Introduction to Cryptography - Exercise session 3

Prof. Sebastian Faust

November 7, 2018

The purpose of this exercise session is to recall the concept of: a One-Way Function (OWF), a Pseudorandom Function (PRF) and a symmetric encryption scheme secure under the Chosen Plaintext Attack (CPA). For each of these primitives you can find the recap of the definition in a gray box.

ONE WAY FUNCTION

For a function $f\colon \{0,1\}^* \to \{0,1\}^*$ and for a ppt algorithm $\mathcal{A}$, define the inversion exepriment $\mathbf{Invert}_{\mathcal{A},f}(n)$ as follows:

$\mathbf{Invert}_{\mathcal{A},f}(n)$:

1. Choose $x \leftarrow \{0,1\}^n$ uniformly at random and compute $y := f(x)$.
2. $x' \leftarrow \mathcal{A}(1^n, y)$
3. If $f(x') = y$ output 1, else output 0.

Definition 1 (One Way Function) *A function $f\colon \{0,1\}^* \to \{0,1\}^*$ is one-way if the following holds*

1. *Easy to Compute: $\exists$ ppt algorithm $\mathcal{M}_f$, s.t. $\forall x \in \{0,1\}^*\colon \mathcal{M}_f(x) = f(x)$ and*
2. *Hard to Invert: $\forall$ ppt algorithms $\mathcal{A}$, $\exists$ negl s.t.*

$$\Pr[\mathbf{Invert}_{\mathcal{A},f} = 1] \leq \mathsf{negl}(n).$$

Exercise 1 (One-Way Functions)

Let f, g be arbitrary length-preserving one-way functions (i.e. $|f(x)| = |x|$). For each of the following functions f' decide, whether it is a OWF or not. If yes, give a proof else give a counter-example (assuming one-way functions exist, show that there are one-way function f, g such that f' is not a one-way function).

(a) $f'(x) = f(x) \oplus g(x)$.

(b) $f'(x_1 \parallel x_2) = f(x_2) \parallel 0^n$.

(c) $f'(x) = f(f(x))$.

(d) $f'(x_1, x_2) = f(x_1) \parallel f(x_2)$.

PSEUDORANDOM FUNCTION

Let $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be an efficient, length-preserving, keyed function. F is a *pseudorandom function* if for all probabilistic polynomial-time distinguishers D, there exists a negligible function negl such that:

$$|\Pr[\mathsf{D}^{F_k(\cdot)}(1^n) = 1] - \Pr[\mathsf{D}^{f(\cdot)}(1^n) = 1]| \leq \mathsf{negl}(n)$$

where the first probability is taken over uniform choice of $k \in \{0,1\}^n$ and the randomness of D, and the second probability is taken over uniform choice of $f \in \mathsf{Func}_n$ and the randomness of D.

Exercise 2 (PRF)

For security parameter n, consider the following keyed function $F : \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$. The key is a pair (k_1, k_2), where $k_1, k_2 \in \{0,1\}^n$ and F is defined by

$$F_{(k_1,k_2)}(x) := k_1 \oplus x \oplus k_2.$$

Show that F is not a PRF.

CPA-security

Consider the following experiment defined for any encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, adversary $\mathcal{A}$, and value n for the security parameter:

The CPA indistinguishability experiment $\mathbf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\mathbf{\Pi}}(\mathbf{n})$:

1. A key k is generated by running $\mathsf{Gen}(1^n)$.
2. The adversary $\mathcal{A}$ is given input 1^n and oracle access to $\mathsf{Enc}_k(\cdot)$, and outputs a pair of messages m_0, m_1 of the same length.
3. A uniform bit $b \in \{0,1\}$ is chosen, and then a ciphertext $c \leftarrow \mathsf{Enc}_k(m_b)$ is computed and given to $\mathcal{A}$.
4. The adversary $\mathcal{A}$ continues to have oracle access to $\mathsf{Enc}_k(\cdot)$, and outputs a bit b'.
5. The output of the experiment is defined to be 1 if $b_0 = b'$, and 0 otherwise. In the former case, we say that $\mathcal{A}$ succeeds.

Definition 2 (CPA security) *A private-key encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *has indistinguishable encryptions under a chosen-plaintext attack, or is* CPA-secure*, if for all probabilistic polynomial-time adversaries* $\mathcal{A}$ *there is a negligible function* negl *such that*

$$\Pr[\mathbf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathsf{negl}(n)$$

where the probability is taken over the randomness used by $\mathcal{A}$*, as well as the randomness used in the experiment.*

Exercise 3 (CPA security - Combiner)

Let $\Pi_1 = (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ and $\Pi_2 = (\mathsf{Gen}_2, \mathsf{Enc}_2, \mathsf{Dec}_2)$ be two encryption schemes for which it is known that at least one of them is CPA-secure (but you do not know which one). Show how to construct an encryption scheme Π that is guaranteed to be CPA-secure as long as at least one of Π_1, Π_2 is CPA-secure. Provide a full proof of your solution.

Exercise 4 (CPA-security - Voluntary homework exercise)

Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a deterministic, stateless symmetric encryption scheme. Then the scheme Π is not CPA-secure.