Système de cryptographie RSA

Exercice 1. Dans un cryptosystème utilisant la méthode RSA, déterminer la clef secrète $(\varphi(n), d)$ et le message envoyé $M \in \mathbf{Z}/n\mathbf{Z}$ pour les clefs publiques (n, e) et les messages reçus $C = M^e$ suivants :

1. $n = 35$, $e = 5$, $C = 10$.
2. $n = 265$, $e = 139$, $C = 10$.
3. $n = 667$, $e = 493$, $C = 10$.
4. $n = 3599$, $e = 31$, $C = 60$.

Exercice 2. 1. On considère le cryptosystème (sans clef) suivant. Un grand nombre premier p est public et les unités de message sont des entiers m, $1 \leq m < p$. Si Alice veut envoyer un message m à Bob, elle procède comme suit (on suppose que les transmissions s'effectuent sans erreurs) :

(i) Alice choisit un entier a tel que $1 \leq a < p$ et $\text{pgcd}(a, p) = 1$.
Elle calcule l'inverse a' de a dans $\mathbf{Z}/(p-1)\mathbf{Z}$ et envoie $C = m^a \bmod p$ à Bob.

(ii) Bob choisit un entier b tel que $1 \leq b < p$ et $\text{pgcd}(b, p) = 1$.
Il calcule l'inverse b' de b dans $\mathbf{Z}/(p-1)\mathbf{Z}$ et renvoie $D = C^b \bmod p$ à Alice.

(iii) Alice envoie $E = D^{a'} \bmod p$ à Bob.

Bob calcule $E^{b'} \bmod p$ et retrouve m. Pourquoi ?

2. Soit $p = 31$.

a) Quels sont les ordres multiplicatifs possibles des éléments de $U_{31} = (\mathbf{Z}/31\mathbf{Z})^*$? Donner les ordres multiplicatifs de 2 et 4.

b) Soit $\mathcal{A}$ l'ensemble des entiers x, $1 \leq x < 31$, tels que $\text{pgcd}(x, 30) = 1$. Calculer le cardinal de $\mathcal{A}$ puis énumérer tous ses éléments, ainsi que leurs inverses modulo 30.

c) Trouver $b \in \mathcal{A}$, $b \neq 1$ tel que $4^b \equiv 4 \pmod{31}$.

d) On utilise le cryptosystème du **1.** avec $p = 31$. Un *pirate* intercepte les échanges entre Alice et Bob et connait $C = 4$, $D = 4$ et $E = 8$. Montrer qu'il peut facilement retrouver m, dont on donnera la valeur.

Exercice 3. Alice et Bob communiquent en utilisant la méthode RSA. Bob cherche donc deux nombres premiers p et q, et calcule leur produit $n = 253$. Il rend public le couple $(n, 13)$.

1. Quelle est la clef secrète de Bob ?

2. Alice veut transmettre le message $m = 2$ à Bob ; quel message M ce dernier va-t-il recevoir ?

3. Pour chacun des messages M' suivants reçus par Bob, quel est le message m' initial qu'Alice lui a envoyé ?

a) $M' = 22$;

b) $M' = 18$.

Exercice 4. 1. Soient p et q deux nombres premiers distincts tels que $p \equiv q \equiv 2 \pmod 3$. Montrer que $2(p-1)(q-1)+1$ est divisible par 3.
On pose $k = \varphi(pq)$. Calculer l'inverse d dans $\mathbf{Z}/k\mathbf{Z}$ de $e = \frac{2(p-1)(q-1)+1}{3}$.
2. Soient $p = 17,\ q = 11$ On pose $n = pq$. Alice et Bob communiquent en utilisant la méthode RSA. La clef publique de Bob est $(n, 107)$.

a) Quelle est sa clef secrète ?

b) Alice veut transmettre le message M à Bob. Bob reçoit $C = 9$. Quel était le message M envoyé par Alice ?