TD Cryptographie à Clé Publique

Chiffrement RSA

Sebastien.Varrette@imag.fr

Dans toute la suite, on pourra utiliser les résultats numériques suivants :
- $319 = 11 \times 29$; $10^{11} = 263 \pmod{319}$; $263^2 = 216 \times 319 + 265$;
- $133^3 = 12 \pmod{319}$; $133^{25} = 133 \pmod{319}$;
- $11^2 = 121 \pmod{280}$; $11^4 = 81 \pmod{280}$; $11^8 = 121 \pmod{280}$; $11^{16} = 81 \pmod{280}$;
- $95 = 64 + 31$; $81.11 = 51 \pmod{280}$; $81.121 = 1 \pmod{280}$.

Exercice 1. [Chiffrement/Déchiffrement RSA]
On considère la clef publique RSA (11, 319), c'est-à-dire pour $n = 319$ et $e = 11$.

1. Quel est le chiffrement avec cette clé du message $M = 100$?
2. Calculer d la clé privée correspondant à la clé publique e.
3. Déchiffrer le message $C = 133$.
4. Le message codé 625 peut-il résulter d'un codage avec la clé publique ? Même question avec la clé privée.

Exercice 2. [Cryptographie RSA et authentification]
Un professeur envoie ses notes au secrétariat de l'École par mail. La clef publique du professeur est (3,55), celle du secrétariat (3,33).

1. Déterminer la clé privée du professeur et du secrétariat de l'Ecole.
2. Pour assurer la confidentialité de ses messages, le professeur chiffre les notes avec la clef RSA du secrétariat. Quel message chiffré correspond à la note 12 ?
3. Pour assurer l'authenticité de ses messages, le professeur signe chaque note avec sa clé privée et chiffre le résultat avec la clef RSA du secrétariat. Le secrétariat recoit ainsi le message 23. Quelle est la note correspondante ?

Exercice 3. [Attaque RSA par exposant commun]
William, Jack et Averell ont respectivement les clefs RSA publiques $(n_W, 3)$, $(n_J, 3)$ et $(n_A, 3)$. Joe envoie en secret à chacun d'eux le même message x avec $0 \leq x < \text{Min}(n_W, n_J, n_A)$.
Montrer que Lucky Luke, qui voit passer sur le réseau $c_W = x^3 \mod n_W$, $c_J = x^3 \mod n_J$ et $c_A = x^3 \mod n_A$ peut facilement calculer x.
Indication. On rappelle (ou on admettra !) que pour a et k entier, la méthode de Newton permet de calculer très rapidement $\lfloor a^{1/k} \rfloor$, en temps $O(\log^2 a)$.

Exercice 4. [Attaque RSA par module commun]
Une implémentation de RSA donne à deux personnes (Alice et Bob) le même nombre n (produit de deux nombres premiers) mais des clefs (e_A, d_A) et (e_B, d_B) différentes. On suppose de plus que e_A et e_B sont premiers entre eux (ce qui est le plus général).

Supposons alors que Alice et Bob chiffrent un même message m et que Oscar intercepte les deux messages $c_A = m^{e_A} \mod n_A$ et $c_B = m^{e_B} \mod n_B$ qu'ille sait être deux chiffrements du même message m.
Montrer qu'Oscar peut alors très facilement découvrir le message m.