TD 7 : RSA

Christina Boura

Exercice 1 *Théorème des restes chinois*
Bob a des poules dans sa maison de campagne. S'il divise le nombre de ses poules par 5, il reste 4 poules. S'il le divise par 8, il en reste 6 et s'il le divise par 9, il en reste 8. Quel est le plus petit nombre de poules que Bob peut avoir ? (Utiliser le théorème des restes chinois).

Exercice 2 *RSA*
Alice et Bob souhaitent utiliser le cryptosystème RSA pour communiquer. Alice choisit $p = 5$ et $q = 7$ comme nombres premiers. Elle choisit $e = 7$ comme exposant public.

1. Montrer que $e = 7$ est un exposant public valide.
2. Trouver l'exposant privé correspondant d.
3. Chiffrer $m = 4$.
4. Déchiffrer $c = 33$.

Exercice 3 *RSA - Connaître $\phi(n)$ c'est connaître p et q*
On suppose que n est un entier naturel non nul dont la décomposition en facteurs premiers est $n = pq$.

1. Montrer explicitement comment obtenir p et q lorsque l'on connaît n et $\phi(n)$.
2. Si $n = 17063$ et $\phi(n) = 16800$, calculer p et q.

Exercice 4 *RSA - Module commun*
On suppose qu'Alice et Bob possèdent des clés publiques RSA avec le même module n, mais avec deux exposants e_A et e_B différents.

1. Montrer qu'Alice peut déchiffrer les messages destinés à Bob.
2. Supposons maintenant que $\text{pgcd}(e_A, e_B) = 1$. Montrer qu'Oscar peut déchiffrer des messages qui sont envoyés à la fois à Alice *et* à Bob.

Exercice 5 *RSA - Petit exposant commun*
Supposons qu'Alice veut envoyer le même message m à trois personnes B_1, B_2 et B_3, en utilisant le cryptosystème RSA. 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 $m^3 < n_1 \cdot n_2 \cdot n_3$, expliquer comment Oscar peut retrouver le message en observant les trois chiffrés qu'Alice aurait produit.

Exercice 6 *RSA- Accélérer le déchiffrement*
Le but de cet exercice est de montrer comment on peut accélérer le déchiffrement du système RSA en utilisant le théorème des restes chinois. Soit $n = pq$ le module RSA et soit d l'exposant privé. Si $c = m^d \mod n$ on note

$$\begin{aligned} c_p &\equiv c \mod p \\ c_q &\equiv c \mod q. \end{aligned}$$

et

$$\begin{aligned} d_p &\equiv d \mod p-1 \\ d_q &\equiv d \mod q-1. \end{aligned}$$

Cette méthode consiste en deux étapes :

1. Calculer

$$\begin{aligned} m_p &\equiv c_p^{d_p} \mod p \\ m_q &\equiv c_q^{d_q} \mod q, \end{aligned}$$

2. Résoudre le système en utilisant le théorème des restes chinois.

$$\begin{aligned} m &\equiv m_p \mod p \\ m &\equiv m_q \mod q. \end{aligned}$$

— En utilisant cette méthode, déchiffrer le message $c = 15$ pour $n = 143 = 11 \cdot 13$ et $d \equiv 103 \mod 120$.

Exercice 7 *RSA en réseau*
Nous souhaitons mettre en place un cryptosystème RSA pour un réseau de n utilisateurs.

1. Combien de nombres premiers doit-on générer ?

2. On veut réduire ce nombre en générant un plus petit ensemble de nombres premiers et faire des combinaisons de deux nombres premiers de cet ensemble : Pour chaque utilisateur on choisit un nouveau couple de nombres premiers afin de constituer sa clé. Montrer comment un utilisateur peut éventuellement factoriser le module d'un autre utilisateur.

3. Montrer comment quelqu'un peut factoriser tous les modules pour lesquels au moins un facteur premier a été utilisé pour former au moins un autre module.