Digital Signatures

One-Way Functions.

Def: an OWF is a func $F: X \to Y$ s.t.

1. $\exists$ "eff." alg to eval. F
2. $\forall$ "eff." alg A:

$$\Pr[F[\underbrace{A(F(x))}_{\text{inversion/preimage}}] = F[x]] \text{ is negligible}$$

where $x \xleftarrow{R} X$

given $y = f(x)$, hard to find preimage x of y

Ex.

1. General OWF: let (E, D) be block cipher

$$F^E(k) = [E(k,0), E(k,1), \ldots E(k,10)]$$

No special props, bad for key exch.

2. G fcg of order q w/gen $g \in G$

w/ gen $g \in G$

$$F^{Dlog}(x) = g^x \in G$$

$$F^{Dlog}: \mathbb{Z}_q \to G$$

inversion: Dlog in G base g

props: $F(x)F(y) = F(x+y)$

$F(x)^a = F(ax) \qquad a \in \mathbb{Z}$

$\Rightarrow$ DH key exch and ElGamal

3. RSA $\quad n = pq, \quad e \in \mathbb{Z}^*_{\varphi(n)}$

$F^{RSA}(x) = x^e$ in $\mathbb{Z}_n$

inversion: RSA assumption

$F^{RSA}: \mathbb{Z}_n \to \mathbb{Z}_n$

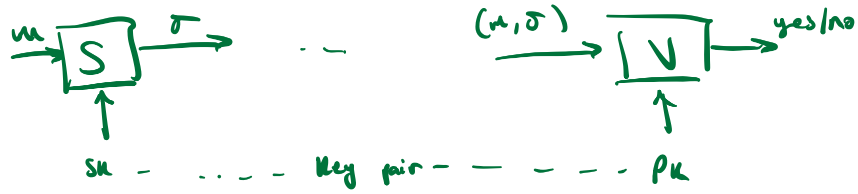
props: 1. $F^{RSA}(x) \cdot F^{RSA}(y) = F^{RSA}(xy)$

2. Trapdoor $d = e^{-1} \bmod \varphi(n)$

$\to$ RSA enc, signatures

Digital signatures

My dig. sig. on m is a fn on m



Def: A sig. scheme is a tuple of algs (Gen, S, V)

- Gen( ) → pk, sk
- S(sk, m) → σ
- V(pk, m, σ) → yes/no (deterministic)

s.t. if (pk, sk) ← Gen( ) then

$\forall m \in \mathcal{M}$: V(pk, m, S(sk, m)) = "yes"

note: signer signs m once → σ ← one person

anyone w/ pk, m can verify σ ← many people

Security

Attacker power: chosen msg attack

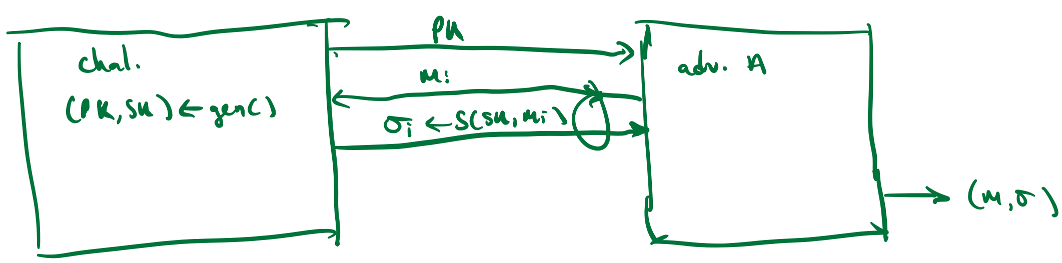
→ for $m_1, \dots m_\ell \in \mathcal{M}$: attacker given $\sigma_i \leftarrow S(sk, m_i)$

Attacker goal: existential forgery

→ produce some new valid pair (m, σ)

s.t. $m \notin \{m_1, \dots m_\ell\}$

For sig scheme (Gen, S, V) and adv A:



Adv. wins if V(pk, m, σ) = "yes" and $m \notin \{m_1, \dots m_\ell\}$

Def. Sig scheme (Gen, S, V) secure if $\forall$ eff. adv A:

Pr[A wins game] ≤ negligible