

Feuille d'exercices n° 2

Cryptographie asymétrique : *RSA*

Exercice 1 (exemple). Soit $p = 7$, $q = 11$ et $e = 7$. Calculer la clé privée d associée à la clé publique e , puis chiffrer et déchiffrer le message $m = 4$.

Exercice 2 (le modulo commun). En utilisant le système *RSA*, pourquoi ne peut-on pas attribuer à différents utilisateurs des couples clé publique/clé privée (e_1, d_1) , (e_2, d_2) , ... modulo un même entier n ?
Indication : considérer que deux clés publiques e_1 et e_2 sont des entiers premiers entre eux ; montrer comment retrouver le message en clair.

Exercice 3 (les petits exposants). On considère le système *RSA* avec l'exposant $e = 3$. Supposons qu'un même message M doit être envoyé à trois destinataires. Faut-il attribuer des entiers de modulo *RSA* différents n_1, n_2, n_3 aux trois destinataires, ou est-il préférable d'utiliser le même entier n pour chiffrer le message ?

Exercice 4 (difficulté de découvrir la parité du message en clair). Soit f une fonction de chiffrement *RSA*, c'est-à-dire de la forme :

$$f : \mathbb{Z}_n \rightarrow \mathbb{Z}_n, \quad x \mapsto x^e,$$

avec $n = pq$. On identifie \mathbb{Z}_n avec $\{0, 1, \dots, n-1\}$. On considère la fonction $\delta : \mathbb{Z}_n \rightarrow \{0, 1\}$ définie ainsi :

$$\delta(y) = \begin{cases} 0, & \text{si } 0 \leq f^{-1}(y) < \frac{n}{2}, \\ 1, & \text{si } \frac{n}{2} < f^{-1}(y) \leq n-1. \end{cases}$$

1. Montrer les équivalences :

$$\delta(f(x)) = 0 \iff x \in \left[0, \frac{n}{2}[,$$

$$\delta(f(2x)) = 0 \iff x \in \left[0, \frac{n}{4}[\cup \left[\frac{n}{2}, \frac{3n}{4}[\right.$$

Généraliser à $\delta(f(2^i x))$.

2. Montrer comment transformer tout algorithme polynomial calculant $\delta(y)$ pour tout y en un algorithme polynomial qui calcule $f^{-1}(y)$ pour tout y .
3. En déduire qu'il est aussi difficile de déterminer le dernier bit d'un message en clair à partir du message chiffré par une fonction *RSA* que de déterminer le message en clair tout entier.

Exercice 5 (deux équivalences de la factorisation de n). Soit e et d deux exposants *RSA*, c'est-à-dire tels que $ed = 1 \pmod{\varphi(n)}$, où $n = pq$.

1. Supposons que l'on connaisse e et d mais pas p et q . Trouver une heuristique pour factoriser n .
Indication : chercher une racine b non triviale de 1, sous la forme $b = a^{2^j u}$ où on a écrit $ed - 1 = 2^k u$.
2. Montrer que la connaissance de $\varphi(n)$ est équivalente à connaître la factorisation de n .

Exercice 6 (nombres de Carmichael : critère de Korselt). On appelle *nombre de Carmichael* un nombre n pseudo-premier de Fermat pour toute base ; c'est-à-dire, un entier naturel non nul et composé n tel que $a^n = a \pmod n$ pour tout entier $a > 0$. On se propose de démontrer que n est un nombre de Carmichael si et seulement si n est composé, sans facteur (premier) carré, et tel que pour tout facteur premier p de n , on ait aussi $p-1 | n-1$.

1. On suppose que n est de Carmichael. Soit p un facteur premier de n .

- (a) Montrer que p^2 ne divise pas n . *Indication* : utiliser $p^n = p \pmod n$.
 - (b) Montrer que $p - 1 | n - 1$. *Indication* : considérer une racine primitive a modulo p , et montrer que $a^{n-1} = 1 \pmod p$.
2. Soit maintenant un entier $n > 0$, composé, sans facteur carré et tel que $p - 1 | n - 1$ pour tout facteur premier p de n . Montrer que n est Carmichael. *Indication* : remarquer qu'il suffit de montrer $a^n = a \pmod p$ pour tout facteur premier p de n ; puis distinguer suivant les cas où a est divisible ou non par p .

Exercice 7 (attaque RSA : clés trop proches). Soit $n = pq$ un modulo RSA.

1. Montrer que factoriser n est équivalent à trouver un entier x tel que $x^2 - n$ est un carré.
2. En supposant $q < p < (1 + \epsilon)\sqrt{n}$, évaluer le nombre d'entiers à tester pour trouver un carré permettant de factoriser n .

Exercice 8 (sur les racines carrées de 1 modulo n). On détermine le nombre de racines carrées de 1 modulo n , suivant les valeurs de l'entier n .

1. Montrer que si n est de la forme $n = p^\alpha$ ou $n = 2p^\alpha$ avec $p \geq 3$ premier, alors l'équation $x^2 = 1 \pmod n$ a exactement 2 solutions.
2. Montrer que, si n n'est pas de la forme précédente, alors il existe un entier $x \not\equiv \pm 1 \pmod n$ tel que $x^2 = 1 \pmod n$.
3. Déterminer le nombre de racines distinctes de 1 dans $\mathbb{Z}/n\mathbb{Z}$, lorsque $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ avec les p_i tous distincts et premiers.

Exercice 9 (RSA : factorisation et racines carrées). On suppose qu'on dispose d'un algorithme permettant d'extraire une racine carrée modulo n en temps polynomial. En déduire un algorithme probabiliste permettant de factoriser le modulo RSA n en un temps d'espérance polynomiale. Préciser les hypothèses sur l'algorithme de départ.