Sécurité Appliquée : chiffrement asymétrique, TD

Jean-François COUCHOT
couchot[arobase]femto-st[point]fr

1 Application directe de RSA

Exercice 1.1. *Rejouer RSA. Dans cet exercice, on considère tous que l'on a tiré les nombres $p = 23$ et $p = 43$.*

1. *Montrer que la clef publique $K_A = (65, 989)$ est acceptable.*
2. *Trouver la clef privée associée.*
3. *Chiffrer le nombre 520.*
4. *Déchiffrer le nombre 1\|\|624.*

2 Factorisation de grands nombres

Exercice 2.1. *On considère que l'étape 1 de l'algorithme RSA a généré deux grands nombre premiers p et q proches tels que $p > q$. On définit $t = \frac{p+q}{2}$ et $s = \frac{p-q}{2}$. L'objectif de cet exercice est de montrer que si les nombres p et q sont trops proches l'un de l'autre, alors il est possible de factoriser n, produit de p et de q. Montrer que*

1. *t et s sont des entiers ;*
2. *le produit $n = pq = t^2 - s^2$;*
3. *l'entier s est petit et que t est légèrement supérieur à la racine carrée de n*
4. *que l'on peut utiliser ces informations pour factoriser n c.-à-d. retrouver p et q ; pour cela, on pourra commencer par choisir $t = \lceil \sqrt{n} \rceil$, puis faire croître t jusqu'à...*
5. *Factoriser 1643, 8968261 et 318040531.*

3 Un autre chiffrement asymétrique

Exercice 3.1. *Un chiffrement simple.*

On considère l'algorithme suivant : Alice choisit deux nombres premiers p et q distincts tels que $p \equiv 2[3]$ et $q \equiv 2[3]$. Elle calcule $n = pq$ et partage le résultat n.

Les message que Bob peut envoyer à Alice sont les nombres $m \in \{1, ..., n-1\}$ tel que $\text{pgcd}(m, n) = 1$.

Bob chiffre le message en calculant $a \equiv m^3 \bmod n$ et renvoie a.

Alice déchiffre a en calculant

$$m' \equiv a^d \bmod n \text{ où } d = \frac{2(p-1)(q-1)+1}{3}$$

Normalement m doit être égal à m'.

1. *Dans cet algorithmes, quelles sont les clefs ?*
2. *Choisir $p = 11$, $q = 5$, $m = 4$ puis construire le chiffré a. Déchiffrer ensuite a.*
3. *Montrer que d est toujours un entier.*
4. *Expliquer pourquoi a et m' ne sont pas divisibles par n.*
5. *Montrer que l'algorithme est correct.*