Mathématiques pour l'informatique
Arithmétique

Durée : 1h30.

22 Avril 2011

Exercice 1 :
Déterminer tous les solutions, si elles existent, de l'équation diophantienne :

$$122x + 343y = 3.$$

Exercice 2 :
Un entier $a \in \mathbb{Z}/n\mathbb{Z}$ est un carré modulo n s'il existe un entier $x \in \mathbb{Z}/n\mathbb{Z}$ solution de l'équation $x^2 \equiv a[n]$.
Dans ce cas on dit que x est une racine carré de a modulo n.

1. Trouver les racines carrées de 1 et -1 modulo $n = 7$.
2. Soit n un nombre premier impair.
   (a) Montrer que $a \in \mathbb{Z}/n\mathbb{Z}$ est un carré si, et seulement si,
   $$a^{\frac{n-1}{2}} \equiv 1[n].$$
   (b) Pour $n = 139$, quels sont parmi les nombres $a = 106$ et $a' = 97$ ceux qui sont des carrés
3. Soit n un nombre premier congru à 3 modulo 4 et a un carré modulo n.
   (a) Montrer que les deux racines de a modulo n sont données par $\pm a^{\frac{n+1}{4}}[n]$.
   (b) Calculez, si elles existent, les racines carrés modulo 139 de $a = 106$ et $a' = 97$.

Exercice 3 :
On considère la clef publique RSA $(11, 319)$, c'est à dire pour $n = 319$ et $e = 11$.

1. Quel est le chiffrement avec cette clé du message $M = 100$?
2. Calculer d la clé privée correspondant à la clef publique e.
3. Déchiffrer le message $C = 133$.
4. Le message codé 625 peut-il résulter d'un codage avec la clef publique ? Même question avec la clé privée.

Exercice 4 :
Un professeur envoie ses notes au secrétariat de l'École par mail. La clef publique du professeur est $(3, 55)$, celle du secrétariat $(3, 33)$.

1. Vérifier que la clef privée du professeur (supposée connue de lui seul) est 27 ; et que celle du secrétariat est 7.
2. Pour assurer la confidentialité de ses messages, le professeur chiffre les notes avec la clef du secrétariat. Quel message chiffré correspond à la note 8 ?
3. Pour assurer l'authenticité des messages contenant les notes, le professeur signe ses messages pour le secrétariat après les avoir chiffrés. Le secrétariat reçoit le message $(XX|9$ où 9 est la signature.
   Quelle est la note correspondante ?