Université de Bretagne Occidentale
UFR Sciences et Techniques
L3 DE MATHEMATIQUES

ARITHMÉTIQUE ET APPLICATIONS

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

Documents et calculatrices interdits.

Exercice 1. Alice et Bob souhaitent partager une clé secrète par le biais du protocole de Diffie-Hellman. Alice communique à Bob le corps fini

$$\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2+1)$$

et le générateur

$$g = \overline{X+2}$$

du groupe multiplicatif $\mathbb{F}_9^\times$. Alice et Bob choisissent des entiers a et b respectivement qu'ils gardent secret. Alice calcule $h = g^a$, et obtient et transmet

$$h = \overline{2X+1}.$$

Bob calcule $k = g^b$, et obtient et transmet

$$k = \overline{2X+2}.$$

Déterminer la clé secrète que Alice et Bob partagent.

Exercice 2. Soit

$$\mathbb{F}_{64} = \mathbb{F}_2[X]/(X^6+X^4+X^3+X+1).$$

Montrer que $\bar{X}$ est un générateur du groupe multiplicatif $\mathbb{F}_{64}^\times$ de $\mathbb{F}_{64}$.