ENSIM
3A Informatique

Mercredi 05 Octobre 2016
de 13h45 à 15h00

L'usage de tout instrument électronique est interdit

Les calculs devront être détaillés et ***s'appuyer sur des algorithmes vus en cours !***

Le seul document autorisé est une feuille A4 recto/verso manuscrite

Exercice 1. Donner **toutes** les solutions dans $\mathbb{Z}^2$ de l'équation $13x + 12y = 2$.

Exercice 2. Calculer les inverses de 5 et 13 dans $\mathbb{Z}/87\mathbb{Z}$.

Exercice 3. Déterminer la plus petite solution positive $x \in \mathbb{N}$ du système

$$\begin{cases} x \equiv 1 \text{ dans } \mathbb{Z}/7\mathbb{Z} \\ x \equiv 5 \text{ dans } \mathbb{Z}/11\mathbb{Z}. \end{cases}$$

Exercice 4. Montrer que 3 est un générateur de $(\mathbb{Z}/17\mathbb{Z})^*$.
Calculer le logarithme discret $\log_3 2$ dans $(\mathbb{Z}/13\mathbb{Z})^*$.

Exercice 5. Considérons les nombres $p = 7$, $q = 13$, $e = 7$.

- Calculer les clefs publique et privée avec ces données pour un cryptage avec RSA.
- Coder le message $m = 2$ en utilisant la clef publique.
- Décoder le message obtenu à la question précédente (justifier le résultat par le calcul !).

Exercice 6. Supposons avoir intercepté le message $M = 2$ codé avec RSA pour la clef publique $(551, 121)$. Quel est le message d'origine ?