p ?

2) Soit $N = 30167$ et $\mathcal{B} = \{-1, 2, 7, 11, 17, 29, 31, 37, 41, 43, 53, 67\}$. On calcule

t	x_t	y_t
0	173	$-2 \cdot 7 \cdot 17$
-1	172	$-11 \cdot 53$
-5	168	$-29 \cdot 67$
5	178	$37 \cdot 41$
-6	167	$-2 \cdot 17 \cdot 67$
7	180	$7 \cdot 11 \cdot 29$
11	184	$7 \cdot 17 \cdot 31$

t	x_t	y_t
14	187	$2 \cdot 7^4$
-15	158	$-11 \cdot 43$
-17	156	$-7^3 \cdot 17$
18	191	$2 \cdot 7 \cdot 11 \cdot 41$
-23	150	$-11 \cdot 17 \cdot 41$
28	201	$2 \cdot 7 \cdot 17 \cdot 43$

Factoriser N.

Exercice 2 – [Méthode $p-1$ de Pollard]
Si $B > 1$, un entier N est dit *B-friable* si pour tout premier q et tout s tel que $q^s \mid N$, alors $q^s \leqslant B$. On considère l'algorithme suivant :

Entrées: N un entier impair, $B > 2$ une borne de friabilité.

1: $a \leftarrow 2$.
2: **pour** j from 2 to B **faire**
3: $\quad a \leftarrow a^j \bmod N$
4: $d \leftarrow (a-1, N)$
5: **si** $1 < d < N$ **alors**
6: $\quad$ on renvoie d.
7: On renvoie « Échec ».

1) Que vaut a à la fin de la boucle **for** ?

2) Supposons que p premier divise N et que $p-1$ soit B-friable. Montrer que p divise d et que l'algorithme retourne un facteur non trivial de N sauf si $a = 1$.

3) Appliquer avec $N = 13927189$ et $B = 14$.

4) Écrire un autre algorithme qui s'appuiera sur le calcul d'un autre a ne faisant appel qu'aux q premiers $\leqslant B$ et aux exposants $m_q = \lfloor \log N / \log q \rfloor$.

Exercice 3 – [Le chiffrement de ElGamal]
On rappelle le principe du chiffrement de ElGamal :

Clé publique	(p, α, β) où p premier, α d'ordre q dans $\mathbb{F}_p^*$, $\beta \in \langle\alpha\rangle$, $\beta \neq 1$.
Clé privée	$a \in [1 \dots q-1]$ tel que $\beta = \alpha^a \mod p$.
Chiffrement de $m < p$	$E(m) = (\alpha^k, m\beta^k)$ où $1 \leqslant k < q$ est aléatoire.
Déchiffrement de $c = (r, t)$	$D(c) = tr^{-a} \mod p$.

1) La clé publique de Bob est $p = 17$, $\alpha = 3$, $\beta = 10$. Aidez Alice à chiffrer le message $m = 5$ et Bob à déchiffrer $(7, 6)$.

2) Montrez que $D(E(m)) = m$.

3) Montrez qu'un attaquant peut déchiffrer tous les messages dès qu'il sait calculer le log en base α de β.

4) Montrez qu'un attaquant peut déchiffrer $c = (r, t)$ dès qu'il sait calculer le log en base α de r.

5) Pourquoi faut-il que l'ordre de α modulo p soit un « grand » nombre q ?

6) Quel avantage procure l'utilisation du nombre aléatoire k ?

7) Alice chiffre deux messages m_1 et m_2 avec le même k. Montrez que, si Oscar connaît m_1, alors il connaît aussi m_2.

Exercice 4 – [UNE ATTAQUE SUR RSA : MODULE COMMUN]
On rappelle le principe du chiffrement RSA :

Clé publique	(N, e) où $N = pq$ et $(e, \varphi(N)) = 1$
Clé privée	d tel que $ed \equiv 1 \mod (p-1)(q-1)$
Chiffrement de $m < N$	$E(m) = m^e \mod N$
Déchiffrement de c	$D(c) = c^d \mod N$

Bob et Catherine ont choisi le même module RSA N. Leurs exposants publics e_B et e_C sont distincts.

1) Expliquez pourquoi Bob peut déchiffrer les messages reçus par Catherine et réciproquement.

2) On suppose que $(e_B, e_C) = 1$ et qu'Alice envoie un même message chiffré à Bob et à Catherine. Expliquez comment l'attaquant Oscar peut obtenir m.

Exercice 5 – [UNE ATTAQUE SUR RSA : PETIT EXPOSANT PUBLIC COMMUN]
On suppose que k personnes $B_1, \ldots, B_k$ ont pour exposant public RSA $e = 3$ avec des modules respectifs N_i, $1 \leqslant i \leqslant k$ deux à deux premiers entre eux. Si Alice envoie un même message m à tous les B_i, montrez qu'un attaquant peut déterminer m^3 modulo $P := \prod_{i=1}^{k} n_i$; en déduire qu'il peut calculer m si $P > m^3$.