HMAC

• Hash MAC: same security as a MAC
  \[\rightarrow\text{Not PRF}\]

• Apply a hash function H to your original message

• What properties should H satisfy?

\[\exists (m_1, m_2 \ldots m_n) \text{ s.t.} \]
\[H(m_1) = H(m_2) \ldots = H(m_n)\]
In a secure MAC, given \((m_1, \text{tag}_1), (m_2, \text{tag}_2), \ldots, (m_n, \text{tag}_n)\) it is hard to find \((\tilde{m}, \tilde{\text{tag}})\) that passes verification.

**Collision-resistance**

Let \(H: M \rightarrow T\) be a hash function (\(|M| \gg |T|\))

A **collision** for \(H\) is a pair \(m_0, m_1 \in M\) such that:

\[H(m_0) = H(m_1) \text{ and } m_0 \neq m_1\]

A function \(H\) is **collision resistant** if for all PPT algs. \(A:\)

\[\text{Adv}_{CR}[A,H] = \Pr[A \text{ outputs collision for } H] = \text{negl}\]

Example: SHA-256 (outputs 256 bits)
MAC from Collision-resistant Hash Functions

Let \((S,V)\) be a MAC for short messages over \((K,M,T)\) (e.g. AES)

Let \(H: M^{\text{big}} \rightarrow M\)

Def: \((S^{\text{big}}, V^{\text{big}})\) over \((K, M^{\text{big}}, T)\) as:

\[ S^{\text{big}}(k,m) = S(k,H(m)) \quad ; \quad V^{\text{big}}(k,m,t) = V(k,H(m),t) \]

**Thm:** If \(I\) is a secure MAC and \(H\) is collision resistant
then \(I^{\text{big}}\) is a secure MAC.

Example: \(S(k,m) = \text{AES}_{2\text{-block-cbc}}(k, \text{SHA-256}(m))\) is a secure MAC.
MAC from Collision-resistant Hash Functions

\[ S^{\text{big}}(k, m) = S(k, H(m)) ; \quad V^{\text{big}}(k, m, t) = V(k, H(m), t) \]

Collision resistance is necessary for security:

Suppose adversary can find \( m_0 \neq m_1 \) s.t. \( H(m_0) = H(m_1) \).

Then: \( S^{\text{big}} \) is insecure under a 1-chosen msg attack

step 1: adversary asks for \( t \leftarrow S(k, m_0) \)

step 2: output \( (m_1, t) \) as forgery
Protecting File Integrity

Software packages:

\[ \text{package name} \quad \text{package name} \quad \ldots \quad \text{package name} \]

\[ F_1 \quad F_2 \quad \ldots \quad F_n \]

\[ H(m) \rightarrow y \]

\[ \text{read-only public space} \]

\[ 256\text{-bit string} \]

\[ H(F_1) \quad H(F_2) \quad H(F_n) \]

\[ |m| = 2 \text{ bits} \quad 2^2 = 4 \]

\[ |l| = 1 \text{ bit} \quad 2 \]
The birthday attack

Let $H: M \rightarrow \{0,1\}^n$ be a hash function \((|M| \gg 2^n)\).

Generic alg. to find a collision in time $O(2^{n/2})$.

$B =$ output space $= 2^n$

After hashing \((1.2\sqrt{B} \approx 2^{n/2})\) values, the probability that you saw a collision is $\approx 0.5$.
The birthday attack

Let \( H: M \rightarrow \{0,1\}^n \) be a hash function \((|M| >> 2^n)\)

Generic alg. to find a collision in time \(\mathcal{O}(2^{n/2})\) hashes

Algorithm:
1. Choose \(2^{n/2}\) random messages in \(M\): \(m_1, \ldots, m_{2^{n/2}}\) (distinct w.h.p)
2. For \(i = 1, \ldots, 2^{n/2}\) compute \(t_i = H(m_i) \in \{0,1\}^n\)
3. Look for a collision \((t_i = t_j)\). If not found, got back to step 1.

How well will this work?
The birthday attack

Let \( r_1, \ldots, r_n \in \{1, \ldots, B\} \) be indep. identically distributed integers.

**Thm:** when \( n = 1.2 \times B^{1/2} \) then \( \Pr \left[ \exists i \neq j: r_i = r_j \right] \geq \frac{1}{2} \)

**Proof:** (for uniform indep. \( r_1, \ldots, r_n \))

\[
\Pr \left[ \exists i, j \text{ st. } r_i = r_j \right] = 1 - \Pr \left[ \forall i \neq j, r_i \neq r_j \right] \\
= 1 - \frac{B^n}{B(B-1)(B-2)B - 3B \ldots} \\
\geq 1 - e^{-n^2/2B} \\
\Rightarrow n = 1.2 \sqrt{B} \Rightarrow n^2 = 1.44B \Rightarrow e^{-n^2/2B} = e^{-0.7} \approx 0.5
\]
The birthday attack

H: M → \{0,1\}^n . Collision finding algorithm:
1. Choose $2^{n/2}$ random elements in M: $m_1, ..., m_{2^{n/2}}$
2. For $i = 1, ..., 2^{n/2}$ compute $t_i = H(m_i) \in \{0,1\}^n$
3. Look for a collision ($t_i = t_j$). If not found, got back to step 1.

Expected number of iteration ≈ $2$ (by previous Thm)

Running time: $O(2^{n/2})$ (space $O(2^{n/2})$)

Example: SHA1 has output size 160 bits. Birthday attack: $2^{80}$. Best attack: $2^{51}$
Merkle-Damgarding

Given \( h: T \times X \rightarrow T \) (compression function)

we obtain \( H: X^{<L} \rightarrow T \)

\( H_i \) - chaining variables

PB: padding block

-- If no space for PB add another block
Merkle-Damgard

**Theorem:** If $h$ is collision resistant, then so is $H$.

**Proof:** collision on $H$ $\Rightarrow$ collision on $h$

Suppose $H(M) = H(M')$. We build collision for $h$.

$h(\,H_t, M_t \parallel PB) = H_{t+1} = H'_{r+1} = h(\,H'_r, M'_r \parallel PB')$
Merkle-Damgård

**Theorem:** If h is collision resistant, then so is H.

**Proof:** If collision on H \( \Rightarrow \) collision on h

Suppose \( H(M) = H(M') \). We build collision for h.

\[
\begin{align*}
IV &= H_0, H_1, \ldots, H_t, H_{t+1} = H(M) \\
IV &= H_0', H_1', \ldots, H_r', H_{r+1}' = H(M')
\end{align*}
\]

Otherwise suppose \( H_t = H_r' \) and \( M_t = M_r' \) and \( PB = PB' \)

Then: \( h(H_{t-1}, M_{t-1}) = H_t = H'_t = h(H'_t, M'_t) \)
Merkle-Damgard

Thm: $h$ collision resistant $\Rightarrow$ $H$ collision resistant

Goal: construct compression function $h: T \times X \rightarrow T$
Standardized Method: HMAC

Most widely used MAC on the Internet.

\[ H: \text{ hash function.} \]
\[ \text{example: SHA-256 ; output is 256 bits} \]

Can we build a MAC directly out of a hash function?

\[ \text{HMAC: } S(k, m) = H(k \oplus \text{opad} \ || \ H(k \oplus \text{ipad} \ || \ m)) \]
The HMAC Construction

\[ \text{tag} = h(k \oplus \text{ipad}) \circ \text{h} (m[0] | m[1] | m[2] \| \text{PB}) \circ h(k \oplus \text{opad}) \]

IV (fixed)

CBC-MAC.
HMAC: Features

Built from a black-box implementation of SHA-256.

HMAC is assumed to be a secure PRF
• Can be proven under certain PRF assumptions about \( h(\cdot,\cdot) \)
• Can even be truncated, to say the first 80 bits of output

This is used in TLS
Summary

• Message Authentication Codes (MACs)

• Hash Functions

• HMAC