Mathématiques pour l'informatique
Évaluation intermédiaire

Durée : 1 heure.

4 décembre 2024

Exercice 1 :

1. Écrire 103 en base 2.
2. Décomposer 143 en facteurs premiers.
3. Calculer le pgcd d de 103 et 120 et déterminer des entiers u et v tels que $120u+103v = d$.
4. Soit a et n des entiers relatifs. À quelle condition existe-t-il un entier x tel que $ax \equiv 1[n]$?
5. Déterminer tous les entiers x compris entre 0 et 119 tels que $103x \equiv 1[120]$.
6. Rappeler l'énoncé du petit théorème de Fermat.
7. Trouver $a \in \{0, 1, \ldots, 12\}$ tel que $27^{103} \equiv a[13]$.
8. Trouver $b \in \{0, 1, \ldots, 10\}$ tel que $27^{103} \equiv b[11]$.
9. Calculer le reste de la division euclidienne de 27^{103} par 143.
10. Juliette et Roméo ont lu dans la revue *Pour la Science* un article sur le principe de cryptographie RSA. Ils décident de le tester sur un exemple simple pour vérifier qu'ils ont compris. Pour cela, Juliette choisit la clef publique ($n = 143$, $c = 7$; Roméo choisit alors un entier, compris entre 0 et 142, puis le code avant de transmettre à Juliette le résultat : 27.
    Pouvez-vous aider Juliette à retrouver l'entier choisi par Roméo ? Justifiez soigneusement votre réponse ; en particulier, rappelez le principe du codage et du décodage et calculez la clef secrète qui permet le décodage.
    Vous pourrez bien sûr utiliser les questions précédentes.

Exercice 2 :
Soit p et q deux nombres premiers distincts tels que

$$p \equiv 2[3] \quad q \equiv 2[3].$$

1. Montrer que $2(p-1)(q-1)+1$ est divisible par 3.
2. On pose $k = \phi(pq)$. Calculer l'inverse d dans $\mathbb{Z}/k\mathbb{Z}$ de

$$e = \frac{2(p-1)(q-1)+1}{3}.$$

3. Soit $p = 17$ et $q = 11$. On pose $n = pq$. Alice et Bob communiquent en utilisant l'algorithme RSA.
   (a) La clef publique de Bob est $(107, n)$. Quelle est sa clef secrète ?
   (b) Alice veut transmettre le message M à Bob, Bob reçoit $C = 9$.
   (c) Quel était le message M envoyé par Alice ?