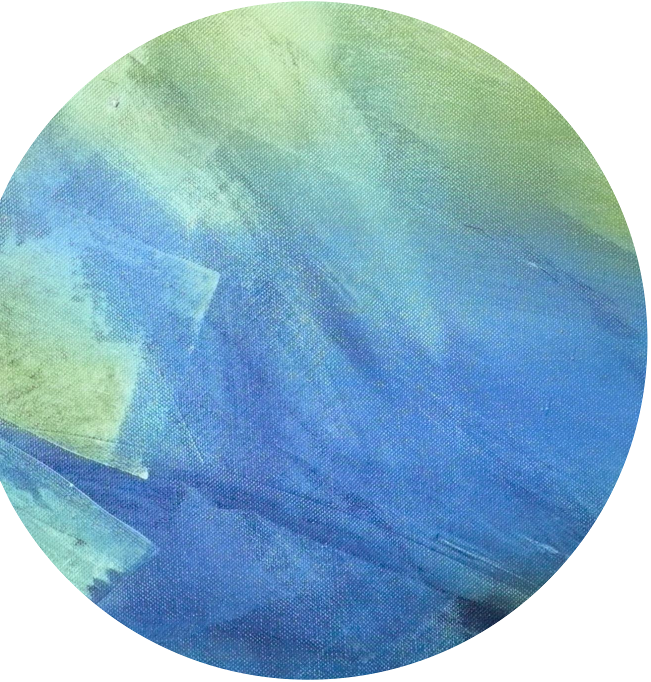
Lecture 8



Outline

(Maria)

Hash - MAC

HMAC

Collision Resistance

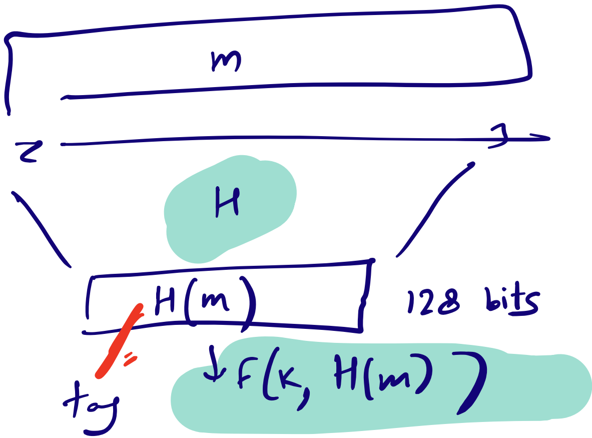
(Encrypted CBC-MAC)

HMAC

- Hash MAC : same security as a MAC
  - → Not PRF
- Apply a *hash* function H to your original message
- What properties should H satisfy?

$\exists\, (m_1, m_2 \ldots m_n)$ s.t.

$H(m_1) = H(m_2) \ldots = H(m_n)$



In a secure MAC, given $(m_1, tag_1), (m_2, tag_2) \ldots (m_n, tag_n)$ hard to find $(\tilde{m}, \tilde{tag})$ that passes verification.

Collision-resistance

Let H: M →T be a hash function (|M| >> |T|)

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

$$H(m_0) = H(m_1) \quad \text{and} \quad m_0 \neq m_1$$

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

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

Example: SHA-256 (outputs 256 bits)

If given H, easy to find m_1, m_2 s.t. $H(m_1) = H(m_2)$

then $F(K, H(m_1)) = F(K, H(m_2))$

$\Rightarrow tag(m_1) = tag(m_2)$

$H(m)$

$H(k \| m)$

$((k_1 \| m_1), (k_2 \| m_2))$ s.t. $H(k_1 \| m_1) = H(k_2 \| m_2)$

MAC from Collision-resistant Hash Functions

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

Let H: $M^{big} \to M$

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

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

<u>Thm</u>: If I is a secure MAC and H is collision resistant

then I^{big} is a secure MAC.

Example: $S(k,m) = AES_{2\text{-block-cbc}}(k, \text{SHA-256}(m))$ is a secure MAC.

MAC from Collision-resistant Hash Functions

$S^{big}(k, m) = S(k, H(m))$; $V^{big}(k, m, t) = V(k, H(m), t)$

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^{big} is insecure under a 1-chosen msg attack

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

step 2: output (m_1, t) as forgery

Protecting File Integrity

$H(\underline{m}) \to y$

Software packages:

package name	package name		package name
F_1	F_2	•••	F_n

read-only public space

256-bit string

$H(F_1)$ $H(F_2)$ $H(F_n)$

$|m| = 2$ bits $\quad 2^2 = 4$

$|\ | = 1$ bit $\quad 2$

The birthday attack

2n-bits long $|M| = 2^{2n}$

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

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

B = output space = 2^n

After hashing $(1.2\sqrt{B} \sim 2^{n/2})$ values,

Pr that you saw a collision is $\simeq 0.5$

The birthday attack

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

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

Algorithm:

1. Choose $\mathbf{2^{n/2}}$ random messages in M: $m_1, \ldots, m_{2^{n/2}}$ (distinct w.h.p)
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.

How well will this work?

The birthday attack

$[1 \ldots \underset{B}{365}]$

$n = 32$ bdays that we collected

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

Thm: when $\mathbf{n} = 1.2 \times \mathbf{B}^{1/2}$ then $\Pr[\, \exists i \neq j: \; r_i = r_j \,] \geq 1/2$

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

$$\Pr[\exists\, i,j \text{ s.t. } r_i = r_j] = 1 - \Pr[\forall\, i \neq j,\ r_i \neq r_j]$$

$$= 1 - \frac{(B-1)}{B} \cdot \frac{(B-2)}{B} \cdot \frac{(B-3)}{B} \cdots \frac{B-(n-1)}{B}$$

$$\geq 1 - e^{-n^2/2B}$$

$$n = 1.2\sqrt{B} \Rightarrow n^2 = 1.44 B \Rightarrow e^{-n^2/2B} = e^{-0.7} \approx 0.5$$

The birthday attack

$H: M \to \{0,1\}^n$.   Collision finding algorithm:

1. Choose $\mathbf{2^{n/2}}$ random elements in M: $m_1, \ldots, m_{2^{n/2}}$
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.

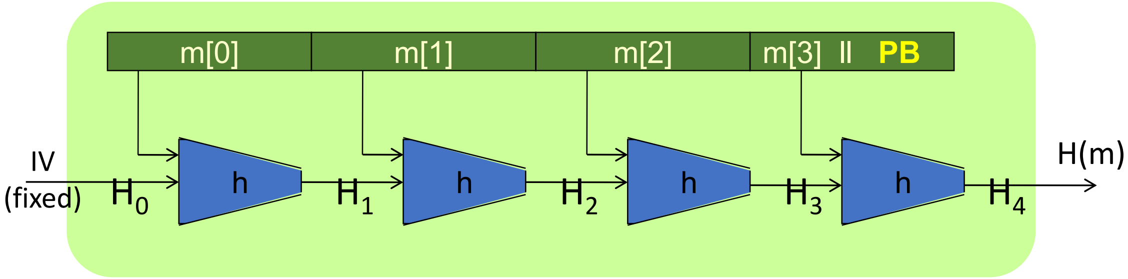
Expected number of iteration ≈ 2 (by previous Thm)

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

SHA-256   256 2^{120}

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

Merkle-Damgard



Given **$h: T \times X \longrightarrow T$** (compression function)

we obtain **$H: X^{\leq L} \longrightarrow T$**

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.

$IV = H_0, H_1, \ldots, H_t, H_{t+1} = H(M)$

$IV = H_0', H_1', \ldots, H'_r, H'_{r+1} = H(M')$

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

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.

$IV = H_0, H_1, \ldots, H_t, H_{t+1} = H(M)$

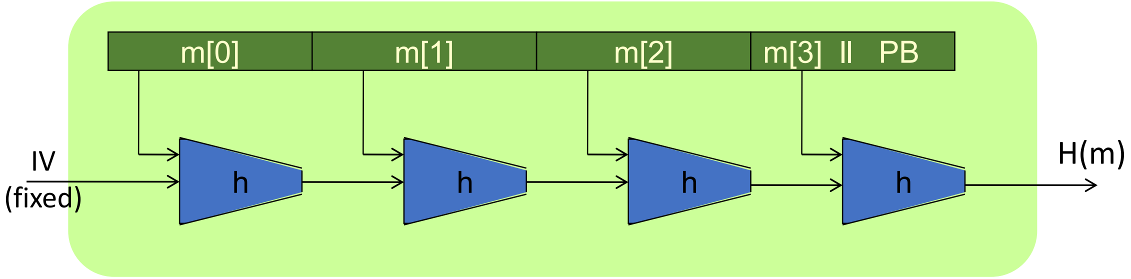
$IV = H_0', H_1', \ldots, H'_r, H'_{r+1} = H(M')$

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

Otherwise suppose $H_t = H'_r$ and $M_t = M'_r$ and $PB = PB'$

Then: $h(H_{t-1}, M_{t-1}) = H_t = H'_t = h(H'_{t-1}, M'_{t-1})$

Merkle-Damgard



Thm: h collision resistant ⇒ H collision resistant

Goal: construct compression function **h: T × X ⟶ T**

Standardized Method: HMAC

Most widely used MAC on the Internet.

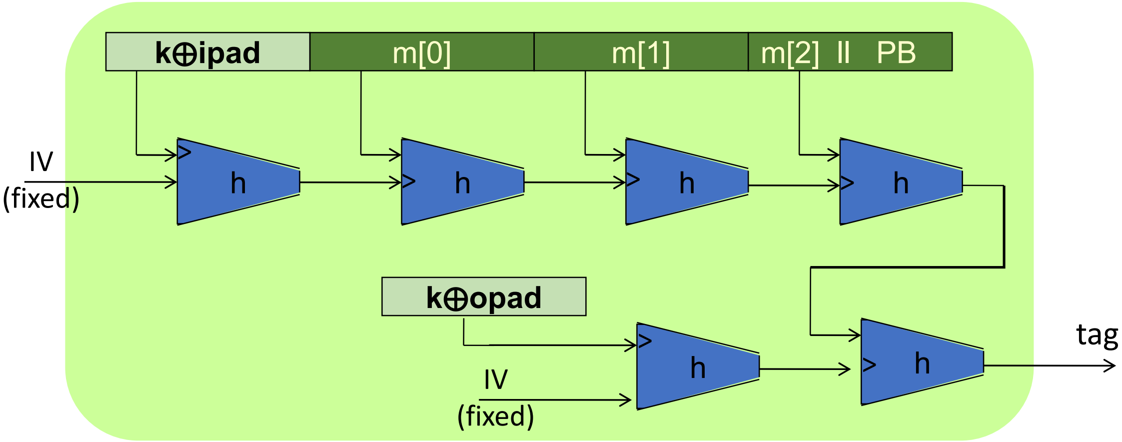
H:	hash function.
	example: SHA-256 ; output is 256 bits

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

HMAC: $S(k, m) = H\big(\, k \oplus opad \,\|\, \mathbf{H(\, k \oplus ipad \,\|\, m\,)} \,\big)$

CBC-MAC.

The HMAC Construction



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(.,.)
- Can even be truncated, to say the first 80 bits of output

This is used in TLS

H y easy to find smallest m s.t. $H(m)=y$

Summary

- Message Authentication Codes (MACs)
- Hash Functions
- HMAC