D31: Protocoles cryptographiques
TD 2: Cryptosystème RSA

Exercice 1. Généralités

1. Sur quel problème repose la sécurité du protocole RSA? Quelle type de compléxité possèdent les meilleurs algorihtmes pour le résoudre?
2. Rappeler les critères de sécurités que doivent vérifier les différents paramètres du système RSA.

Exercice 2. Chiffrement/déchiffrement

1. Dire si les paramètres privés (p, q, a) suivants sont corrects et, le cas échéant, calculer les paramètres publics correspondants:
   (i) $(5, 7, 5), (ii)$ $(13, 7, 9), (iii)$ $(63, 47, 17), (iv)$ $(229, 257, 125)$
2. Soient les paramètres publics $(n = 187, b = 3)$.
   1. Chiffrer le message $m = 64$
   2. Sachant que $\phi(n) = 160$, retrouver la factorisation de n.

Exercice 3. Variante de RSA (D.R. Stinson, p 227)

Soient $n = pq$, où p et q sont deux premiers impairs disctincts. On définit

$$\lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)}.$$

On mondifie le cryptosystème RSA de sorte que les exposants vérifient désormais $ab \equiv 1 \mod \lambda(n)$.

1. Montrer que les fonctions de chiffrement/déchiffrement fonctionnent toujours.
2. Pour $p = 37$, $q = 79$ et $b = 7$ calculer a dans les deux configurations (originale et modifiée).

Exercice 4. Exposant commun

Soient $A_i, i \in \{1, 2, 3, 4\}$ posédant chacun un module RSA n_i. On suppose qu'ils possèdent tous la même clé de chiffrement $b_i = 4$. Un même message x est chiffré et leur est envoyé a chacun.

1. Montrer qu'en interceptant les différents chiffrés (i.e. $y_i = x^4 \mod n_i$) un attaquant peut déchiffrer le message sans connaître la clé de déchiffrement.
2. Appliquer cette attaque au cas: $n_1 = 38, n_2 = 51, n_3 = 65, n_4 = 77$ et $y_1 = 23, y_2 = 16, y_3 = 40, y_4 = 4$.

Exercice 5. Factorisation de Fermat

On considère un module RSA $n = pq$ (impair) avec $q > p$.

1. On suppose que $q - p = 2d > 0$. Montrer que $n + d^2$ est un carré dans $\mathbb{N}$.
2. Réciproquement, montrer que si l'on parvient à trouver un entier m tel que $m^2 - n$ est un carré parfait, alors peut en déduire la factorisation de n.
3. Déduire de tout ceci un algorithme de factorisation. Montrer que le nombre d'étapes de l'algorithme est environ $\frac{\left(\sqrt{n}-p\right)^2}{2p}$. En particulier, montrer que si $p < q < p + 4\sqrt{p} + 4$ l'algorithme factorise n en une seule étape.

Exercice 6. CRT-RSA

CRT-RSA (Chinese Remainder Theorem RSA) est une manière parallèle d'implanter les fonctions de chiffrements et déchiffrements. On considère les paramètres RSA suivants $K_{pub} = (n, b)$ et $K_{sec} = (p, q, a)$.

1. Soit $x < n$. On définit $x_p = x \mod p - 1$ et $x_q = x \mod q - 1$. Montrer que $m^x \mod p = m^{x_p} \mod p$.
2. À l'aide du CRT, montrer comment obtenir $m^x \mod n$ à partir de $m^{x_p} \mod p$ et $m^{x_q} \mod q$.