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 $n > n_0$*
>
> $$|f(n)| \leq \frac{1}{p(n)}.$$
>
> *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.

> **Solution:**
>
> We know from the lecture that the one-time pad is perfectly secret, and one can see as follows that the encryption scheme is simply a different way of defining the one-time pad: Guessing a function $f\colon \{0,1\}^n \to \{0,1\}^n$ is the same as guessing 2^n elements from $\{0,1\}^n$(i.e., guessing the image of every element in the domain). We can interpret the outcome of this such that the first string is the image of 0^n under f, which is then nothing else as a random element from $\{0,1\}^n$. This means that picking $f(0^n)$ for uniformly random f is the same as picking uniformly at random some $k \in \{0,1\}^n$. The encryption scheme is then identical to the one-time pad, as claimed.

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 $n > n_0$

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

Solution:

$\Rightarrow$ Let us fix an arbitrary positive integer c. Note that $p_c(n) := n^c$ is a positive polynomial. Hence, by the definition of negligible function, there exist n_0 such that for all $n > n_0$ it holds that $|f(n)| \leq 1/p_c(n) = 1/n^c$.

$\Leftarrow$ Let us fix an arbitrary positive polynomial $p(n)$. Let c and n_1 be two positive integers such that for all $n > n_1$ it holds that

$$p(n) \leq n^c. \tag{1}$$

From our assumption we know that there exists a positive integer n_2 such that for all $n > n_2$ it holds that

$$|f(n)| \leq \frac{1}{n^c}. \tag{2}$$

Let us define $n_0 := \max\{n_1, n_2\}$. Then for all $n > n_0$ if holds that

$$|f(n)| \overset{\text{Eq.(2)}}{\leq} \frac{1}{n^c} \overset{\text{Eq.(1)}}{\leq} \frac{1}{p(n)},$$

which completes the proof.

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.

Solution:
Fix arbitrary $c \in \mathbb{N}$. We need to prove that there exists $n_0 \in \mathbb{N}$ such that for all $n > n_0$ we have $|h_1(n)| < \frac{1}{n^c}$.
Since $f(n), g(n)$ are negligible, then there exist $n_f, n_g \in \mathbb{N}$ such that

$$\forall n > n_f\colon\ |f(n)| < \frac{1}{n^c},$$
$$\forall n > n_g\colon\ |g(n)| < \frac{1}{n^c}.$$

Set $n_0 := \max\{n_f, n_g\}$. Then for every $n > n_0$ it holds

$$|h_1(n)| = |f(n) \cdot g(n)| = |f(n)| \cdot |g(n)| < \frac{1}{n^c} \cdot \frac{1}{n^c} = \frac{1}{n^{2c}} \leq \frac{1}{n^c}.$$

The last inequality holds since for every $n \in \mathbb{N}$ and $c \in \mathbb{N}$ it hold that $n^c \leq n^{2c}$. We complete the proof using the equivalence from Exercise 2.

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

Solution:
Fix arbitrary $c \in \mathbb{N}$. We need to prove that there exists $n_0 \in \mathbb{N}$ such that for all $n > n_0$ we have $|h_1(n)| < \frac{1}{n^c}$.
Since $f(n), g(n)$ are negligible, then there exist $n_f, n_g \in \mathbb{N}$ such that

$$\forall n > n_f\colon\ |f(n)| < \frac{1}{n^{c+1}},$$
$$\forall n > n_g\colon\ |g(n)| < \frac{1}{n^{c+1}}.$$

Set $n_0 := \max\{n_f, n_g, 2\}$. Then for every $n > n_0$ it holds

$$|h_2(n)| = |f(n)+g(n)| \le |f(n)|+|g(n)| < \frac{1}{n^{c+1}} + \frac{1}{n^{c+1}} = 2\cdot\frac{1}{n^{c+1}} \le n\cdot\frac{1}{n^{c+1}} = \frac{1}{n^c}.$$

We complete the proof using the equivalence from Exercise 2.

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

Solution:
Since $|h_3| = |f(n) - g(n)| \le |f(n)| + |g(n)|$, the same proof as for addition works.

(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.

Solution:
For example if $f(n) = g(n) = 2^{-n}$, then $h_4 = 1$.

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

Solution:
Let us fix an arbitrary positive polynomial $p(n)$. We need to find a positive integer n_0 such that for every $n > n_0$ it holds that $|q(n) \cdot f(n)| \le 1/p(n)$.
Since f is a negligible function and $p(n) \cdot q(n)$ is a positive polynomial, we know that there exists a positive integer n_0 such that for every $n > n_0$ it holds that

$$|f(n)| \le \frac{1}{q(n)\cdot p(n)} \tag{3}$$

Hence, for every $n > n_0$ we have that

$$|q(n)\cdot f(n)| = q(n)\cdot|f(n)| \overset{\text{Eq.(3)}}{\le} q(n)\cdot\frac{1}{q(n)\cdot p(n)} = \frac{1}{p(n)}.$$

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

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

Solution:

f_1 **: YES** The function can be written as $f_1(n) = q_1(n) \cdot \mathsf{negl}(n)$, for $q(n) = n^4 + n^2 + 1$ and $\mathsf{negl}(n) = \frac{1}{2^n}$. Since $q(n)$ is a positive polynomial in n and $\mathsf{negl}(n)$ is a negligible function in n, we can use Exercise 3, part (e) to conclude the proof.

f_2**: NO** Consider for example $p(n) = n$. Then for every $n > 2^{1000000}$ it holds that $\frac{1}{p(n)} < \frac{1}{2^{1000000}}$. In general, no constant function can be a negligible function.

f_3**: YES** It holds that $|\frac{(-1)^n}{2^n}| = \frac{1}{2^n}$ which is a negligible function.

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

Solution:

By definition of PRG, need to prove that for every PPT distinguisher D

$$|\Pr[\mathsf{D}(G'(s)) = 1] - \Pr[\mathsf{D}(r) = 1]| \leq \mathsf{negl}(n),$$

where $s \leftarrow \{0,1\}^{2n}$ and $r \leftarrow \{0,1\}^{2n+2}$ are chosen uniformly at random and $\mathsf{negl}(n)$ is a negligible function in n. By definition of the function G', the left hand side of the inequality can be expressed as:

$$\begin{aligned}
|\Pr[\mathsf{D}(G'(s)) = 1] - \Pr[\mathsf{D}(r) = 1]| &= |\Pr[\mathsf{D}(G(s_1)||G(s_2)) = 1] - \Pr[\mathsf{D}(r_1||r_2) = 1] \\
&= \big|\Pr[\mathsf{D}(G(s_1)||G(s_2)) = 1] - \Pr[\mathsf{D}(G(s_1)||r_2) = 1] \\
&+ \Pr[\mathsf{D}(G(s_1)||r_2) = 1] - \Pr[\mathsf{D}(r_1||r_2) = 1]\big| \\
&\leq |\Pr[\mathsf{D}(G(s_1)||G(s_2)) = 1] - \Pr[\mathsf{D}(G(s_1)||r_2) = 1]| \\
&+ |\Pr[\mathsf{D}(G(s_1)||r_2) = 1] - \Pr[\mathsf{D}(r_1||r_2) = 1]|,
\end{aligned}$$

where the last inequality follows from The Triangular Inequality.

Our strategy is to prove the following two statements: for every PPT distinguisher D

$$|\Pr[\mathsf{D}(G(s_1)||G(s_2)) = 1] - \Pr[\mathsf{D}(G(s_1)||r_2) = 1]| \leq \mathsf{negl}_1(n), \quad (4)$$

$$|\Pr[\mathsf{D}(G(s_1)||r_2) = 1] - \Pr[\mathsf{D}(r_1||r_2) = 1]| \leq \mathsf{negl}_2(n) \quad (5)$$

where $(s_1, s_2) \leftarrow \{0,1\}^{2n}$ and $(r_1, r_2) \leftarrow \{0,1\}^{2n+2}$ are chosen uniformly at random and $negl_1, \mathsf{negl}_2$ are two negligible functions in n. Once we prove the above two statements, we get

$$|\Pr[\mathsf{D}(G'(s)) = 1] - \Pr[\mathsf{D}(r) = 1]| \leq \mathsf{negl}_1(n) + \mathsf{negl}_2(n) =: \mathsf{negl}(n)$$

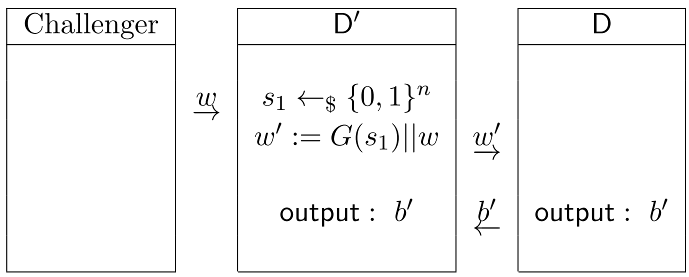
which concludes the proof since sum of negligible functions is a negligible function (viz Exercise 3 b).

Hence, it remains to prove Eq.(4) and (5). Let us begin with Eq.(4). For sake of contradiction, assume that there exists a PPT distingusiher D such that

$$|\Pr[\mathsf{D}(G(s_1)||G(s_2)) = 1] - \Pr[\mathsf{D}(G(s_1)||r_2) = 1]| > \frac{1}{p(n)}$$

for some positive polynomial $p(n)$. We construct a distinguisher D' which distinguishes between random string and output of the function G as follows:

1. Upon receiving a string $w \in \{0,1\}^{n+1}$, choose uniformly at random $s_1 \leftarrow_\$ \{0,1\}^n$, and define $w' := G(s_1)||w$.
2. Send w' to the distinguisher D.
3. Upon receiving a bit b' from D, output b' as your guess.

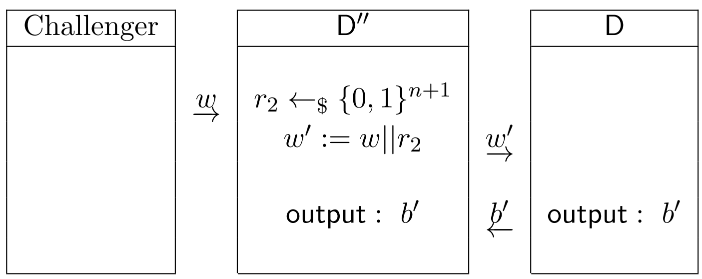


Since D' perfectly simulates the game for D and always outputs the same guess as D, the constructed distinguisher D' wins its game if and only if D wins it game. Hence

$$\begin{aligned}|\Pr[\mathsf{D}(G(s_2)) = 1] - \Pr[\mathsf{D}(r_2) = 1]| &= |\Pr[\mathsf{D}(G(s_1)||G(s_2)) = 1] - \Pr[\mathsf{D}(G(s_1)||r_2) = 1]| \\ &> \frac{1}{p(n)}\end{aligned}$$

which contradicts the assumption that G is a PRG.

The proof of Eq.(5) is very similar. The constructed distinguisher D'' on input $w \in \{0,1\}^{n+1}$, chooses $r_2 \leftarrow_\$ \{0,1\}^{n+1}$ and sends $w' := w||r_2$ to the distinguisher D.



Exercise 5 (Pseudorandom Generator - Voluntary homework exercise)

Let G be a PRG with expansion factor $l(n) > n$ and let $f : \{0,1\}^* \rightarrow \{0,1\}^*$ 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.

Solution:

From the definition of G' it directly follows that the expansion factor of G' is also l. We prove the claim by reduction. Let us assume that G' is not a PRG. Then there exists a ppt distinguisher D' for G' such that there is a polynomial q such that for all n

$$\left| \Pr_{s\leftarrow\{0,1\}^n}[\mathsf{D}'(G'(s)) = 1] - \Pr_{r\leftarrow\{0,1\}^{l(n)}}[\mathsf{D}'(r) = 1] \right| > \frac{1}{q(n)} \tag{6}$$

We construct a distinguisher D for G from D' as follows.

$$\mathsf{D}(t) := 1 \iff \mathsf{D}'(f(t)) = 1$$

As D' is ppt and f is polynomial time computable it follows that D is also ppt. Now we have that for all n:

$$\begin{aligned}
&\left| \Pr_{s\leftarrow\{0,1\}^n}[\mathsf{D}(G(s)) = 1] - \Pr_{r\leftarrow\{0,1\}^{l(n)}}[\mathsf{D}(r) = 1] \right| \\
=&\left| \Pr_{s\leftarrow\{0,1\}^n}[\mathsf{D}'(f(G(s))) = 1] - \Pr_{r\leftarrow\{0,1\}^{l(n)}}[\mathsf{D}'(f(r)) = 1] \right| \\
=&\left| \Pr_{s\leftarrow\{0,1\}^n}[\mathsf{D}'(G'(s)) = 1] - \Pr_{r\leftarrow\{0,1\}^{l(n)}}[\mathsf{D}'(f(r)) = 1] \right| \\
=&\left| \Pr_{s\leftarrow\{0,1\}^n}[\mathsf{D}'(G'(s)) = 1] - \Pr_{r\leftarrow\{0,1\}^{l(n)}}[\mathsf{D}'(r) = 1] \right| \\
>&\frac{1}{q(n)}
\end{aligned}$$

where the third equality follows from the fact that f is a length-preserving bijection and the inequality follows from Equation 6.
This contradicts the fact that G is a PRG, completing the proof.