**Niveau : 2** **Orange**

# Attaque de RSA par fractions continues

## 1 Introduction

La primitive de chiffrement RSA (ou de signature) est sensible à une attaque dûe à Wiener, utilisant un développement en fraction continue, dans le cas où l'exposant de chiffrement (ou de signature) $d$ est "petit". Si la taille de $d$ (son nombre de bits) est inférieure au quart de la taille du module, cette attaque fonctionne. Nous allons voir comment la monter.

## 2 Rappels sur la primitive RSA

On rappelle que le système RSA est construit à partir de deux grands nombres premiers distincts $p$ et $q$ dont on note $n$ le produit ($n = pq$). Ce nombre $n$ qui est appelé le module est public (mais bien sûr $p$ et $q$ sont secrets). On note $\phi(n) = (p-1)(q-1)$. L'exposant de chiffrement $1 < e < \phi(n)$ est un nombre premier avec $\phi(n)$ qui est aussi public. L'exposant de déchiffrement $d$ (clé privée) est secret. Il est calculé de manière à ce que $ed \equiv 1 \quad (\phi(n)), 1 < d < \phi(n)$. Dans la suite on va supposer que $p > \sqrt{n} > q$ et que $p$ et $q$ ont la même taille, ce qui implique que :

$$1 < \frac{p}{q} < 2,$$

On supposera aussi que :

$$\log_2(d) \leq \frac{1}{4}\log_2(n) - 3.$$

### 2.1 Si on connaît $d$ alors on peut factoriser $n$

**Théorème 2.1** *Il existe un* **algorithme probabiliste** *de type Las Vegas, ayant pour entrées le module $n$ les exposants de chiffrement $e$ et de déchiffrement $d$, qui calcule la factorisation $pq$ de $n$.*

**Remarque importante :** L'algorithme permet aussi de déterminer si la valeur de $d$ est la bonne ou non.

## 3 L'attaque

### 3.1 Partie technique

Par construction :

$$ed = 1 + k\phi(n),$$

Compte tenu des résultats connus sur la résolution d'une équation de Bézout (voir l'annexe B de [BRV], p. 346), on peut affirmer que puisque $0 < e < \phi(n)$ on a aussi $0 < k < d$. En outre :

$$\phi(n) = (p-1)(q-1) = n - (p+q) + 1.$$

Donc :

$$ed = 1 + k(n - (p+q) + 1),$$

ce qui donne en divisant par $dn$ les relations successives suivantes :

$$\frac{e}{n} = \frac{k}{d} + \frac{1 + k - k(p+q)}{dn},$$

$$\left|\frac{e}{n} - \frac{k}{d}\right| = \frac{k(p+q) - k - 1}{dn},$$

$$\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{k(p+q)}{dn},$$

$$\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{kq(\frac{p}{q} + 1)}{dn},$$

$$\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{3kq}{dn},$$

$$\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{3k}{d\sqrt{n}},$$

$$\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{3}{\sqrt{n}}.$$

Donc si :

$$d \leq \frac{n^{0.25}}{\sqrt{6}},$$

alors :

$$\frac{1}{2d^2} \geq \frac{6}{2\sqrt{n}},$$

et en conséquence :

$$\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

D'après un résultat sur les fractions continues on en conclut que $\frac{k}{d}$ est une réduite de $\frac{e}{n}$.

## 3.2 Réalisation de l'attaque

L'attaque est alors la suivante : $e$ et $n$ sont publics, donc l'attaquant peut développer $\frac{e}{n}$ en fraction continue. Il teste alors pour toutes les réduites successives, si le dénominateur $d$ permet ou non de factoriser $n$, et s' arrête dès qu'il a trouvé le bon $d$ et donc la factorisation de $n$.