ECE 471/571. Digital Signatures

Alice $\xrightarrow{m,\ \sigma = sign_{K_{priv_A}}(m)}$ Bob

K_{priv_A} non-repudiation K_{pub_A}

Verify (σ, m, K_{pub_A})

$\stackrel{?}{=}$ true / false.

RSA signature

$\langle \underline{d}, \underline{n} \rangle$ private key p, q.

$\langle e, n \rangle$ pub key. $n = p \cdot q$

sign.

$\sigma = m^d \bmod n$

e co-prime to $\phi(n)$

$d = e^{-1} \bmod \phi(n)$

ver

$\sigma^e \bmod n \stackrel{?}{=} m \bmod n$

✓ Existential forgery w/ key only attack

① $m = 1$. $\sigma = 1$. ✓ $1^d = 1 \bmod n$

$1^e = 1 \bmod n$

② randomly pick # y

$$m = y^e \bmod n$$

$$m^d \equiv (y^e)^d \bmod n$$

$$\equiv y^{1 \bmod \phi(n)} \bmod n$$

$$\equiv y \bmod n$$

$$\langle m, y \rangle = \langle \underbrace{y^e}_{\text{publickey only}}, y \rangle \overset{=\sigma}{}$$

existential forgery

solution:

hash-then-sign

$$\langle m, \sigma = (H(m))^d \bmod n \rangle$$

$$\sigma^e = H(m)$$

↳ pre-image resistence

✓

Existential forgery w/ known message attack

$\langle m_1, \sigma_1 \rangle$ $\quad \sigma_1 = m_1^d \bmod n$

$\langle m_2, \sigma_2 \rangle$ $\quad \sigma_2 = m_2^d \bmod n$

$? \langle m', \sigma \rangle \quad \sigma = \sigma_1 \cdot \sigma_2 = (m_1 \cdot m_2)^d$

$\sigma = \sigma_1 \sigma_2$ ... mod n

$\langle m' = m_1 \cdot m_2, \ \sigma = \sigma_1 \cdot \sigma_2 \rangle$

✓ selective forgery w/ chosen message attack

choose m_1, ..., m_q ? ↓ σ_1

choose m, gets σ for m

choose $m/m_q = m_2$, gets σ_2 for m_2

$m = m_1 \cdot m_2$.

$\sigma_1 = \sigma / \sigma_2 \mod n$

Hash-then sign

- Exist. forgery w/ known msg. attack.

✗ ? exist (m, σ) given (m', σ') known

adv: find $m \neq m'$

s.t. $h(m) = h(m')$

$h(m)^d \bmod n = h(m') \bmod n$

second-preimage resistance

- Exist. forgery w/ chosen msg attack ?

X

choose $\langle m, \sigma \rangle$

find any m'. forge $\langle m', \sigma' \rangle$

find collision, s.t. $m \neq m'$

$$h(m') = h(m)$$

$\downarrow$

obtain σ'

$$h(m)^d \bmod n = h(m')^d \bmod n$$