Master CSI 2 2013-2014

Crypto avancée : feuille de TD 6

– Exercice 1. Les paramètres d'un système de chiffrement d'El Gamal sont $p = 67$ et $g = 11$. La clé publique de votre destinataire est $P = 22$. Vous souhaitez retrouver le message m correspondant au chiffré $(u, v) = (40, 30)$. Vous demandez à un oracle le déchiffrement du cryptogramme (u', v') avec $u' = ug^2$ et $v' = 2vP^2$. L'oracle répond $m' = 33$: quel est le message m ?

– Exercice 2. On considère le système de chiffrement de Cramer-Shoup avec les paramètres $p = 31$, $q = 5$, $g_1 = 2$ et $g_2 = 4$. On utilise la fonction de hachage $H : (x, y, z) \mapsto x + y + z \bmod 5$.

a) Quel est le sous-groupe G d'ordre 5 de $\mathbb{Z}/31\mathbb{Z}$?

b) Si la clé privée est $x = (1, 2)$, $y = (2, 3)$, $z = (3, 4)$, quelle est la clé publique (a, b, c) associée ?

c) Pour chiffrer le message $m = 16$, l'aléa tiré est $r = 2$. Quel est le message chiffré ?

d) Déchiffrer le cryptogramme $(8, 2, 8, 4)$.

e) Déchiffrer le cryptogramme $(16, 8, 2, 2)$.

f) En supposant que la clé publique est le triplet (a, b, c) calculé ci-dessus, montrer que la clé secrète $(x_1, x_2, y_1, y_2, z_1, z_2)$ appartient à un espace affine de dimension 3 de $\mathbb{F}_q^6$ dont on déterminera les équations.

g) vérifier que la clé secrète $x' = (3, 1)$, $y' = (2, 3)$, $z' = (3, 4)$ est compatible avec la clé publique (a, b, c).

h) Le cryptogramme $(16, 4, 2, 2)$ est-il valide ? Est-il accepté avec la clé secrète (x, y, z) ? Avec la clé secrète (x', y', z') ?

i) Vérifier que si le cryptogramme (u_1, u_2, v, w) est valide, alors il est accepté ou refusé suivant la valeur de w, mais indépendamment de la clé secrète.