Introduction to Cryptography

TEK 4500 (Fall 2021)
Problem Set 6

Problem 1.
Read Chapter 11 in [PP] and Chapter 6 in [BR] + Appendix A in [BR] (Birthday problem).

Problem 2.
Suppose we have three different hash functions producing output of lengths 64, 128 and 160 bits. How many random computations do you approximately need to find a collision with probability $p = 0.5$? How many different random hash values do you approximately need to find a collision with probability $p = 0.1$?

Hint: Use whatever formulation of the birthday paradox you want.

Problem 3.
Suppose $H_1, H_2 : \mathcal{M} \to \mathcal{Y}$ are two hash functions for which we know that at least one is collision-resistant. Unfortunately, we don't know which. Consider now the following derived hash functions.

a) $H : \mathcal{M} \to \mathcal{Y} \times \mathcal{Y}$, defined by $H(X) = H_1(X) \| H_2(X)$. Is H collision-resistant? Justify your answer.

b) $H : \mathcal{M} \to \mathcal{Y}$ defined by $H(X) = H_2(H_1(X))$ (here we assume that $\mathcal{Y} \subset \mathcal{M}$). Is H collision-resistant? What about $H(X) = H_1(H_2(X))$? Justify your answer.

Problem 4. [2nd-preimage-resistance]
The two main security properties for hash functions are *collision-resistance* and *one-wayness*. However, there is also a third security property commonly defined for hash functions called *2nd preimage-resistance*. In a 2nd-preimage attack the adversary is given $X \in \mathcal{M}$ and $Y \leftarrow H(X)$, and then asked to find a *different* $X' \in \mathcal{M}$ that hash to the same value as X. That is: given X and Y, find $X' \neq X$ such that $H(X') = H(X) = Y$. In other words, the adversary is asked to find a *second* pre-image for Y, hence the name. See Fig.1 for the formal definitions. Note that 2nd preimage-resistance is a *weaker* security requirement than collision-resistance, i.e., we're asking for *more* from the adversary. Indeed, for finite $\mathcal{M}$ and $\mathcal{Y}$, and assuming $|\mathcal{M}| >> |\mathcal{Y}|$, we have

$\mathbf{Exp}_H^{\mathsf{cr}}(\mathcal{A})$:

$(X_1, X_2) \leftarrow \mathcal{A}_H$
if $X_1 \neq X_2 \wedge H(X_1) = H(X_2)$**:**
  return 1
else
  return 0

$\mathbf{Exp}_H^{\mathsf{2pre}}(\mathcal{A})$:

$X \xleftarrow{\$} \mathcal{M}$
$Y \leftarrow H(X)$
$X' \leftarrow \mathcal{A}_H(X, Y)$
if $X' \neq X \wedge H(X') = Y$**:**
  return 1
else
  return 0

$\mathbf{Exp}_H^{\mathsf{ow}}(\mathcal{A})$:

$X \xleftarrow{\$} \mathcal{M}$
$Y \leftarrow H(X)$
$X' \leftarrow \mathcal{A}_H(Y)$
if $H(X') = Y$**:**
  return 1
else
  return 0

$\mathbf{Adv}_H^{\mathsf{cr}}(\mathcal{A}) = \Pr[\mathbf{Exp}_H^{\mathsf{cr}}(\mathcal{A}) \Rightarrow 1]$
$\mathbf{Adv}_H^{\mathsf{2pre}}(\mathcal{A}) = \Pr[\mathbf{Exp}_H^{\mathsf{2pre}}(\mathcal{A}) \Rightarrow 1]$
$\mathbf{Adv}_H^{\mathsf{ow}}(\mathcal{A}) = \Pr[\mathbf{Exp}_H^{\mathsf{ow}}(\mathcal{A}) \Rightarrow 1]$

Figure 1: Security definitions for *collision-resistance*, *2nd preimage-resistance*, and *one-wayness* for a hash function $H : \mathcal{M} \to \mathcal{Y}$.

$$\text{collision-resistance} \implies \text{2nd preimage-resistance} \implies \text{one-wayness.}$$

a) Explain why the first implication above holds, i.e., why collision-resistance implies 2nd preimage-resistance.

b) Suppose $\{0,1\}^{200} \subset \mathcal{M}$ and that $H : \mathcal{M} \to \mathcal{Y}$ is a collision-resistant hash function. Now define $H' : \mathcal{M} \to \mathcal{Y}$ as follows:

$$H'(X) = \begin{cases} 0^{200} & \text{if } X = 0^{200} \text{ or } X = 1^{200} \\ H(X) & \text{otherwise} \end{cases}$$

Show that H' is 2nd preimage-resistant, but not collision-resistant.

Problem 5.

Suppose that $F : \{0,1\}^m \to \{0,1\}^m$ is a one-way secure *permutation*. Define $H : \{0,1\}^{2m} \to \{0,1\}^m$ as follows. Given $X \in \{0,1\}^{2m}$, write

$$X = X' || X'',$$

where $X', X'' \in \{0,1\}^m$. Then define

$$H(X) = F(X' \oplus X'').$$

Is H one-way? Is it 2nd preimage-resistant? Justify your answers.

Problem 6.

Suppose $H_1 : \{0,1\}^{2m} \to \{0,1\}^m$ is a collision resistant hash function.

a) Define $H_2 : \{0,1\}^{4m} \to \{0,1\}^m$ as follows:

- Write $X \in \{0,1\}^{4m}$ as $X = X_1||X_2$, where $X_1, X_2 \in \{0,1\}^{2m}$
- Define $H_2(X) = H_1(H_1(X_1)||H_1(X_2))$.

Prove that H_2 is collision resistant.

b) For an integer $i \geq 2$, define a hash function $H_i : \{0,1\}^{2^i m} \to \{0,1\}^m$ as follows:

- Write $X \in \{0,1\}^{2^i m}$ as $X = X_1||X_2$, where $X_1, X_2 \in \{0,1\}^{2^{i-1}m}$
- Define $H_i(x) = H_1(H_{i-1}(X_1)||H_{i-1}(X_2))$.

Prove that H_i is collision resistant.

Problem 7. [Problem 11.3 in [Ros]]

I've designed a hash function $H : \{0,1\}^* \to \{0,1\}^n$. One of my ideas is to make $H(X) = X$ if X is an n-bit string (assume the behavior of H is much more complicated on inputs of other lengths). That way, we know with certainty that there are no collisions among n-bit strings. Have I made a good design decision?

Problem 8. [Davies-Meyer alternatives]

Recall that the Davies-Meyer construction is a way of turning a block cipher $E : \{0,1\}^b \times \{0,1\}^n \to \{0,1\}^n$ into a collision-resistant compression function $h : \{0,1\}^{n+b} \to \{0,1\}^n$ as:

$$h(V\|M) = E(M, V) \oplus V.$$

Here we look at some alternative constructions to Davies-Meyer that all turn out to be insecure. For *b*) and *c*) we assume that $b = n$.

a) $h_1(V\|M) = E(M, V)$

b) $h_2(V\|M) = E(M, V) \oplus M$

c) $h_3(V\|M) = E(V, V \oplus M) \oplus V$

Show that none of the compression functions above are collision-resistant.

References

[BR] Mihir Bellare and Phillip Rogaway. *Introduction to Modern Cryptography*. https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.

[PP] Christof Paar and Jan Pelzl. *Understanding Cryptography - A Textbook for Students and Practitioners*. Springer, 2010.

[Ros] Mike Rosulek. *The Joy of Cryptography*, (draft Feb 6, 2020). https://web.engr.oregonstate.edu/~rosulekm/crypto/crypto.pdf.