TD

Attaque de Wiener sur RSA avec des petites clefs publiques

I. Préliminaires

On rappelle que dans le cryptosystème RSA, la clef de chiffrement publique est un couple d'entiers (N, e), et la clef secrète de déchiffrement un entier d tel que $de = 1 \bmod \varphi(N)$; le chiffrement et le déchiffrement se font à l'aide des fonctions $m \mapsto m^e$ et $c \mapsto c^d$ in $\mathbb{Z}/N\mathbb{Z}$ respectivement. Comme le coût de ces opérations dépend de e et d, il est tentant de choisir de petits exposants e et d pour accélérer les calculs.

- Il est assez standard de prendre e petit ; choisir $e = 3$ peut poser problème (cf attaques broadcast et Coppersmith), mais il est très courant de prendre $e = 65537$. Cependant ce choix ne permet d'accélérer que la partie chiffrement.
- Pour accélérer la partie déchiffrement on peut vouloir prendre d également petit. On va voir cependant dans ce TD que ce choix compromet fortement la sécurité du cryptosystème RSA.

1. Expliquer pourquoi prendre d vraiment petit (par exemple $d < 100000$) est une mauvaise idée.
2. Est-il possible d'avoir à la fois e et d petits (disons $< N^{1/3}$) ?

II. Pré-requis sur les fractions continues

Une *fraction continue* finie est une expression de la forme

$$[a_0, a_1, a_2, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

avec $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{N}^*$ pour $i > 0$, et $a_n > 1$.

3. Soit $x = a/b \in \mathbb{Q}$ avec $a \wedge b = 1$ et $b > 0$. Soit (q_i) (resp. (r_i)) la suite des quotients (resp. restes) dans l'algorithme d'Euclide appliqué à a et b : $r_0 = a$, $r_1 = b$, et pour tout $i > 0$ tel que $r_i \neq 0$, la division euclidienne de r_{i-1} par r_i est $r_{i-1} = q_i r_i + r_{i+1}$.
   Montrer que $x = [q_1, q_2, \ldots, q_N]$ où r_N est le dernier reste non nul.
4. Montrer que le développement en fraction continue d'un entier rationnel est unique.

Soit $[a_0, a_1, \ldots, a_n]$ le développement en fraction continue d'un rationnel x. Pour tout $0 \leq i \leq n$, le i-ème *convergent* de x est $[a_0, a_1, \ldots, a_i]$. Pour pouvoir calculer les convergents successifs, on introduit (h_i), (k_i) deux suites d'entiers satisfaisant les relations

$$h_0 = a_0,\ h_1 = a_0 a_1 + 1,\ \text{et } h_i = a_i h_{i-1} + h_{i-2} \text{ pour tout } 2 \leq i \leq n,$$

$$k_0 = 1,\ k_1 = a_1,\ \text{et } k_i = a_i k_{i-1} + k_{i-2} \text{ pour tout } 2 \leq i \leq n.$$

(Il peut être utile de poser $h_{-1} = 1$, $h_{-2} = 0$, $k_{-1} = 0$ et $k_{-2} = 1$ de façon à étendre la relation de récurrence à tout $i \geq 0$.)

5. Montrer par récurrence que $k_i h_{i-1} - h_i k_{i-1} = (-1)^i$ pour tout $i \geq 1$. En déduire que h_i et k_i sont premiers entre eux.

6. Pour $0 \leq i \leq n$, soit $f_i : \mathbb{R} \to \mathbb{R}$ une fonction telle que

$$f_i(t) = a_0 + \cfrac{1}{\ddots + \cfrac{1}{a_{i-2} + \cfrac{1}{a_{i-1} + \cfrac{1}{t}}}}.$$

   (a) Montrer par récurrence que $f_i(t) = \dfrac{h_{i-1}t + h_{i-2}}{k_{i-1}t + k_{i-2}}$

   (b) Montrer que le i-ème convergent $[a_0, a_1, \ldots, a_i]$ est égal à la fraction irréductible $\dfrac{h_i}{k_i}$.

7. (a) En exprimant $\dfrac{h_N}{k_N} - \dfrac{h_i}{k_i}$ comme une somme téléscopique, montrer que $\dfrac{h_N}{k_N} - \dfrac{h_i}{k_i} = \displaystyle\sum_{j=i}^{N-1} \frac{(-1)^j}{k_j k_{j+1}}$.

   (b) Montrer l'inégalité $\left| x - \dfrac{h_i}{k_i} \right| \leq \dfrac{1}{k_i k_{i+1}} < \dfrac{1}{k_i^2}$.

8. Soient $p, q \in \mathbb{Z} \times \mathbb{N}^*$ deux entiers tels que $\left| x - \dfrac{p}{q} \right| < \left| x - \dfrac{h_i}{k_i} \right|$. Montrer que $q > k_{i+1}/2$.

Ce dernier résultat peut être amélioré : il est possible de montrer qu'en fait $q > k_i$. Les convergents sont intéressants car ils fournissent les "meilleures" approximations de x, au sens où toute fraction plus proche de x que $\frac{h_i}{k_i}$ doit avoir un plus grand dénominateur. Il y a également une réciproque partiellement vraie du résultat de la question 7.(b):

Théorème. *Soit $\dfrac{p}{q}$ un rationnel tel que $\left| x - \dfrac{p}{q} \right| < \dfrac{1}{2q^2}$. Alors $\dfrac{p}{q}$ est un convergent de x, i.e. il existe $i \in \mathbb{N}$ tel que $\dfrac{p}{q} = \dfrac{h_i}{k_i}$.*

Ce résultat sera utilisé (sans être prouvé) dans la section suivante.

III. Attaque de Wiener

Soit $N = pq$ un entier de type RSA, et $e, d \in [\![1, \varphi(N) - 1]\!]$ tels que $ed = 1 \bmod \varphi(N)$. Soit $k \in \mathbb{N}$ tel que $ed = 1 + k\varphi(N)$. L'idée de l'attaque de Wiener est que $\dfrac{e}{N} \approx \dfrac{e}{\varphi(N)} \approx \dfrac{k}{d}$. En particulier si d est petit et $\varphi(N)$ n'est pas trop éloigné de N, la fraction $\dfrac{k}{d}$ est une bonne approximation de $\dfrac{e}{N}$, qui est connu, et pourra être retrouvé en en calculant le développement en fractions continues. De façon plus précise, on a :

Théorème (Wiener)**.** *Si $p < q < 2p$ et $d \leq \frac{1}{3}N^{1/4}$, alors $\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}$. En particulier, $\frac{k}{d}$ est un convergent dans le développement en fractions continues de $\frac{e}{N}$.*

9. (Preuve du théorème)
   (a) Montrer que $p + q < 3\sqrt{N}$.
   (b) Montrer que $\left|\frac{e}{N} - \frac{k}{d}\right| = \frac{k(p+q-1)-1}{dN}$.
   (c) En utilisant l'inégalité $e \leq \varphi(N)$, montrer que $k < d$, et finalement que
   $$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{3d^2}.$$
10. Montrer que k et d sont premiers entre eux, et donc que la fraction k/d permet de calculer efficacement k et d.
11. Donner un descriptif d'une attaque complète de RSA avec une petite clef privée et estimer sa complexité.

Il est à noter cependant qu'en général, le cryptosystème RSA requiert seulement $ed = 1 + k\lambda(N)$ avec $\lambda(N) = (p-1) \vee (q-1)$ et $e, d \in [\![1, \lambda(N) - 1]\!]$. Soit $m = (p-1) \wedge (q-1)$, de telle sorte que $\varphi(N) = m\lambda(N)$.

12. Sous les mêmes hypothèses ($p < q < 2p$ et $d \leq \frac{1}{3}N^{1/4}$), montrer l'inégalité
    $$\left|\frac{e}{N} - \frac{k}{md}\right| < \frac{1}{3d^2}.$$
13. Donc $\frac{k}{md}$ est un convergent de $\frac{e}{N}$. Mais k et m ne sont pas nécessairement premiers entre eux, donc la connaissance de k/md n'est pas suffisante pour retrouver k, m et d.
    (a) Montrer que $e\frac{md}{k} = \frac{m}{k} + \varphi(N)$.
    (b) Sous l'hypothèse supplémentaire (raisonnable) $ed > N$, montrer que $\varphi(N) = \left\lfloor e\frac{md}{k} \right\rfloor$.
14. Expliquer pourquoi la connaissance de $\varphi(N)$ (et N) est équivalente à la connaissance de p et q.