M1MI2016 : Codes et cryptologie

DS n°2

22 avril 2013, durée 1h30

Documents interdits, calculatrices autorisées

Exercice 1. Résoudre le système de congruences :

$$\begin{cases} x & \equiv 1 \mod 3 \\ x & \equiv 2 \mod 11 \\ x & \equiv 51 \mod 61 \end{cases}$$

Exercice 2. Montrer que pour tout $n \in \mathbb{Z}$, on a $n^7 \equiv n \mod 42$ (on pourra utiliser le théorème chinois).

Exercice 3. On pose

$$\begin{aligned} f : \mathbb{Z}/256\mathbb{Z} &\to \mathbb{Z}/256\mathbb{Z} \\ x &\mapsto 137x + 187 \end{aligned}$$

et pour $n \in \mathbb{N}_{>0}$, on note $f^{(n)}$ la fonction f itérée n-fois, c'est-à-dire $\underbrace{f \circ f \circ \cdots \circ f \circ f}_{n \text{ fois}}$.

(1) Calculer $f^{(2)}$.

(2) Montrer par récurrence sur $k \in \mathbb{N}$ qu'il existe des suites $(a_k)_{k\in\mathbb{N}}$ et $(b_k)_{k\in\mathbb{N}}$ d'éléments de $\mathbb{Z}/256\mathbb{Z}$ telles que :

$$f^{(2^k)}(x) = a_k x + b_k$$

pour tout $x \in \mathbb{Z}/256\mathbb{Z}$ (on précisera la valeur de a_{k+1} en fonction de a_k, et celle de b_{k+1} en fonction de a_k et de b_k).

(3) Calculer les valeurs de a_k et de b_k pour $0 \leq k \leq 8$ (il est conseillé de présenter le résultat sous la forme d'un tableau). En déduire que pour tout $x \in \mathbb{Z}/256\mathbb{Z}$, on a $f^{(256)}(x) = x$.

(4) On considère le générateur linéaire congruentiel dans $\mathbb{Z}/256\mathbb{Z}$ donné par la récurrence linéaire :

$$x_{n+1} = f(x_n) = 137x_n + 187$$

Montrer que toutes les suites engendrées par ce générateur sont de période 256, quelle que soit leur initialisation.

(5) Montrer que l'application $f^{(2^7)}$ n'a pas de point fixe (*ie* d'élément $x \in \mathbb{Z}/256\mathbb{Z}$ tel que $f^{(2^7)}(x) = x$). En déduire que la plus petite période de $(x_n)_{n\in\mathbb{N}}$ vaut 256 (on pourra d'abord montrer qu'elle divise 256).

Exercice 4. Alice et Bob communiquent en utilisant le protocole RSA. La clé publique de Bob est $N = 209$ et $e = 7$.

(1) Alice veut transmettre le message $m = 5$ à Bob : quel message M va-t-il recevoir ?

(2) Quelle est la clé secrète de Bob ?

(3) Bob reçoit $M = 2$: quel est le message m qu'Alice lui a envoyé ?