FEUILLE D'EXERCICES n° 6

Cryptographie asymétrique (2)

Exercice 1 – [L'algorithme ρ de Pollard pour la factorisation]
Soit n un nombre entier dont on veut calculer un facteur non trivial. Soit p le plus petit facteur premier (inconnu) de n. L'idée est de construire une suite « aléatoire » $x_1, x_2, \ldots, x_i, \ldots$ d'éléments de $\mathbb{Z}/n\mathbb{Z}$, de sorte qu'une collision $x_i = x_j \mod p$ pour $i < j$ permette de trouver un facteur de n donné par $(x_i - x_j, n)$.

On admettra le résultat suivant, connu sous le nom de *paradoxe des anniversaires* : en tirant au hasard des éléments d'un ensemble de cardinal N, on obtient une collision avec probabilité supérieure à $1/2$ au bout d'environ $\sqrt{N}$ tirages.

1) Estimez le nombre de termes de la suite et le nombre de pgcd à calculer avant de trouver un facteur de n.

2) On choisit de définir la suite x_i par la donnée de x_1 et la formule de récurrence $x_{i+1} = P(x_i)$, où $P \in \mathbb{Z}[X]$.

a) Montrez que $x_i = x_j \mod p \Longrightarrow x_{i+1} = x_{j+1} \mod p$.

b) En déduire que, si $x_i = x_j \mod p$ avec $i < j$ alors $x_u = x_{2u} \mod p$ pour un indice u tel que $u < j$.

c) Comment calculer $(x_{i+1}, x_{2(i+1)})$ à partir de (x_i, x_{2i}) ?

d) On *suppose* que la suite (x_i) obtenue a le même comportement qu'une suite de tirages indépendants dans $\mathbb{Z}/N\mathbb{Z}$, et donc qu'on peut appliquer le paradoxe des anniversaires. En déduire un algorithme qui nécessite environ $\sqrt{p}$ calculs de pgcd de nombres entiers naturels $\leqslant n$ pour factoriser n.

3) Factorisez $n = 7171$ avec $x_1 = 1$ et $P(x) = x^2 + 1$.

Exercice 2 – [Le cryptosystème de Rabin]

1) Soit p un nombre premier impair. Soit

$$\begin{aligned} \varphi : (\mathbb{Z}/p\mathbb{Z})^* &\to (\mathbb{Z}/p\mathbb{Z})^* \\ x &\mapsto x^2 \end{aligned}$$

a) Montrez que $\operatorname{Ker}\varphi = \{\pm 1\}$.

b) En déduire que $\operatorname{Im}\varphi$ est un sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^*$ d'ordre $(p-1)/2$, et que, si $y \in \operatorname{Im}\varphi$ alors l'équation $x^2 = y$ a exactement deux solutions.

c) En déduire que y est un carré de $(\mathbb{Z}/p\mathbb{Z})^*$ si et seulement si $y^{\frac{p-1}{2}} = 1$.

d) On suppose de plus que $p \equiv 3 \mod 4$. Montrez que, si y est un carré de $(\mathbb{Z}/p\mathbb{Z})^*$, alors

$$y = (\pm y^{\frac{p+1}{4}})^2.$$

2) Soit $n = pq$ avec p, q deux nombres premiers impairs distincts. Montrez que, si $y \in (\mathbb{Z}/n\mathbb{Z})^*$, l'équation $x^2 = y$ a soit aucune soit quatre solutions (on pourra utiliser le théorème Chinois). Caractérisez ce dernier cas.

3) Le cryptosystème de Rabin utilise un entier $n = pq$ avec p, q deux nombres premiers distincts tels que $p, q \equiv 3 \mod 4$. La clé publique est n, la clé privée est (n, p, q). La fonction de chiffrement est $e(x) = x^2 \mod n$.

a) Expliquez pourquoi la fonction de chiffrement n'est pas injective.

b) Expliquez comment Bob, qui connait la clé privée, peut calculer à partir d'un chiffré, un ensemble de quatre éléments contenant le clair.

c) Soit $n = 77$. Le chiffré est 23. Calculez les quatre possibilités pour le clair.

Exercice 3 – Trouvez un diviseur non trivial de $N = 1829$ avec l'algorithme de Dixon et la base de facteurs $\mathcal{B} = \{-1, 2, 3, 5, 7, 11, 13\}$. On pourra utiliser les entiers $42, 43, 61, 74, 85, 86$.

Exercice 4 – Soit n un entier de la forme $n = pq$ avec p, q premiers distincts.

1) Montrez que p et q sont racines de l'équation

$$X^2 - (n - \varphi(n) + 1)X + n = 0.$$

2) En déduire qu'il n'est pas plus facile de calculer $\varphi(n)$ que de factoriser n.

3) Soit $n = 84773093$. Sachant que $\varphi(n) = 84754668$, factorisez n.