TD 8 : Tests de primalité et cryptographie à clé publique

christina.boura@uvsq.fr

27 mars 2018

Exercice 1 *Génération de nombres premiers pour RSA*

Les tailles les plus courantes pour un module RSA sont $1024, 2048, 3072$ et 4096 bits.

1. Combien de nombres aléatoires impairs doit-on tester en moyenne avant de trouver un nombre premier ?
2. Dériver une formule simple pour un module RSA de taille arbitraire.

Exercice 2 *Probabilité d'erreur du test de Fermat*
On peut montrer que la probabilité que le test de Fermat se trompe (renvoie premier à tort) après ℓ itérations est au plus $1/2^{\ell}$. Combien d'itérations doit-on effectuer afin d'avoir une probabilité d'erreur inférieure à 2^{-80} ?

Exercice 3 *RSA avec p et q très proches*
Soit $n = pq$ impair avec $p > q$.

1. Vérifier que $n = t^2 - s^2 = (t + s)(t - s)$ avec $t = \frac{p+q}{2}$ et $s = \frac{p-q}{2}$.
2. On suppose maintenant que p est très proche de q (ou encore que s est petit), montrer que t est supérieur à $\sqrt{n}$ et très proche de $\sqrt{n}$.
3. Utiliser ces remarques pour factoriser $n = 4397231$.

Exercice 4 *Nombres de Carmichael*
Un *nombre de Caramichael*, n, est un entier positif composé tel que $a^{n-1} \equiv 1 \mod n$ pour tout a tel que $\text{pgcd}(a, n) = 1$. Montrer qu'un nombre $n \geq 4$ de Carmichael est toujours impair.

Exercice 5 *Établissement d'une clé de session*

Une des applications les plus intéressantes des algorithmes à clé publique est l'établissement d'une clé secrète pour un algorithme symétrique (par exemple le `3DES`) à travers un canal pas sûr. On suppose que Bob a une paire de clés RSA. Montrer un protocole simple utilisant RSA qui permet à Alice et Bob de se mettre d'accord sur une clé secrète partagée. Qui determine la clé dans ce protocole, Alice, Bob ou tous les deux ?

Exercice 6 *Établissement d'une clé de session (suite)*

En pratique, il est parfois désiré que les deux parties aient une influence sur le choix de la clé partagée. Ceci est par exemple demandé pour empêcher l'autre personne de choisir une clé faible pour un algorithme symétrique. Plusieurs chiffrements par blocs possèdent des clés faibles et DES en fait partie. Des messages chiffrés avec des clés faibles peuvent être facilement retrouvés à partir du chiffré.

Développer un protocole dans lequel les deux parties influencent le choix de la clé. On suppose que Alice et Bob possèdent tous les deux une paire de clés RSA.