CS-E4340 Cryptography: Exercise Sheet 3

Submission Deadline: September 26, 11:30 via MyCourses

Each exercise can give up to two participation points, 2 for a mostly correct solution and 1 point for a good attempt. Overall, the exercise sheet gives at most 4 participation points.

Exercise Sheet 3 is intended to help...

(a) ...understand the definition of pseudorandom functions (PRFs).
(b) ...understand the difference between a PRF and a pseudorandom generator (PRG), which we considered before.
(c) ...familiarize yourself with the notion of a reduction (continued).
(d) ...familiarize yourself with the notion of a negligible function.

Exercise 1 shows PRFs *do* hide their input unlike some other primitives we saw thus far.
Ex. 2 & Ex. 3 concern properties of PRFs and PRGs.
Exercise 2 shows that the existence of PRFs implies the existence of PRGs.
Exercise 3 shows how a quadratic key PRF and PRG can be used to obtain a standard PRF.
Exercise 4 is intended to help with the notions of negligible functions and why they are a convenient notion of a "small" function.

Exercise 1 (**PRFs hide their input**)**.** Let f be a (λ, λ)-PRF, and consider the following transformations:

(a) $h_1(k, x) := f(k, 0||x_{2..|x|})$.
(b) $h_2(k, x) := x_1||f(k, x)_{2..|x|}$.

Task: Show that h_1 and h_2 are not PRFs (even though f is a PRF).
Hint: Find an efficient adversary $\mathcal{A}$ such that $\mathbf{Adv}^{\mathsf{PRF}}_{h,\mathcal{A}}(1^\lambda)$ is non-negligible. (In fact, we can even give an adversary which has advantage almost 1, but this is not required to solve this exercise.)

Exercise 2 (**PRFs imply PRGs**)**.** Let f be a PRF. Define

$$G(z) := f(z, 0^{|z|})||f(z, 1^{|z|}).$$

Task: Prove via reduction, that G is a PRG with output length $|G(z)| = 2\,|z|$.

Exercise 3. (Key Expansion) A *quadratic-key* (λ, λ)-PRF f_q is a PRF which maps a key k of length λ^2, and an input x of length λ to an output y of length λ. Let f_q be a quadratic-key PRF. Let G be a PRG with $|G(z)| = |z|^2$. Define

$$f(k, x) := f_q(G(k), x)$$

Task: Show that f is a (standard) PRF.
Hint: Given a successful distinguisher for the PRF f, show that one of the following is true: (i) There exists a successful distinguisher for the PRG G or (ii) there exists a successful distinguisher for the quadradic-key PRF f_q.

Exercise 4 (**Negligible Functions**)**.** Recall the definition of negligible functions.

Definition 1 A function $\nu : \mathbb{N} \to \mathbb{R}^+_0$ is *negligible* if for all constants c there exists a natural number $N \in \mathbb{N}$ such that for all $n > N$ it holds that $\nu(n) < \frac{1}{n^c}$.

Closer to the verbal description of negligible function given in the lecture notes for lecture 3, we may like to define negligible functions as follows:

Definition 1' A function $\nu : \mathbb{N} \to \mathbb{R}^+_0$ is *negligible* if for all positive polynomials p there exists a natural number $N \in \mathbb{N}$ such that for all $n > N$ it holds that $\nu(n) < \frac{1}{p(n)}$.

Prove at least two out of (a), (b) and (c):

(a) Definitions 1 and 1' of negligible functions are equivalent.
(b) The following are true:
  (i) The sum of two negligible functions is negligible.
  (ii) Multiplying a negligible function by an (arbitrary) positive polynomial yields a negligible function.
  Hint: You may use either of the two definitions in your proof.
(c) (Challenging) There exists a sequence of negligible functions $\nu_\lambda : \mathbb{N} \to [0, 1]$ such that the function $\mu(\lambda) := \sum_{i=1}^{\lambda} \nu_i(\lambda)$ is the constant 1 function, i.e., for all $\lambda \in \mathbb{N}$, it holds that $\mu(\lambda) = 1$.
  Hint: Use diagonalization.