Factorisation des entiers

Vincent Dalsheimer Gaëtan Pradel

Année 2016 - Semestre 10

Table des matières

1 Introduction

Théorème 1 (Théorème fondamental de l'arithmétique)**.** *Tout entier strictement positif peut être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs.*

Théorème 2. *Il existe une infinité de nombres premiers.*

2 Rappels sur l'utilité des nombres premiers en cryptographie

En cryptographie, les nombres premiers sont très utilisés et très utiles car ils apportent, grâce à leurs propriétés, de la sécurité.

2.1 Chiffrement RSA

En effet, présentons l'algorithme RSA qui les utilise.

Tout d'abord, le chiffrement RSA est un chiffrement asymétrique, c'est-à-dire qu'il utilise une paire de clés, qui sont des nombres entiers, composée d'une clé publique pour chiffrer et d'une clé privée pour déchiffrer. La clé privée peut être aussi utilisée pour signer un message.

2.1.1 Création des clés

- Choisir p et q, deux nombres premiers entiers distincts ;
- calculer leur produit $n = p * q$
- calculer $\phi(n) = (p-1)(q-1)$ qui est la valeur de l'indicatrice d'Euler en n ;
- choisir un entier naturel e premier avec $\phi(n)$ et strictement inférieur à $\phi(n)$;
- calculer l'entier naturel d, inverse de e modulo $\phi(n)$, et strictement inférieur à $\phi(n)$; d peut se calculer efficacement par l'algorithme d'Euclide étendu.

Le couple (n, e) est la clé publique et le triplet (p, q, d) est la clé privée.

La sécurité de cet algorithme repose sur le fait que la factorisation (de grands nombres) est un problème difficile, c'est-à-dire qu'on ne peut pas le résoudre en temps polynomial.

2.1.2 Chiffrement

Soit m un message à chiffrer. Le message chiffré c de m sera :

$$m \equiv m^e \pmod{n}.$$

2.1.3 Déchiffrement

Soit le message chiffré c comme ci-dessus. Pour retrouver le message m on fait :

$$c^d \equiv m^{e*d} \equiv m \pmod{n}.$$

2.1.4 Justification

La démonstration repose sur le petit théorème de Fermat, à savoir que comme p et q sont deux nombres premiers, si m n'est pas un multiple de p on a la première égalité, et la seconde s'il n'est pas un multiple de q :

$$m^{p-1} \equiv 1 \pmod{p}\ ,\quad m^{q-1} \equiv 1 \pmod{q}.$$

En effet

$$c^d \equiv (m^e)^d \equiv m^{ed} \pmod{n}.$$

Or

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

ce qui signifie que pour un entier k

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

donc, si m n'est pas multiple de p d'après le petit théorème de Fermat

$$m^{ed} \equiv m^{1+k(p-1)(q-1)} \equiv m \cdot \left(m^{p-1}\right)^{k(q-1)} \equiv m \pmod{p}$$

et de même, si m n'est pas multiple de q

$$m^{ed} \equiv m \pmod{q}.$$

3 Méthode naïve de la factorisation

Pour factoriser un nombre n, la méthode la plus naïve et la plus naturelle consiste à faire les divisions euclidiennes successives de n par 2 (autant de fois que l'on peut), puis 3, etc ... jusqu'à la partie entière de $\sqrt[2]{n}$.

4 L'algorithme $p-1$ de Pollard

5 Crible $x \equiv x + N \bmod N$