Université d'Évry Val d'Essonne 2011-2012

M54 algèbre et arithmétique 2

Feuille 9 — Cryptographie dans les corps finis

Exercice 1. On reprend les notations de l'exercice 4 de la feuille 8 et on note $g = -\alpha$ le générateur de $K^\times$ trouvé. Alice et Bob décident d'utiliser $K^\times$ et g pour construire ensemble un secret partagé avec le protocle de Diffie-Hellman.

1. Quels exposants peuvent-il choisir ?
2. Alice choisit 9 comme exposant ; que doit-elle envoyer à Bob ?
3. Bob envoie à Alice l'élément $\alpha^2 - 1$; quelle est le secret partagé d'Alice et Bob ?
4. En utilisant l'exercice cité, trouver l'exposant de Bob et expliquer comment s'est passée la transaction de son point de vue.

Exercice 2. Soient $P = X^4 + X + 1 \in \mathbf{F}_2[X]$ et $K = \mathbf{F}_2[X]/(P)$; on note α la classe de X dans K.

1. Donner la liste des polynômes unitaires irréductibles de degré 2 dans $\mathbf{F}_2[X]$.
2. Montrer que K est un corps ; donner sa caractéritique, son cardinal et une base de K en tant que $\mathbf{F}_2$-espace vectoriel.
3. Montrer que α est un générateur de $K^\times$.
4. Alice choisit d'utiliser $K^\times$ et son générateur $g = \alpha$ pour recevoir des messages avec le cryptosystème El Gamal. Elle chosit 8 comme exposant secret ; quelles informations doit-elle publier ?
5. Bob veut transmettre à Alice le message $m = 1 + \alpha$ en utilisant l'exposant $x = 3$; que doit-il lui envoyer ?
6. Alice reçoit de Bob le message chiffré $\alpha^3, \alpha^3 + \alpha^2 + \alpha$; quelle était le message transmis par Bob ?