Applied Cryptography: Homework 6

(Deadline: 10:00am, 2020/10/28)

Justify your answers with calculations, proofs, and programs.

1. (20 points, question 5.10, page 181 of the textbook)

   Suppose that messages are designated as "safe" or "dangerous" and an adversary is trying to find a collision of one safe and one dangerous message under a hash function h. That is, the adversary is trying to find a safe message x and a dangerous message x' such that $h(x) = h(x')$. An obvious attack would be to choose a set $\mathcal{X}_0$ of Q safe messages and a set $\mathcal{X}'_0$ of Q' dangerous messages, and test the QQ' resulting ordered pairs $(x, x') \in \mathcal{X}_0 \times \mathcal{X}'_0$ to see if a collision occurs. We analyze the success of this approach in the random oracle model, assuming that there are M possible message digests.

   (a) For a fixed value $x \in \mathcal{X}_0$, determine an upper bound on the probability that $h(x) \neq h(x')$ for all $x' \in \mathcal{X}'_0$.

   (b) Using the result from (a), determine an upper bound on the probability that $h(x) \neq h(x')$ for all $x \in \mathcal{X}_0$ and all $x' \in \mathcal{X}'_0$.

   (c) Show that there is a 50% probability of finding at least one collision using this method if $QQ' \approx cM$, for a suitable positive constant c.

2. (10 points, question 5.11, page 181 of the textbook)

   Suppose $h : \mathcal{X} \to \mathcal{Y}$ is a hash function where $|\mathcal{X}|$ and $|\mathcal{Y}|$ are finite and $|\mathcal{X}| \geq 2|\mathcal{Y}|$. Suppose that h is a **balanced hash function** (i.e.,

   $$|h^{-1}(y)|=\frac{|\mathcal{X}|}{|\mathcal{Y}|}$$

   for all $y \in \mathcal{Y}$). Finally, suppose ORACLE-PREIMAGE is an (ϵ, Q) -algorithm for **Preimage**, for the fixed hash function h. Prove that COLLISION-TO-PREIMAGE is an $(\epsilon/2, Q+1)$-algorithm for **Collision**, for the fixed hash function h.

3. (10 points, question 5.12(a), page 181 of the textbook)

   Suppose $h_1 : \{0,1\}^{2m} \to \{0,1\}^m$ is a collision resistant hash function. Define $h_2 : \{0,1\}^{4m} \to \{0,1\}^m$ as follows:

   1. Write $x \in \{0,1\}^{4m}$ as $x = x_1 \| x_2$, where $x_1, x_2 \in \{0,1\}^{2m}$.
   2. Define $h_2(x) = h_1(h_1(x_1) \| h_1(x_2))$.

   Prove that h_2 is collision resistant (i.e., given a collision for h_2, show how to find a collision for h_1).

4. (20 points, question 5.13, page 182 of the textbook)

   In this exercise, we consider a simplified version of the Merkle-Damgard construction. Suppose

   $$\textbf{compress}:\{0,1\}^{m+t} \to \{0,1\}^m,$$

   where $t \geq 1$, and suppose that

   $$x = x_1 \| x_2 \| \cdots \| x_k,$$

where

$$|x_1| = |x_2| = \cdots = |x_k| = t.$$

We study the following iterated hash function:

Algorithm 5.8: SIMPLIFIED MERKLE-DAMGARD (x, k, t)

external compress
$z_1 \leftarrow 0^m \| x_1$
$g_1 \leftarrow \textbf{compress}(z_1)$
for $i \leftarrow 1$ **to** $k - 1$
$\textbf{do} = \begin{cases} z_{i+1} \leftarrow g_i \| x_{i+1} \\ g_{i+1} \leftarrow \textbf{compress}(z_{i+1}) \end{cases}$
$h(x) \leftarrow g_k$
return $(h(x))$

Suppose that **compress** is collision resistant, and suppose further that **compress** is ***zero preimage resistant***, which means that it is hard to find $z \in \{0,1\}^{m+t}$ such that $\textbf{compress}(z) = 0^m$. Under these assumptions, prove that h is collision resistant.