HAI709I : Fondements cryptographiques de la sécurité, Université de Montpellier, 2023

2 18/09/2023. Homework for Lecture 2.

Exercise 1. Let p be a prime number. A polynomial $f(x) = k + c_1 x + c_2 x^2$ is evaluated et pairwise distinct points a_1, a_2, a_3 modulo p,

$$\begin{array}{rcl} s_1 & = & f(a_1) \mod p, \\ s_2 & = & f(a_2) \mod p, \\ s_3 & = & f(a_3) \mod p. \end{array}$$

Find a formula that returns the value of k given a_1, a_2, a_3 and s_1, s_2, s_3 (you may use in this formula the usual arithmetic operations of addition, subtractions, multiplication, and inversion modulo p).

Exercise 2. Find a quadratic polynomial $f(x) = c_0 + c_x + c_2 x^2$ with integer coefficients (not all coefficients are equal to 0 modulo 35) that has at least three different roots modulo 35, i.e.,

$$f(x_1) = 0 \mod 35,\ f(x_2) = 0 \mod 35,\ f(x_3) = 0 \mod 35.$$

Exercise 3. Let $f(x) = c_0 + c_x + \ldots + c_d x^d$ be a polynomial with integer coefficients such that for some $a \in \{0, 1, \ldots n-1\}$

$$f(a) = 0 \mod n.$$

Prove that there exists a polynomial with integer coefficients $g(x)$ such that

$$f(x) = (x - a) \cdot g(x) \mod n.$$