Introduction to Cryptography - Exercise session 2

Prof. Sebastian Faust

October 31, 2018

The purpose of this exercise session is to get acquainted with the building blocks of Private Key encryption: the concepts of *Negligible functions*, *Pseudo Random Generators* as found in the Chapter 3 of the book.

Recall the definition of a negligible function as it was introduced during the lecture.

Definition 1 *A function $f\colon \mathbb{N} \to \mathbb{R}_{\geq 0}$ is negligible if for any positive polynomial $p(n)$ there exists a natural number $n_0 \in \mathbb{N}$ such that for all $n > n_0$*

$$f(n) < \frac{1}{p(n)}.$$

We call such functions negligible in n and denote $\mathsf{negl}(n)$.

Exercise 1 (Perfect secrecy and indistinguishable encryptions)
Let func_n be a set of all functions $f : \{0,1\}^n \to \{0,1\}^n$ and consider the following encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$:

- On input 1^n , Gen outputs an $f \in \mathsf{func}_n$ uniformly at random.
- Given a key $f \in \mathsf{func}_n$ and a message $m \in \{0,1\}^n$, Enc outputs the ciphertext $c = m \oplus f(0^n)$.
- Given a key $f \in \mathsf{func}_n$ and a ciphertext $c \in \{0,1\}^n$, Dec outputs the plaintext $m = c \oplus f(0^n)$.

Prove that Π is perfectly secret.

Exercise 2 (Negligible function - equivalent definition)
Prove the following equivalence: A function $f\colon \mathbb{N} \to \mathbb{R}_{\geq 0}$ is a negligible function if and only if for every positive integer c, there exists a positive integer n_0 such that for all $n > n_0$

$$f(n) < \frac{1}{n^c}.$$

Exercise 3 (Negligible function)
Assume that $f(n), g(n)$ are two negligible functions in n.

(a) Show that $h_1(n) := f(n) \cdot g(n)$ is also a negligible function in n.

(b) Show that $h_2(n) := f(n) + g(n)$ is also a negligible function in n.

(c) Show that $h_3(n) := |f(n) - g(n)|$ is also a negligible function in n.

(d) Give a concrete example of negligible functions $f(n)$ and $g(n)$ for which $h_4 := \frac{f(n)}{g(n)}$ is *not* a negligible function in n.

(e) Let $q(n)$ be a positive polynomial. Show that $h_4 := q(n) \cdot f(n)$ is a negligible function in n.

(f) Decide if the following functions are negligible in n or not

$$f_1(n) = \frac{n^4 + n^2 + 1}{2^n}, \quad f_2(n) = \frac{1}{2^{1000000}}, \quad f_3(n) = \left| \frac{(-1)^n}{2^n} \right|.$$

Exercise 4 (Pseudorandom Generator)

Let $G\colon \{0,1\}^n \to \{0,1\}^{n+1}$ be a PRG. Define $G'\colon \{0,1\}^{2n} \to \{0,1\}^{2n+2}$ as

$$G'(x_1 \parallel x_2) := G(x_1) \parallel G(x_2),$$

where "$\parallel$" means concatenation. Prove that G' is a PRG.

Exercise 5 (Pseudorandom Generator - Voluntary homework exercise)

Let G be a PRG with expansion factor $l(n) > n$ and let $f : \{0,1\}^* \to \{0,1\}^*$ be a length-preserving bijection (i.e., a permutation) such that f is computable in deterministic polynomial time and define G' as follows:

$$G'(s) := f\big(G(s)\big)$$

Show that G' is a PRG.