Exercises Classical Cryptography 5b

crypto@os3.nl

Thursday, March 5, 2020

(version 19.2, 2020/03/05 14:25:57 UTC)

Problem 1: **Polynomials over finite fields**

(a) Calculate over $\mathbb{Z}_2$:

i. $(X^3 + X^2 + 1) \cdot (X^3 + X + 1)$

ii. $(X^5 + X^3 + 1)/(X^2 + X + 1)$ (quotient plus remainder)

(b) Calculate over $\mathbb{Z}_5$:

i. $(X^3 + 2X^2 + 3) \cdot (X^3 + 2X + 3)$

ii. $(X^5 + X^3 + 1)/(X^2 + X + 1)$ (quotient plus remainder)

Problem 2: **Irreducible and primitive polynomials for the 16 element field**

(a) Find an irreducible polynomial of degree 4 over $\mathbb{Z}_2$.

(b) Find a primitive polynomial of degree 4 over $\mathbb{Z}_2$.

(c) Find a generator for $\mathbb{F}_{16}$ and calculate all its powers.