Université du Sud Toulon-Var — Licence d'Informatique

I 23 : Mathématiques discrètes

Examen - 1ère session 2008/2009.

Lundi 2 juin 2008

Les documents sont interdits. La calculatrice est autorisée. Le barème est approximatif et il est donné à titre indicatif.

Exercice 1. [4pts] Calculer le reste de la division euclidienne de 731^{8732} par 11.

Exercice 2. [6pts]

1. [1pt] Décomposer l'entier 539 en produit de facteurs premiers en utilisant les critères de divisibilité par étudiés en TD.

2. [1pt] Calculer le nombre d'éléments inversibles de l'anneau $\mathbf{Z}/539\mathbf{Z}$ en utilisant les propriétés de la fonction indicatrice d'Euler ϕ.

3. [1pt] Alice utilise le chiffrement affine dans $\mathbf{Z}/539/\mathbf{Z}$ pour communiquer avec Bob. La fonction de chiffrement $e : \mathbf{Z}/539\mathbf{Z} \to \mathbf{Z}/539\mathbf{Z}$ est définie par

$$e(x) := ax + b, \tag{1}$$

où le couple $k := (a, b) \in \mathbf{Z}/539\mathbf{Z} \times \mathbf{Z}/539\mathbf{Z}$ constitue la clef secrète connue uniquement d'Alice et Bob. Calculer la taille de l'espace des clefs k possibles pour que Bob soit à même de pouvoir déchiffrer le message $y := ax + b$.

4. [1pt] Alice peut-elle utiliser la valeur $a = 91$ pour constituer une clef secrète avec Bob ? Et la valeur $a = 68$?

5. [2pts] Bob reçoit le message secret $y = 27$ avec la clef secrète $(a, b) = (68, 5)/$. Déchiffrer le message clair d'Alice.