Autour de RSA

Exercice 1. Échec de protocoles. Algorithme de Naggle. Alice ouvre une session à distance sur l'ordinateur de Bob. Elle chiffre la session en utilisant RSA. La clé publique est incassable (1024 bits). La liaison et la machine d'Alice sont très rapides, si bien que les caractères saisis au clavier par Alice sont envoyés un par un (cf algorithme de Naggle).

1. Comment l'espionne Ève peut-elle déchiffrer les messages d'Alice.

2. Comment peut-on résoudre ce problème ?

3. L'amélioration du protocole que vous avez proposée permet-elle d'empêcher Ève de distinguer deux messages identiques d'Alice ? Permet-elle d'empêcher Melvil de ré-envoyer plus tard un message qu'il aura intercepté (sans pouvoir le comprendre) ?

4. Est-il réaliste de chiffrer une telle liaison avec RSA ? Pourquoi ? Que font les systèmes comme SSH ou SSL ? Cela change-t'il quelque chose au problème ?

5. Lire, comprendre et discuter le RSAES-OAEP (*RSA Encryption Scheme - Optimal Asymmetric Encryption Padding*) : PKCS#1 pages 17 à 21. Vous devrez vous en servir en TP.

Exercice 2. Échec de protocoles. Attaque du modulo commun. Alice envoie le même message x à Bob et Bart. Tous deux utilisent le même modulo n et des exposants publics a_1 et a_2 qui sont premiers entre-eux. Alice publie donc vers Bob et Bart respectivement $y_1 = x^{a_1}$ modulo n et $y_2 = x^{a_2}$ modulo n.

1. Montrer que si u_1 et u_2 sont tels que $u_1 a_1 + u_2 a_2 = 1$ alors $x = {y_1}^{u_1} {y_2}^{u_2}$ modulo n. Comment trouver u_1 et u_2 ?

2. Effectuer cette attaque avec $n = 18721$, $b_1 = 43$, $b_2 = 7717$, $y_1 = 12677$ et $y_2 = 14702$.

Exercice 3. Algorithmes de Monte-Carlo

Dans le test de Miller-Rabin, si N n'est pas premier au moins trois nombres sur quatre font répondre « N n'est pas premier » à l'algorithme.

1. Si un nombre passe dix fois le test de Miller-Rabin quel est la probabilité qu'il soit premier.

2. Combien de fois faut-il faire le test de Miller-Rabin pour être sûr avec une probabilité de plus de 99.999999% que N est premier.

3. Donner un ordre de grandeur de la complexité de trouver un nombre de 512 bits dont on est sûr qu'il est premier avec une probabilité plus grande que 99.999999%.