Initiation à la cryptographie

Travaux Dirigés de cryptographie n°5

—Télécom Nancy 2A ISS—

1 RSA

▸ **Exercice 1.** À la main !

Considérons le système RSA construit à partir des entier $p = 19$ et $q = 23$. Vous avez le droit à la calculatrice : ce n'est pas un exercice de calcul !

1. Calculer N et $\varphi(N)$.
2. Calculer l'exposant de déchiffrement d associé à $e = 5$ et l'exposant de déchiffrement d associé à $e = 9$.
3. Calculer le chiffré associé au message $m = 42$ quand $e = 5$.

▸ **Exercice 2.** Malléabilité de RSA.

Nous allons montrer comment les propriétés multiplicatives de RSA rendent une utilisation naïve de ce cryptosystème complètement illusoire.

1. Proposer un procédé de signature « naïf » d'un message $m \in \mathbb{Z}/N\mathbb{Z}$ par Alice avec sa clé privée RSA.
2. Ève a réussi à se procurer les signatures du message m_1 et du message m_2. Montrer quels autres messages elle peut signer au nom d'Alice, et comment.
3. Nous allons montrer une sorte de généralisation de ce procédé. On suppose qu'Ève s'est procuré un ensemble de signatures de messages : elle connaît un *grand* nombre de couples $(m_i, S(m_i))$. De plus, les m_i sont petits et Ève a pu les factoriser :
$$\forall i, m_i = \prod_j \mu_j^{\alpha_{i,j}}.$$
On appelle falsifier une signature le fait d'en créer une de toutes pièces.
Quelles signatures Ève est-elle capable de falsifier dans ces conditions ?
4. On suppose qu'Ève souhaite falsifier la signature d'un message cible noté m_t qu'elle a aussi réussi à factoriser en fonction des μ_j :
$$m_t = \prod_j \mu_j^{\beta_j}.$$
Montrer comment Ève doit s'y prendre pour falsifier la signature de m_t.

▸ **Exercice 3.** Petit exposant commun

Alice veut envoyer le même message m chiffré par RSA à trois personnes B_1, B_2 et B_3. Chacune de ces personnes B_i utilise un module RSA N_i différent mais tous utilisent le même exposant public $e = 3$. En supposant que leurs modules RSA sont premiers entre eux et que $m^3 < N_1 \cdot N_2 \cdot N_3$, dire comment Ève peut retrouver le message en observant les trois chiffrés qu'Alice aura produit.

▸ **Exercice 4.** Module commun

Alice et Bob ont choisi le même module RSA $N = N_A = N_B$ mais choisissent deux exposants publics différents et premiers entre eux ($e_A \wedge e_B = 1$).

1. Pourrez-vous déclarer votre flamme à Alice ou Bob sans que l'autre soit au courant en utilisant sa clé publique RSA ?
2. On suppose maintenant qu'Alice et Bob reçoivent le même message m chiffré (Alice reçoit $m^{e_A} \mod N$, Bob reçoit $m^{e_B} \mod N$). Pouvez vous retrouver ce message ? Si oui, estimer le coût de votre calcul.