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

16/10/2023. Homework for Lecture 6.

Exercise 1. Construct a polynomial time deterministic algorithm that takes as input a prime number p and a polynomial with integer coefficients

$$f(x) = c_0 + c_1 x + \ldots c_d x^d$$

(with degree $d < p$) and returns a number $a \in \{0, \ldots, p-1\}$ such that $f(a) \neq 0 \mod p$.

Exercise 2. Let $G : \{0,1\}^{0.5n} \to \{0,1\}^n$ be a function computable by a deterministic algorithm in polynomial time. Assume that there exists randomized polynomial time algorithm Rev that for every $y \in \{0,1\}^n$ in the range of G with a probability $\geq 1/10$ returns an $x \in \{0,1\}^n$ such that $G(x) = y$. Prove that there exists another polynomial time algorithm Rev' that for every $y \in \{0,1\}^n$ in the range of G with a probability $\geq 9/10$ returns an $x \in \{0,1\}^{0.5n}$ such that $G(x) = y$. Show that such a G cannot be a pseudo-random generator.

Exercise 3. (a) Let $G : \{0,1\}^{0.5n} \to \{0,1\}^n$ be a function such that for every $(x_1 \ldots x_{0.5n}) \in \{0,1\}^{0.5n}$ in the bit string $(y_1 \ldots y_n) := G(x_1 \ldots x_{0.5n})$, the first and the last bits (i.e., y_1 and y_n) are equal to each other. Show that G does not satisfy the definition of a pseudo-random generator.

(b) Let $G : \{0,1\}^{0.5n} \to \{0,1\}^n$ be a function such that for every $(x_1 \ldots x_{0.5n}) \in \{0,1\}^{0.5n}$ in the bit string $(y_1 \ldots y_n) := G(x_1 \ldots x_n)$, the number of *ones* is even, i.e., $y_1 \oplus y_2 \oplus \ldots \oplus y_n = 0$. Show that G does not satisfy the definition of a pseudo-random generator.