Niveau : 1 **Jaune**

Construction de nombres premiers

1 Introduction

Dans la mise en place de nombreux problèmes de cryptographie à clé publique, il est nécessaire de **construire de grands nombres premiers**. Le premier problème est alors de reconnaître si un nombre est premier ou pas.

2 Tester si un nombre est premier

2.1 Complexité du problème

Déterminer si un nombre est premier est appelé le problème "Prime" noté $\mathcal{P}$. On sait depuis peu que ce problème est polynomial (Manindra Agarwal, Nitin Saxena, Neeraj Kayal, PRIMES is in P, 2002). Cependant l'algorithme polynomial qui prouve ce résultat ne donne pas un temps d'exécution faisable pour les tailles que nous avons en vue. De ce fait en pratique on utilise un test probabiliste de non-primalité et si besoin est, on lance un algorithme déterministe pour confirmer que le candidat premier trouvé par l'algorithme probabiliste est réellement premier (il en existe qui peuvent aboutir en temps envisageable, pourvu qu'on ne les lance pas en boucle).

2.2 Le test de non-primalité de Miller-Rabin

Le petit théorème de Fermat énonce que si p est premier, pour tout élément a de $(Z/pZ)^*$ on a $a^{p-1} = 1$ (dans $(Z/pZ)^*$). La réciproque est fausse. C'est-à-dire qu'on peut avoir ce résultat pour des nombres p non premiers (nombre de Carmichael). Cependant une amélioration de la méthode conduit au test de Miller-Rabin. Ce test est en fait un test de non-primalité, c'est-à-dire que s'il répond qu'un nombre n'est pas premier alors il est sûr que ce nombre ne l'est pas. Il peut aussi répondre qu'un nombre est probablement premier. Dans ce cas si ce nombre n'est pas premier, la probabilité de ne pas avoir été détecté non premier est infime : on peut imposer par exemple que cette probabilité soit $< 2^{-100}$. Un tel algorithme est appelé un algorithme de Monte-Carlo.

2.2.1 Les témoins de Miller

Théorème 2.1 *Soit n un entier impair > 1. Posons $n-1 = 2^s t$ avec t impair. S'il existe a ($1 < a < n$) tel que :*

$$a^t \not\equiv 1 \quad (n)$$

et :

$$a^{2^i t} \not\equiv -1 \quad (n) \quad \forall i = 0, \cdots, s-1,$$

alors n n'est pas premier.

Preuve. Supposons n premier. Pour $i = 0, \cdots, s$ posons $a_i = a^{2^i t} \mod n$. D'après le petit théorème de Fermat $a_s = 1$. Dans ces conditions ou bien tous les a_i valent 1 et dans ce cas a_0 vaut 1, ou bien il existe un i tel que $0 \leq i < s$, $a_i \neq 1$ et $a_{i+1} = 1$. Dans ce cas, puisque $a_{i+1} \equiv a_i^2 \quad (n)$ et que $\mathbb{Z}/n\mathbb{Z}$ est un corps on en déduit que $a_i \equiv -1 \quad (n)$. □

Définition 2.2 *Un élément a qui vérifie les conditions du théorème et qui donc apporte une preuve de la non-primalité de n s'appelle un témoin de Miller relatif à n.*

2.2.2 Proportion de témoins de Miller

L'idée qu'on peut avoir maintenant est d'utiliser le théorème 2.1 pour détecter si un nombre est premier ou tout au moins s'il a de bonnes chances de l'être. Le théorème de Rabin qui suit va nous permettre de majorer pour un entier n composé, le nombre d'éléments strictement compris entre 1 et n qui ne sont pas des témoins de Miller. Ceci nous permettra ensuite de mettre en place le test de Miller-Rabin.

Théorème 2.3 (Théorème de Rabin) *Soit n un entier impair composé > 9. Posons $n-1 = 2^s t$ avec t impair. Les entiers $1 < a < n$ qui satisfont à la condition :*

$$a^t \equiv 1 \quad (n),$$

ou bien à l'une des conditions :

$$a^{2^i t} \equiv -1 \quad (n) \qquad (0 \leq i \leq s-1),$$

sont en nombre au plus :

$$\frac{\Phi(n)}{4}.$$

Preuve. Nous renvoyons au livre de Michel Demazure *Cours d'algèbre (Cassini)* pour une démonstration de ce théorème. □

2.3 Conséquences

La propriété de Miller et le théorème de Rabin procurent le test suivant appelé **test de Miller-Rabin** :

On choisit a au hasard ($a < n$) et on calcule :

$$a^t \qquad \mod n.$$

Si on trouve 1 alors a n'est pas un témoin de Miller pour n, sinon on calcule les nombres :

$$a^{2^i t} \qquad \mod n,$$

et si pour un certain i on trouve -1 alors a n'est pas un témoin de Miller pour n.
Faisons ce test avec k valeurs aléatoires de a ; si aucune des valeurs a, tirées au hasard, n'est témoin de Miller, le nombre n est vraisemblablement premier. Plus précisément, si n est composé, la probabilité d'être déclaré premier est $< \frac{1}{4^k}$. On peut prendre par exemple $k = 50$.

Remarque : Notons A l'événement "n est composé" et C l'événement "au bout de k essais on n'a pas trouvé de témoin de Miller". Nous avons majoré la probabilité conditionnelle $P(C|A)$. En fait on aimerait bien avoir $P(A|C)$: sachant qu'on n'est pas tombé sur un témoins de Miller et donc qu'on pense que le nombre est vraisemblablement premier, quelle est la probabilité pour qu'il ne le soit pas ? Le théorème de Bayes ainsi que l'évaluation habituelle de la proportion de nombre premiers permet d'obtenir une évaluation de cette probabilité.

3 Construire un nombre premier de taille donnée

La construction d'un nombre premier p de taille donnée passe par le tirage aléatoire d'un nombre impair de la taille indiquée qu'on met dans une variable X. On teste si le contenu de X est un nombre premier, tant qu'il ne l'est pas on lui ajoute 2. À vrai dire, il vaudrait mieux retirer un nombre impair de la taille donnée au hasard, la méthode indiquée précédemment ne respectant pas l'équiprobabilité des tirages. Comme la concentration en nombres premiers est asymptotiquement $\ln(x)/x$, l'espérance mathématique du nombre de boucles à faire est de l'ordre de $\ln(p)$.

4 Construire p et q premiers tels que $p = kq + 1$

4.1 q fixé

On fixe un nombre premier q (qu'on a pu construire par exemple comme indiqué dans le paragraphe précédent). Le problème est alors de trouver k tel que le nombre $p = kq + 1$ soit premier. Pour cela on peut tirer un nombre k pair au sort, on l'incrémente de 2 jusqu'à ce que $kq + 1$ soit premier. Un résultat de Dedekind sur la concentration en nombres premiers des termes d'une suite arithmétique permet là encore de prévoir que cet algorithme aboutit en un nombre d'itérations moyen majoré par la taille espérée pour p.

4.2 Les nombres de Sophie Germain

Au lieu de fixer q on peut fixer k. Par exemple prendre $k = 2$. Si q et $2q + 1$ sont premiers on dit alors que q est un nombre de Sophie Germain. On ne sait pas dans ce cas s'il y a une infinité de nombres de Sophie Germain ni évidemment la concentration de ces nombres. Mais pour les tailles cryptographiques qui nous intéressent, l'algorithme suivant aboutit en pratique : on construit q au hasard et on teste si $2q + 1$ est premier, sinon on passe au nombre premier q suivant.

5 Le contexte cryptographique

5.1 RSA et systèmes dérivés

Le système RSA demande la construction de nombres premiers. La méthode du paragraphe 3 s'applique.

5.2 Groupe multiplicatif $(Z/pZ)^*$ et sous groupes d'ordre q premier

Dans de nombreuses situations on doit construire un groupe multiplicatif $(Z/pZ)^*$ et un sous groupe d'ordre premier q de ce groupe.

5.3 Cas où on a besoin de q grand

C'est le cas par exemple où un utilise le groupe multiplicatif $(Z/pZ)^*$ pour l'échange de clé de Diffie-Hellman. Dans ce cas on doit disposer d'un générateur de $(Z/pZ)^*$ (élément primitif) ou tout au moins d'un générateur d'un grand sous-groupe de $(Z/pZ)^*$. Deux méthodes peuvent alors se concevoir :

1) On utilise 4.1 en cherchant p et q tels que le nombre $taille(p) - taille(q)$ soit suffisamment petit pour que k puisse être factorisé. On tire alors au sort $alpha$ et on teste avec la méthode indiquée dans la "fichecrypto_ 107" s'il est primitif ou pas. Tant qu'il n'est pas primitif on en retire un autre.

2) On utilise un nombre de Sophie Germain q (cf. 4.2). Dans ce cas si on prend un élément $\alpha \in (Z/pZ)^*$, alors son ordre peut être 1, 2, $q = (p-1)/2$ ou $p-1$. Si on évite l'élément 1 qui est d'ordre 1 et l'élément $p-1$ (c'est-à-dire -1) qui est d'ordre 2 les autres sont soit d'ordre $p-1$ soit d'ordre $(p-1)/2$ (et c'est facile de le savoir en calculant $\alpha^{(p-1)/2}$). Dans les deux cas cela suffit pour faire de l'échange de clé de Diffie-Hellman. Ceci est la méthode utilisée dans le protocole SSH.

5.4 Cas où on a besoin de q plus petit

Dans certains cas on ne cherche pas à construire un élément primitif de $(Z/pZ)^*$, mais un sous groupe qui sans être dans l'absolu de petite taille a une taille relativement petite devant p. C'est le cas du chiffrement d'ElGamal, ou de la signature DSA où p a 1024 bits alors que q a 160 bits. Dans ce cas on utilise l'algorithme du paragraphe 4.1 pour obtenir un couple de nombres premiers p et q de la taille indiquée et vérifiant $p = kq + 1$. On tire au sort un $\beta \in (Z/pZ)^*$. On calcule $\alpha = \beta^k$. Si ce nombre n'est pas 1 alors il est d'ordre q. Sinon on retire un autre β. On a donc construit par cette méthode un générateur α du sous groupe d'ordre q de $(Z/pZ)^*$.