Announcements

• Midterm
  – Hand back at the end of class.
  – Median was 72/100
  – Solutions are up on canvas

• Extra Credit—up to 15 points added to midterm score
  – 5 min current events presentation. Email me topic + at least one reference before class to get approved. (Up to 5 points added to midterm grade)
  – Summary of a scholarly paper. Sign up sheet will be up by next week. (Up to 10 points added to midterm grade)
Agenda

• This time:
  – Collision-Resistant Hash Functions (K/L 5.1)
  – Hash-and-Mac
  – Class Exercise
Collision Resistant Hashing
Collision Resistant Hashing

Definition: A hash function (with output length $\ell$) is a pair of ppt algorithms $(Gen, H)$ satisfying the following:

- $Gen$ takes as input a security parameter $1^n$ and outputs a key $s$. We assume that $1^n$ is implicit in $s$.
- $H$ takes as input a key $s$ and a string $x \in \{0,1\}^*$ and outputs a string $H^s(x) \in \{0,1\}^{\ell(n)}$.

If $H^s$ is defined only for inputs $x \in \{0,1\}^{\ell'(n)}$ and $\ell'(n) > \ell(n)$, then we say that $(Gen, H)$ is a fixed-length hash function for inputs of length $\ell'$. In this case, we also call $H$ a compression function.
The collision-finding experiment

\[ \text{Hashcoll}_{A, \Pi}(n): \]

1. A key \( s \) is generated by running \( \text{Gen}(1^n) \).
2. The adversary \( A \) is given \( s \) and outputs \( x, x' \). (If \( \Pi \) is a fixed-length hash function for inputs of length \( \ell'(n) \), then we require \( x, x' \in \{0,1\}^{\ell'(n)} \).)
3. The output of the experiment is defined to be 1 if and only if \( x \neq x' \) and \( H^s(x) = H^s(x') \). In such a case we say that \( A \) has found a collision.
Security Definition

Definition: A hash function $\Pi = (Gen, H)$ is collision resistant if for all ppt adversaries $A$ there is a negligible function $\text{neg}$ such that
\[
\Pr[\text{Hashcoll}_{A,\Pi}(n) = 1] \leq \text{neg}(n).
\]
Weaker Notions of Security

- Second preimage or target collision resistance: Given $s$ and a uniform $x$ it is infeasible for a ppt adversary to find $x' \neq x$ such that $H^s(x') = H^s(x)$.

- Preimage resistance: Given $s$ and uniform $y$ it is infeasible for a ppt adversary to find a value $x$ such that $H^s(x) = y$. 
Message Authentication Using Hash Functions
Hash-and-Mac Construction

Let $\Pi = (\text{Mac}, Vrfy)$ be a MAC for messages of length $\ell(n)$, and let $\Pi_H = (\text{Gen}_H, H)$ be a hash function with output length $\ell(n)$. Construct a MAC $\Pi' = (\text{Gen}', \text{Mac}', Vrfy')$ for arbitrary-length messages as follows:

- $\text{Gen}':$ on input $1^n$, choose uniform $k \in \{0,1\}^n$ and run $\text{Gen}_H(1^n)$ to obtain $s$. The key is $k' := \langle k, s \rangle$.
- $\text{Mac}':$ on input a key $\langle k, s \rangle$ and a message $m \in \{0,1\}^*$, output $t \leftarrow \text{Mac}_k(H^s(m))$.
- $\text{Vrfy}':$ on input a key $\langle k, s \rangle$, a message $m \in \{0,1\}^*$, and a MAC tag $t$, output 1 if and only if $Vrfy_k(H^s(m), t) = 1$. 
Security of Hash-and-MAC

Theorem: If $\Pi$ is a secure MAC for messages of length $\ell$ and $\Pi_H$ is collision resistant, then the construction above is a secure MAC for arbitrary-length messages.
Proof Intuition

Let $Q$ be the set of messages $m$ queried by adversary $A$.

Assume $A$ manages to forge a tag for a message $m^* \notin Q$.

There are two cases to consider:

1. $H^S(m^*) = H^S(m)$ for some message $m \in Q$.
   Then $A$ breaks collision resistance of $H^S$.

2. $H^S(m^*) \neq H^S(m)$ for all messages $m \in Q$.
   Then $A$ forges a valid tag with respect to MAC $\Pi$. 