



Message integrity

Message Auth. Codes

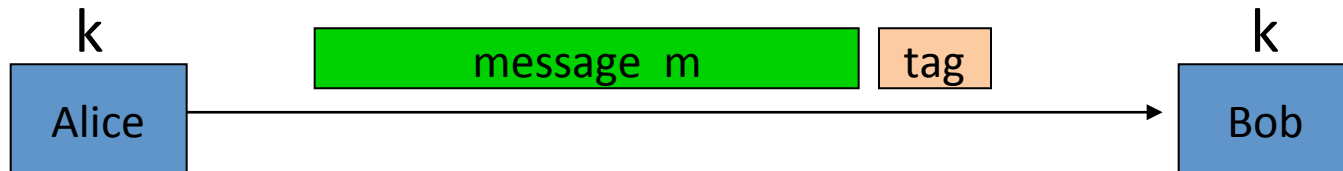
Message Integrity

Goal: **integrity**, no confidentiality.

Examples:

- Protecting public binaries on disk.
- Protecting banner ads on web pages.

Message integrity: MACs



Generate tag:

$$\text{tag} \leftarrow S(k, m)$$

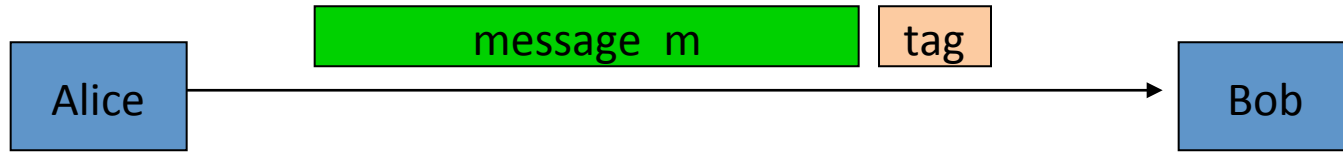
Verify tag:

$$V(k, m, \text{tag}) \stackrel{?}{=} \text{'yes'}$$

Def: **MAC** $I = (S, V)$ defined over (K, M, T) is a pair of algs:

- $S(k, m)$ outputs t in T
- $V(k, m, t)$ outputs 'yes' or 'no'

Integrity requires a secret key



Generate tag:

$\text{tag} \leftarrow \text{CRC}(m)$

Verify tag:

$V(m, \text{tag}) \stackrel{?}{=} \text{'yes'}$

- Attacker can easily modify message m and re-compute CRC.
- CRC designed to detect random, not malicious errors.

Secure MACs

Attacker's power: **chosen message attack**

- for m_1, m_2, \dots, m_q attacker is given $t_i \leftarrow S(k, m_i)$

Attacker's goal: **existential forgery**

- produce some **new** valid message/tag pair (m, t) .

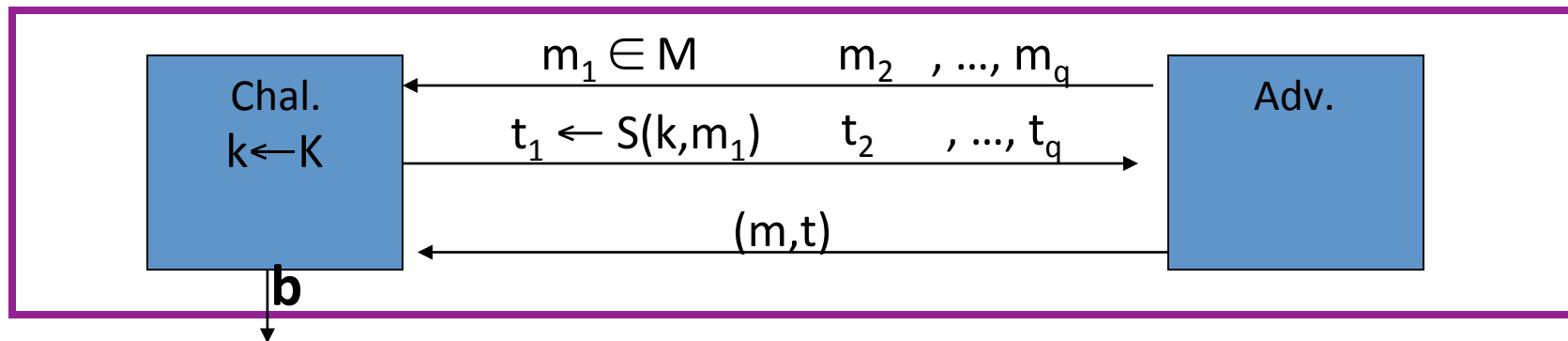
$$(m, t) \notin \{ (m_1, t_1), \dots, (m_q, t_q) \}$$

\Rightarrow attacker cannot produce a valid tag for a new message

\Rightarrow given (m, t) attacker cannot even produce (m, t') for $t' \neq t$

Secure MACs

- For a MAC $I=(S,V)$ and adv. A define a MAC game as:



$$\begin{cases} b=1 & \text{if } V(k, m, t) = \text{'yes'} \text{ and } (m, t) \notin \{ (m_1, t_1), \dots, (m_q, t_q) \} \\ b=0 & \text{otherwise} \end{cases}$$

Def: $I=(S,V)$ is a secure MAC if for all “efficient” A :


$$\text{Adv}_{\text{MAC}}[A, I] = \Pr[\text{Chal. outputs } 1] \text{ is “negligible.”}$$

Let $I = (S, V)$ be a MAC.

Suppose an attacker is able to find $m_0 \neq m_1$ such that

$$S(k, m_0) = S(k, m_1) \quad \text{for } \frac{1}{2} \text{ of the keys } k \text{ in } K$$

Can this MAC be secure?

- ☐ Yes, the attacker cannot generate a valid tag for m_0 or m_1
-  ☒ No, this MAC can be broken using a chosen msg attack
- ☐ It depends on the details of the MAC
- ☐

$$\text{Adv}[A, I] = \frac{1}{2}$$

Let $I = (S, V)$ be a MAC.

Suppose $S(k, m)$ is always 5 bits long

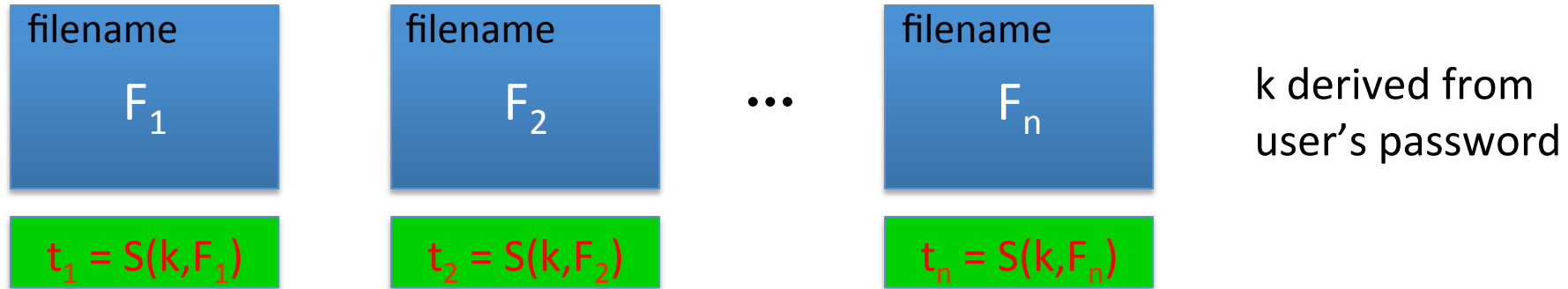
Can this MAC be secure?

- ⇒
- ☐ No, an attacker can simply guess the tag for messages
 - ☐ It depends on the details of the MAC
 - ☐ Yes, the attacker cannot generate a valid tag for any message
 - ☐

$$Adv[A, I] = 1/32$$

Example: protecting system files

Suppose at install time the system computes:



Later a virus infects system and modifies system files

User reboots into clean OS and supplies his password

– Then: secure MAC \Rightarrow all modified files will be detected

End of Segment