M13 – Algèbre et arithmétique

Devoir à la maison — RSA
À rendre la semaine du 2 avril 2007

La rédaction d'un devoir à la maison est un élément fondamental de l'appréciation. Vous devez rendre un devoir parfaitement rédigé et présenté.

Le système RSA (pour Rivest-Shamir-Adleman) a été inventé en 1977 et permet de crypter des messages sans échange de clé secrète préalable.

Description du protocole.

1) Alice veut envoyer un message secret m à Bob.
2) a. Bob choisit deux grands nombres premiers p_1 et p_2 différents.
   b. Bob calcule $n = p_1 p_2$ et $\varphi(n) = (p_1 - 1)(p_2 - 1)$.
   c. Bob choisit un nombre e premier avec $\varphi(n)$.
   d. Bob calcule un nombre d tel que $ed \equiv 1 \mod \varphi(n)$.
3) Bob envoie e et n à Alice (c'est la clé publique).
4) Pour envoyer son message m (qui est un nombre entier modulo n) à Bob, Alice calcule le message crypté $c \equiv m^e \mod n$ et envoie c à Bob.
5) Bob reçoit c et calcule $m \equiv c^d \mod n$.

Exercice 1. Vérification du protocole
1) Expliquer comment Bob peut calculer d après avoir choisi e.
2) Montrer que deux nombres sont égaux modulo n si et seulement si ils sont égaux modulos p_1 et p_2.
3) Montrer que pour tout $x \in \mathbb{Z}/p_1\mathbb{Z}$ et pour tout $\alpha \equiv 1 \mod (p_1 - 1)$, $x^\alpha \equiv x \mod p_1$.
4) En déduire que pour tout $x \in \mathbb{Z}/n\mathbb{Z}$, $x^{ed} \equiv x \mod n$.
5) Montrer que Bob décrypte effectivement le message de Alice.

Exercice 2. Exemple d'application du protocole
Bob choisit $p_1 = 13$, $p_2 = 19$, et $e = 5$. Alice envoie le message

```
67 184 166 232 79 20
```

À vous de déchiffrer le message ! En détaillant vos calculs.
(Alice a transformé chaque lettre de son message en un nombre en utilisant la table ASCII)

Exercice 3. Attaques contre le protocole
1) Montrer que si l'espionne Ève arrive à calculer $\varphi(n)$ alors elle peut facilement calculer p_1 et p_2.
2) Décrire un algorithme pour factoriser n. Ève peut-elle utiliser cet algorithme pour un nombre, n, de 1024 bits ?