Crypto 2024. Additional exercises to prepare for the final exam.

Exercise 1. Let $P(x) = a_0 + a_1 x + a_2 x^2$, where each a_i is an integer number from $\{0, \ldots, 16\}$.

(a) It is known that $P(2) = 1 \mod 17$, $P(3) = 2 \mod 17$, $P(4) = 1 \mod 17$. Express these three conditions as three linear equations modulo 17 for the coefficients a_0, a_1, a_2, i.e., fill in the missing coefficients in

$$\begin{cases} \ldots \cdot a_0 + \ldots \cdot a_1 + \ldots \cdot a_2 = \ldots \mod 17, \\ \ldots \cdot a_0 + \ldots \cdot a_1 + \ldots \cdot a_2 = \ldots \mod 17, \\ \ldots \cdot a_0 + \ldots \cdot a_1 + \ldots \cdot a_2 = \ldots \mod 17. \end{cases}$$

(b) Solve this system of linear equations and find a_0, a_1, a_2.

Exercise 2. Let $Q(x) = b_0 + b_1 x + b_2 x^2 + b_3 x^3$, where each b_i is an integer number from $\{0, \ldots, 18\}$. It is known that

$$(*) \qquad Q(5) = 0 \mod 19,\ Q(10) = 0 \mod 19,\ Q(15) = 0 \mod 19.$$

(a) Prove that this polynomial $Q(x)$ can be represented as

$$(**) \qquad Q(x) = c \cdot (x-5)(x-10)(x-15) \mod 19 \text{ (equation holds for all } x \text{ taken from } \{0, \ldots, 18\}),$$

where c is an integer number from $\{0, \ldots, 18\}$.

(b) Explain how to compute the integer coefficient c from (**) given the values b_0, b_1, b_2, b_3.

(c) Show that (*) does not determine uniquely the values of the coefficients b_0, b_1, b_2, b_3.

(d) Compute $b_0 \cdot b_3^{-1} \mod 19$.

Exercise 3. A secret k is a randomly chosen in $\{0,1\}^n$. We need to share this secret among 9 participants of the protocol: the *Queen* and eight *Pawns* such that

- each of the eight groups $\{$Queen, the i-th Pawn$\}$ (for $i = 1, \ldots, 8$) should know the secret ;
- the group that consists of all eight Pawns should know the secret ;
- the Queen alone should get no information on the secret ;
- every group of at most seven Pawns should get no information on the secret.

(a) Construct a secret sharing scheme that matches these requirements.

(b) Construct a secret sharing scheme that matches the given requirements, and each participant receives a share of size at most $2n$ bits.

Exercise 4. We sample at random an n-bit integer number x (all integer numbers from the interval $[2^{n-1}, \ldots, 2^n - 1]$ are equally probable). Using the number-theoretic theorems discussed in the class, show that for large enough n,

$$\mathrm{Prob}[x \text{ is a prime number}] > 1/n^2.$$

Exercise 5. Assume that there exists a "*magic box*" that takes as input an adjacency matrix of a graph and returns immediatly 1, if this graph is 3-colorable, or returns 0, if this graph is not 3-colorable. Propose a polynomial-time algorithm that finds 3-coloring for every 3-colorbale graph with n vertices in time $\mathrm{poly}(n)$ using this *magic box* as a subroutine.

Exercise 6. Assuming that $\mathrm{P} \neq \mathrm{NP}$ and, moreover, one-way functions and pseudo-random generators exit

(a) prove that there is a one-way function f such that for all arguments x the value $y = f(x)$ starts with 0;

(b) prove that there is no pseudo-random generator g such that for all arguments x the value $y = g(x)$ starts with 0.