Texte court/TP
Cryptosystème de Rabin

auteur : D. Boucher
relecteur : L. Fourquaux

18 avril 2013

Le texte présente un certain nombre de suggestions et d'affirmations non justifiées écrites en italique.

Résumé

Le cryptosystème de Rabin est un cryptosystème dont le chiffrement est basé sur l'élévation au carré d'un entier modulo un produit de deux nombres premiers et dont le déchiffrement utilise l'extraction de racine carrée modulo un nombre premier impair ainsi que le théorème chinois.

1 Racine carrée modulo un nombre premier

Soit p un nombre premier impair et soit a un entier qui est un carré modulo p. Pour déterminer un entier x tel que $x^2 \equiv a \pmod{p}$, on peut faire une recherche exhaustive (*la programmer*) et cela prendrait $O(p)$ opérations, soit une complexité exponentielle.

Dans certains cas particuliers on peut donner une expression d'une racine carrée de a modulo p :

– Si $p \not\equiv 1 \pmod 4$ alors $p \equiv 3 \pmod 4$. *Une solution est donnée par*

$$x = a^{(p+1)/4} \bmod p.$$

– Si $p \equiv 1 \pmod 4$ et $p \not\equiv 1 \pmod 8$, alors $p \equiv 5 \pmod 8$ et $a^{(p-1)/4} \equiv \pm 1 \pmod p$. *Une solution est donnée par*

$$x = \begin{cases} a^{(p+3)/8} \bmod p & si \quad a^{(p-1)/4} \equiv 1 \pmod p \\ 2a(4a)^{(p-5)/8} \bmod p & si \quad a^{(p-1)/4} \equiv -1 \pmod p \end{cases}$$

L'algorithme de Tonelli Shanks est un algorithme probabiliste qui généralise les cas précédents.

Soient s et $t \in \mathbb{N}$ tels que $p-1 = 2^s t$ avec t impair. *Le groupe cyclique $\mathbb{Z}/p\mathbb{Z}^*$ possède un sous-groupe G cyclique d'ordre 2^s : c'est l'unique 2-Sylow d'ordre 2^s de $\mathbb{Z}/p\mathbb{Z}^*$*. Soit z un générateur de G. Comme a est un carré modulo p, on a $a^{(p-1)/2} \equiv 1 \pmod p$ donc $(a^t)^{2^{s-1}} \equiv 1 \pmod p$, donc a^t est dans G et son ordre divise 2^{s-1}. En particulier, *il existe un entier pair $m \in \{0, \ldots, 2^s - 1\}$ tel que*

$$a^t z^m = 1. \tag{1}$$

Si l'on pose

$$x = a^{(t+1)/2} z^{m/2}$$

on a donc $x^2 \equiv a \pmod p$.

Deux questions se posent : comment trouver un générateur z de G ? comment trouver m ?

1.1 Générateur de G

Pour trouver z, on cherche un non carré b dans $\mathbb{Z}/p\mathbb{Z}^*$ et on pose $z = b^t$. Alors $z^{2^{s-1}} = b^{t2^{s-1}} = b^{(p-1)/2} = -1 \bmod p$ et z est d'ordre 2^s. Il y a autant de carrés que de non carrés dans $\mathbb{Z}/p\mathbb{Z}^*$ donc la probabiblité d'échec est 1/2. En cas d'échec on recommence le tirage (c'est cette partie de l'algorithme qui est non déterministe).

1.2 Logarithme discret

Pour trouver m on est ramené à résoudre un problème de logarithme discret dans un groupe d'ordre 2^s, à savoir résoudre

$$a^t = z^\alpha \tag{2}$$

dans G où $\alpha \in \{0, \ldots, 2^s - 1\}$.

On écrit α en base 2 : $\alpha = \alpha_0 + 2\alpha_1 + \cdots + 2^{s-1}\alpha_{s-1}$ avec $\alpha_i \in \{0, 1\}$ et on détermine les α_i en résolvant des logarithmes discrets dans un groupe d'ordre 2, ce qui est très rapide. Soit en effet $\beta = z^{2^{s-1}}$, β est d'ordre 2 et en élevant la relation (2) à la puissance 2^{s-1}, on obtient

$$\beta^{\alpha_0} = a^{t2^{s-1}}$$

d'où $\alpha_0 = 0$.

En élevant à la puissance 2^{s-2} la relation

$$z^{\alpha-\alpha_0} = a^t z^{-\alpha_0}$$

on obtient

$$\beta^{\alpha_1} = (a^t z^{-\alpha 0})^{2^{s-2}}$$

donc

$$\alpha_1 \quad = \quad \begin{array}{ll} 1 & \text{si } (a^t z^{-\alpha 0})^{2^{s-2}} = -1 \\ 0 & \text{sinon} \end{array}$$

On réitère le processus : en élevant à la puissance 2^{s-3} la relation

$$z^{\alpha-\alpha_0-2\alpha_1} = a^t z^{-\alpha_0-2\alpha_1}$$

on obtient

$$\beta^{\alpha_2} = (a^t z^{-\alpha_0-2\alpha_1})^{2^{s-3}}$$

donc

$$\alpha_2 \quad = \quad \begin{array}{ll} 1 & \text{si } (a^t z^{-\alpha 0-2\alpha_1})^{2^{s-3}} = -1 \\ 0 & \text{sinon} \end{array}$$

On construit ainsi les suites (m_i) et (a_i) définies par : $m_0 = 0$, et pour $0 \leq i \leq s-1$

$$a_i = (a^t\, z^{m_i})^{2^{s-1-i}} \mod p$$

$$m_{i+1} \quad = \quad \begin{array}{ll} m_i + 2^i & \text{si } a_i = -1 \\ m_i & \text{sinon} \end{array}$$

L'entier $m = m_s$ est pair et vérifie la relation (1). De plus son calcul a nécessité $s^2/2$ opérations.

1.3 Algorithme de Tonelli-Shanks

Pour résumer on obtient donc l'algorithme suivant *que l'on pourra tester en Maple* :

2 Cryptosystème de Rabin

Pour le cryptosystème RSA, si l'on sait factoriser le module RSA alors on peut casser le cryptosystème, mais la réciproque n'a pas été prouvée.

Le cryptosystème à clé publique de Rabin est un exemple de schéma prouvé sûr : *si on sait retrouver le message à partir du cryptogramme alors on sait factoriser le module.* De plus si on sait factoriser le module, alors on peut retrouver un ensemble de quatre valeurs possibles pour le message (voir section 2.3).

Voici les trois étapes de ce cryptosystème *que l'on pourra programmer en Maple sous forme de trois procédures* : la fabrication des clés, le chiffrement et le déchiffrement.

Algorithme de Tonelli-Shanks

Entrée : p, nombre premier impair ; a carré modulo p
Sortie : une racine carrée de a modulo p

1: Calculer s, t tels que $p-1 = 2^s t$ avec t impair et $s \in \mathbb{N}$
2: Trouver b entre 2 et $p-1$ tel que b ne soit pas un carré modulo p
3: $z \leftarrow b^t$
4: $m \leftarrow 0$
5: **pour** i de 0 à $s-1$ **faire**
6: **si** $(a^t z^m)^{2^{s-1-i}} \equiv -1 \pmod{p}$ **alors**
7: $m \leftarrow m + 2^i$
8: **fin si**
9: **fin pour**
10: **rendre** $a^{(t+1)/2} z^{m/2}$

2.1 Génération des clés

A génère deux grands nombres premiers impairs distincts p et q et calcule $n = pq$.
La clé publique est n, la clé privée est (p, q).

2.2 Chiffrement

B chiffre un message pour A :
- Il consulte l'annuaire des clés où il récupère la clé publique n de A ;
- il représente le message comme un entier m entre 0 et $n-1$;
- il calcule $c = m^2 \bmod n$;
- il envoie le cryptogramme c à A.

2.3 Déchiffrement

A reçoit c et déchiffre c :
- il calcule les racines carrées $\pm m_p$ de c modulo p et $\pm m_q$ de c modulo q à l'aide de l'algorithme de Tonelli-Shanks ;
- *à l'aide du théorème chinois, il en déduit les racines* $m_1, n-m_1, m_2, n-m_2$ *de* c *modulo* n.

Le message initial est l'une de ces quatre valeurs et A n'a aucun moyen de sélectionner le bon message parmi les quatre possibilités. Pour éviter ce problème, on peut ajouter de la redondance au message avant de le chiffrer (par exemple les derniers 64 bits du message peuvent être ajoutés). Dans ce cas cependant, il pourrait être possible de tirer profit de la redondance pour casser le chiffrement sans savoir factoriser le module n.

Exemple 1 *A choisit les nombres premiers* $p = 277$ *et* $q = 331$ *et calcule* $n = pq = 91687$.

B souhaite envoyer le message binaire 1001111001*à A, il ajoute les* 6 *derniers bits et obtient* 1001111001111001 *qui converti, en base* 10 *donne* $m = 40569$.

B calcule $c = m^2 \bmod n = 62111$ *et envoie* c *à A.*

A reçoit c *et calcule les* 4 *racines carrées de* c *:* $69654, 22033, 40569, 51118$ *qui en binaires donnent*

$m1 = 10001000000010110, m2 = 101011000010001, m3 = 1001111001111001, m4 = 1100011110101110$

Comme $m3$ *est le seul message avec redondance, A choisit* $m3$ *et retrouve le message* 1001111001.

3 Question de jury

Etant donné un nombre premier p et un entier a qui est un carré modulo p, comment résoudre l'équation $x^2 \equiv a \pmod{p^\alpha}$ où α est un entier > 1 ?

Comment procéder si l'on remplace p par un nombre composé n ?