TD2 : RSA

Le but de ce TD est de prouver le principe fondamental derrière RSA. Ce TD est un peu matheux, mais les preuves sont courtes.

1 Indicatrice d'Euler

Pour un entier n, on dénote $\mathcal{P}(n) = \{k \in \mathbb{N} \mid k \leq n \text{ et } pgcd(k,n) = 1\}$. Autrement dit c'est l'ensemble des entiers plus petit que n qui son premier avec n. On dénote $\phi(n)$ la fonction indicatrice d'Euler, définie par $\phi(n) = card(\mathcal{P}(n))$

1. Calculer $\phi(8)$, $\phi(12)$ et $\phi(13)$.
2. Pour p un nombre premier que vaut $\phi(p)$? Et pour k un entier, que vaut $\phi(p^k)$?
3. Soient a et b deux entiers tels que $pgcd(a,b) = 1$. Montrer que $\phi(a \times b) = \phi(a) \times \phi(b)$
4. Soit n un entier. On rappelle que tout entier peut être décomposer comme une multiplication de nombre premiers : $n = \prod_{i=1}^{m} p_i^{k_i}$. Donner l'expression de $\phi(n)$.

2 Théorème d'Euler

Le théorème d'Euler est une généralisation du petit théorème de Fermat. Ici nous allons prouver le petit théorème de Fermat et admettre la généralisation du théorème d'Euler.

1. Soit k un entier. Montrez que pour tout p premier, $(k+1)^p = k^p + 1 \mod p$. (On conseille de se rappeler de l'identité remarquable, ou de regarder celle qui est en fin du paragraphe statement sur la page wikipedia https://en.wikipedia.org/wiki/Binomial_theorem#Statement)
2. Montrez le petit théorème de Fermat :
   Soit p un nombre premier, et a un entier, alors $a^p = a \mod p$. (Montrez le par récurrence sur a).
3. Le théorème d'Euler-Fermat est comme suit :
   Soient p et a des entiers premiers entre eux, alors $a^{\phi(p)} = 1 \mod p$.
   On admet que ce théorème est vrai, montrez que cela implique que le petit théorème de Fermat est vrai.

3 Protocole RSA

Soit p et q deux entiers premiers, on note $n = p \cdot q$.

1. Que vaut $\phi(n)$?
2. On choisit e premier avec $(p-1)(q-1)$. Montrez l'existence d'un entier d tel que $e \cdot d = 1 \mod \phi(n)$.
   (On rappelle le théorème de Bézout : Pour 2 entiers a et b, il existe 2 entiers relatifs u et v tels que $au + bv = pgcd(a, b)$.)
3. Montrez que pour tout entier m, $m^{e \cdot d} = m \mod n$

4 Chiffrement RSA

On rappelle comment fonctionne RSA basiquement :

— On génère un entier n qui est le produit de 2 nombres premiers p et q.

— On génère un entier e premier avec $(p-1) \times (q-1)$. On note (e, n) la clef publique.

— On trouve un entier d tel que $e \times d = 1$ mod $(p-1) \times (q-1)$. On note (d, n) la clef privée.

— On chiffre un message m par m^e mod n, et on déchiffre un message m par m^d mod n.

On vient de prouver pourquoi $m^{e \times d} = m$ mod n.

1. Chiffrez 21 avec la clef publique $(103, 143)$.
2. Décomposez 143 comme un produit de 2 nombres premiers et calculez la clef privée associée à $(103, 143)$.
3. Déchiffrez le message 13.

5 Attaquer RSA

Supposon que vous ayez obtenu une clef publique (e, n) de quelqu'un qui utilise RSA.
Comment feriez-vous pour retrouver la clef privée (d, n) ? Quelles sont les potentielles difficultés d'un point de vue informatique ?