Problem Set 3

Problem 1: Basic properties of PRFs

The set of all functions from n bits to ℓ bits is denoted by

$$\mathsf{Func}_{n,\ell} := \left\{ f : \{0,1\}^n \to \{0,1\}^\ell \right\}.$$

Note that with this definition, we have that Func_n as defined on page 77 of [KL] is equal to $\mathsf{Func}_{n,n}$.

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^\ell$ be a pseudorandom function.

(a) How many functions are there in $\mathsf{Func}_{n,\ell}$?

(b) How many functions $F_k : \{0,1\}^n \to \{0,1\}^\ell$ are there if you vary k?

(c) Let $h(n,\ell)$ denote the fraction of functions F_k among all functions in $\mathsf{Func}_{n,\ell}$. Argue that $h(n,\ell)$ is a negligible function in n. Argue that $h(n,\ell)$ is also negligible in ℓ.

Problem 2: not PRFs

Let us assume that k and x are n-bit strings. For all of the following constructions, explain why they are not PRFs. Give an explicit description of an efficient attacker that distinguishes the given function from a uniform function $f \in \mathsf{Func}_n$.

(a) Let $F_k(x)$ output k.

(b) Let $F_k(x)$ output x.

(c) Let $F_k(x)$ output $x \oplus k$. Program a successful distinguisher in this notebook!

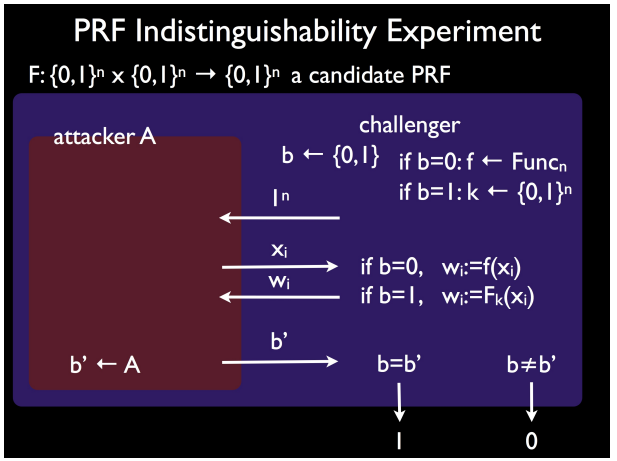

Figure 1: The $\mathsf{PRF}_{\mathcal{A},F}(n)$ experiment

Problem 3: Exercise 3.13

Let F be a keyed function and consider the following experiment:

The PRF indistinguishability experiment $\mathsf{PRF}_{\mathcal{A},F}(n)$**:**, see also Figure 1:

1. *A uniform bit $b \in \{0,1\}$ is chosen. If $b = 1$ then choose uniform $k \in \{0,1\}^n$.*
2. *$\mathcal{A}$ is given 1^n for input. If $b = 0$ then $\mathcal{A}$ is given access to a uniform function $f \in \mathsf{Func}_n$. If $b = 1$ then $\mathcal{A}$ is instead given access to $F_k(\cdot)$.*
3. *$\mathcal{A}$ outputs a bit b'.*
4. *The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise.*

We can give an alternative definition of PRFs using this experiment as follows:

Definition: 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 attackers $\mathcal{A}$, there is a negligible function negl

such that:

$$\Pr[\mathsf{PRF}_{\mathcal{A},F}(n) = 1] \leq \frac{1}{2} + \mathsf{negl}(n)\,,$$

where the probability is taken over the randomness used by $\mathcal{A}$ and the rnadomness used in the experiment (for choosing the bit b as well as f and k).

Prove that the definition above is equivalent to Definition 3.24 in [KL]. **Hint:** For proving the equivalence of the two definitions, argue why the following equalities hold

$$\begin{aligned}
&\Pr[\mathsf{PRF}_{\mathcal{A},F}(n) = 1] \\
&\quad = \Pr[b = 0] \cdot \Pr[0 \leftarrow \mathcal{A}(1^n) | b = 0] + \Pr[b = 1] \cdot \Pr[1 \leftarrow \mathcal{A}(1^n) | b = 1] \\
&\quad = \Pr[b = 0] \cdot \Pr[\mathcal{A}^{f(\cdot)}(1^n) = 0] + \Pr[b = 1] \cdot \Pr[\mathcal{A}^{F_k(\cdot)}(1^n) = 1] \\
&\quad = \frac{1}{2} \Pr[\mathcal{A}^{f(\cdot)}(1^n) = 0] + \frac{1}{2} \Pr[\mathcal{A}^{F_k(\cdot)}(1^n) = 1] \\
&\quad = \frac{1}{2}(1 - \Pr[\mathcal{A}^{f(\cdot)}(1^n) = 1]) + \frac{1}{2} \Pr[\mathcal{A}^{F_k(\cdot)}(1^n) = 1] \\
&\quad = \frac{1}{2} + \frac{1}{2}(\Pr[\mathcal{A}^{F_k(\cdot)}(1^n) = 1] - \Pr[\mathcal{A}^{f(\cdot)}(1^n) = 1])
\end{aligned}$$

and use them in your proof.

Problem 4: Stateful CBC-mode?

Consider a stateful variant of CBC-mode encryption where the sender simply increments the IV by 1 each time a message is encrypted (rather than choosing IV at random each time). Show that the resulting scheme is *not* CPA-secure.

Problem 5: Effects of Communication Errors

(**a**) What is the effect of a single bit flip in the ciphertext when using the CBC, OFB and CTR modes of operation?

(**b**) What is the effect of a dropped ciphertext block (e.g., if the transmitted ciphertext $c_0, c_1, c_2, c_3 \ldots$ is received as $c_0, c_2, c_3, \ldots$) when using the CBC, OFB, and CTR modes of operation?

Problem 6: Exercise 5.1 from [KL]

Show that the CBC, OFB, and CTR modes of operation do not yield CCA-secure encryption schemes (regardless of F). Consider encryptions and decryptions of only single-block messages. Give explicit descriptions of the attacker and compute the success probability.

Problem 7: Combiner for CPA security

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 is CPA-secure (but you don't 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 or Π_2 is CPA-secure. Argue why your construction is secure.

Hint: Generate two plaintext messages from the original plaintext so that knowledge of either one reveals nothing about the original plaintext, but knowledge of both enables the original plaintext to be computed. Try to get some inspiration from the one-time pad!

★ Problem 8: Exercise 3.10 from [KL]

Prove *unconditionally* the existence of a pseudorandom function $F : \{0,1\}^n \times \{0,1\}^{\log(n)} \to \{0,1\}$.

Hint: Implement a *uniform* function with logarithmic input length. Use the function input as index to select part of the key.

★ Problem 9: Exercise 3.18 from [KL]

Define a notion of pefect secrecy against chosen-plaintext attacks by adapting Definition 3.21. Show that the definition cannot be achieved.