Applied Cryptography: Homework 6

(Deadline: 3:00pm, 2022/03/30)

Justify your answers with calculations, proofs, and programs.

1. (20 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:

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

   (b) 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).

2. (30 points, question 5.13, page 182 of the textbook) In this exercise, we consider a simplified version of the Merkle-Damgård 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:

Alogirithm 1: SIMPLIFIED MERKLE-DAMGÅRD (x, k, t)

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