TD12 - Cryptanalyse à Base de Réseaux

Responsable : M. Bombar

1 Factorisation d'Entiers avec Extra Information

On considère un module RSA $N = pq$ connu et on suppose connaître tous les bits de p sauf ses ℓ bits de poids faible. Par exemple, on a pu obtenir cette information via une attaque par cannaux auxiliaires. On note b la suite des bits connus, de sorte que l'on peut écrire $p = a + r$ avec $a = 2^\ell b$.

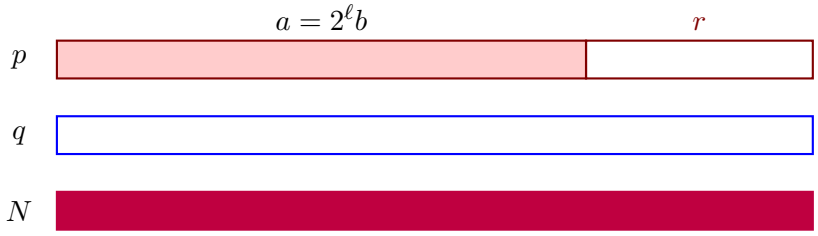

FIGURE 1 – Factorisation de $N = pq$ connaissant les bits de poids forts de p.

Par exemple, on pose

$$N = 531989169769842779734907370680446875855524497380143430583312152409829621$$

et on suppose que l'on connaît

$$a = \mathsf{0x}68323401cb3a10959e7bfdc0000000 = 541017114187426553022141142803677184$$

c'est à dire que l'on connaît tous les bits de p sauf les $\ell = 30$ derniers bits.

(Q1) Déterminer un polynôme simple $F(x) \in \mathbb{Z}[x]$ et un entier R de sorte que r vérifie

$$F(r) \equiv 0 \mod p, \quad \text{et } |r| < R.$$

Notez que l'on ne connaît pas p, mais on connaît N.

Comme dans le cours avec la méthode de Coppersmith, à tout polynôme $A(x) \stackrel{\text{def}}{=} \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$ on associe le vecteur

$$b_A \stackrel{\text{def}}{=} (a_0, a_1 R, \cdots, a_d R^d).$$

De même, tout vecteur de $\mathbb{Z}^{d+1}$ correspond naturellement à un polynôme de degré au plus d dans $\mathbb{Z}[x]$. De fait, on confondra souvent vecteur et polynôme.

On considère le réseau $\mathcal{L}$ défini par la base

$$B \stackrel{\text{def}}{=} \begin{pmatrix} R^2 & Ra & 0 \\ 0 & R & a \\ 0 & 0 & N \end{pmatrix}$$

(Q2) Quelle est la dimension de ce réseau ?

(Q3) Quel est le déterminant de ce réseau ?

(Q4) Montrer que pour tout vecteur $v \in \mathcal{L}$, le polynôme $v(x)$ associé vérifie

$$v(r) \equiv 0 \mod p.$$

(Q5) Pour tout vecteur $v \in \mathcal{L}$, on définit le polynôme

$$\tilde{v}(x) \stackrel{\text{def}}{=} \sum_{i \geq 0} \frac{v_i}{R^i} x^i \in \mathbb{Z}[x].$$

Vérifiez que pour tout vecteur $v \in \mathcal{L}$ on a

$$|\tilde{v}(r)| \leq \|v\|_1 \quad \text{(dans } \mathbb{Z}\text{)}.$$

(Q6) À l'aide de l'algorithme LLL, déterminez un polynôme $G(x) \in \mathbb{Z}[x]$ tel que $G(r) = 0$ dans $\mathbb{Z}$.

(Q7) En déduire r, puis la factorisation complète de N.

(Q8) Sous quelle condition sur R (et donc sur le nombre maximal de bits ℓ inconnus dans p) cette attaque réussit-elle ?

2 Challenge

Le fichier challgengeRSA.sage contient un module RSA $N = pq$ et un entier a contenant un certain nombre de bits de poids forts de p.

(Q9) Factoriser N.