Autour de RSA

Exercice 1. Échec de protocoles

1. ALgorithme de Naggle. Alice et Bob communiquent en utilisant RSA. Leur clé publique est incassable (1024 bits). La liaison entre eux 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.a. Comment l'espionne Ève peut-elle déchiffrer les messages d'Alice.

1.b. Comment peut-on résoudre ce problème ?

1.c. 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) ?

2. 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.

2.a. Montrer que si u_1 et u_2 sont tels que $u_1a_1 + u_2a_2 = 1$ alors $x = {y_1}^{u_1}{y_2}^{u_2}$ modulo n. Comment trouver u_1 et u_2 ?

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

Exercice 2. 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%.

Exercice 3. Lire, comprendre et discuter le RSAES-OAEP (*RSA Encryption Scheme - Optimal Asymmetric Encryption Padding*) : PKCS#1 pages 17 à 21.