CS 346: Cryptography **Fall 2023**

Homework 1: Symmetric Cryptography

Due: September 6, 2023 at 11:59pm (Submit on Gradescope) **Instructor:** David Wu

Instructions. You **must** typeset your solution in LaTeX using the provided template:

`https://www.cs.utexas.edu/~dwu4/courses/fa23/static/homework.tex`

You must submit your problem set via Gradescope (accessible through Canvas).

Collaboration Policy. You may discuss your general *high-level* strategy with other students, but you may not share any written documents or code. You should not search online for solutions to these problems. If you do consult external sources, you must cite them in your submission. You must include the names of all of your collaborators with your submission. Refer to the official course policies for the full details.

Problem 1: Understanding Advantage [24 points]. In this problem, we will get some practice with the notion of advantage. Consider the following two experiments between a challenger and an adversary $\mathcal{A}$:

- **Experiment 0**: In this experiment, the challenger samples a bit $\beta \xleftarrow{R} \{0,1\}$ and gives β to the adversary. The adversary $\mathcal{A}$ outputs a bit $b' \in \{0,1\}$ which is the output of the experiment.
- **Experiment 1**: In this experiment, the challenger gives $\beta = 0$ to the adversary. The adversary $\mathcal{A}$ outputs a bit $b' \in \{0,1\}$ which is the output of the experiment.

For an adversary $\mathcal{A}$ and a bit $b \in \{0,1\}$, we define $W_b = \Pr[\mathcal{A} \text{ outputs 1 in Experiment } b]$. We then define the advantage of $\mathcal{A}$ to be $\mathsf{Adv}[\mathcal{A}] = |W_0 - W_1|$. If the advantage is 1, then that means algorithm $\mathcal{A}$ can perfectly distinguish between the two experiments. If the advantage is 0 for all adversaries $\mathcal{A}$, then the two experiments are identical. If the advantage of every efficient adversary is negligible (with respect to some security parameter), then we say that the two experiments are computationally indistinguishable.

(a) Compute the advantage for each of the following adversaries:

- Algorithm $\mathcal{A}$ always outputs 1.
- Algorithm $\mathcal{A}$ outputs $b' \xleftarrow{R} \{0,1\}$.
- Algorithm $\mathcal{A}$ outputs β.
- Algorithm $\mathcal{A}$ outputs $1 - \beta$.
- Algorithm $\mathcal{A}$ outputs 1 if $\beta = 1$ and $b' \xleftarrow{R} \{0,1\}$ if $\beta = 0$.

(b) What is the maximum possible advantage of any adversary for distinguishing between these two experiments. Give a formal proof of this.

Problem 2: Pseudorandom Generators [25 points]. Let $G\colon \{0,1\}^\lambda \to \{0,1\}^n$ be a secure PRG. For each of the following functions G', indicate whether it is a secure PRG or not. If it is secure, give a *formal* proof. If not, describe an explicit attack.

(a) $G'(s) := G(s) \| (G(s) \oplus 1^n)$, where 1^n denotes the all-ones string of length n.

(b) $G'(s_1 \| s_2) := G(s_1) \oplus G(s_2)$.

(c) $G'(s_1 \| s_2) := s_1 \| G(s_2)$, where $|s_1| = \text{poly}(\lambda)$.

Recall that for two bit-strings $s_1, s_2 \in \{0,1\}^*$, we write $s_1 \| s_2$ to denote the *concatenation* of s_1 and s_2. Please refer to this handout for examples of how to formally show whether a construction is secure or not.

Problem 3: Circular Insecurity [20 points]. Let $(\mathsf{Encrypt}, \mathsf{Decrypt})$ be a semantically-secure cipher with key space $\mathcal{K} = \{0,1\}^\lambda$, message space $\mathcal{M} = \{0,1\}^\lambda$, and ciphertext space $\mathcal{C} = \{0,1\}^n$ (where $n \geq \lambda$). Use $(\mathsf{Encrypt}, \mathsf{Decrypt})$ to construct a new encryption scheme $(\mathsf{Encrypt}', \mathsf{Decrypt}')$with the same key space and message space (but possibly different ciphertext space) that is semantically secure, but is no longer semantically secure if the adversary is given $\mathsf{Encrypt}'(k, k)$.

(a) State your construction of $(\mathsf{Encrypt}', \mathsf{Decrypt}')$ and show that it satisfies correctness.

(b) Prove that $(\mathsf{Encrypt}', \mathsf{Decrypt}')$ satisfies semantic security.

(c) Show how an adversary who knows $\mathsf{Encrypt}'(k, k)$ can break semantic security of $(\mathsf{Encrypt}', \mathsf{Decrypt}')$. Compute the advantage of your attack.

(d) Suppose $(\mathsf{Encrypt}, \mathsf{Decrypt})$ is the one-time pad. Is the one-pad pad semantically secure if the adversary learns the encryption of the secret key? Given an **informal** explanation (i.e., 1-2 sentences suffice).

This problem illustrates that encrypting messages that depend on the secret key of an encryption scheme can be problematic.

Problem 4: Time Spent [1 point]. How long did you spend on this problem set? This is for calibration purposes, and the response you provide does not affect your score.

Optional Feedback. Please answer the following *optional* questions to help us design future problem sets. You do not need to answer these questions. However, we do encourage you to provide us feedback on how to improve the course experience.

(a) What was your favorite problem on this problem set? Why?

(b) What was your least favorite problem on this problem set? Why?

(c) Do you have any other feedback for this problem set?

(d) Do you have any other feedback on the course so far?