Université de Bretagne Occidentale
UFR Sciences et Techniques
L3 DE MATHEMATIQUES

ARITHMÉTIQUE ET APPLICATIONS

Contrôle continu, le 7 mars 2024, 8h00-8h30

CORRIGÉ

Exercice 1. On calcule g^i pour i de 0 à 7 et on s'arrête dès que $g^i = h$ ou $g^i = k$:

$$\begin{aligned} g^0 &= 1 \neq h, k \\ g^1 &= \overline{X+2} \neq h, k \\ g^2 &= (\overline{X+2})^2 = \overline{X^2+X+1} = \overline{X} \neq h, k \\ g^3 &= (\overline{X+2})^3 = \overline{X^3+2^3} = \overline{2X+2} = k \end{aligned}$$

en utilisant Frobenius dans la dernière ligne. On a donc $b \equiv 3$ modulo 8, et la clé secrète est

$$h^3 = (\overline{2X+1})^3 = \overline{2^3X^3+1^3} = \overline{2X^3+1} = \overline{X+1}.$$

Exercice 2. Le groupe multiplicatif $\mathbb{F}_{64}^\times$ est d'ordre $63 = 3^2 \times 7$. Les diviseurs maximaux de 63 sont donc $63/3 = 21$ et $63/7 = 9$. Il suffit de montrer que $\bar{X}^{21} \neq \bar{1}$ et que $\bar{X}^9 \neq \bar{1}$ dans $\mathbb{F}_{64}$.

Or, la divisions euclidienne de X^9 par $X^6+X^4+X^3+X+1$ dans $\mathbb{F}_2[X]$ donne

$$X^9 = (X^3+X+1)(X^6+X^4+X^3+X+1) + X^5+X^4+X^2+1,$$

ce qui veut dire que

$$\bar{X}^9 = \overline{X^5+X^4+X^2+1} \neq \bar{1}.$$

Puis, on calcule $\bar{X}^{21}$ comme $(\bar{X}^9)^2 \cdot \bar{X}^3$:

$$(\bar{X}^9)^2 = (\overline{X^5+X^4+X^2+1})^2 = \overline{X^{10}+X^8+X^4+1}$$

par Frobenius. La division euclidienne de $X^{10}+X^8+X^4+1$ par $X^6+X^4+X^3+X+1$ donne

$$X^{10}+X^8+X^4+1 = (X^4+X)(X^6+X^4+X^3+X+1) + X^4+X^2+X+1.$$

Donc

$$\bar{X}^{18} = \overline{X^4+X^2+X+1}.$$

D'où

$$\bar{X}^{21} = \overline{X^4+X^2+X+1} \cdot \bar{X}^3 = \overline{X^7+X^5+X^4+X^3} = \overline{X^3+X^2+X} \neq \bar{1}$$