definizione formale

Uno schema di firma è una 5-pla $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ dove

1. $\mathcal{P}$ è un insieme finito di possibili messaggi
2. $\mathcal{A}$ è un insieme finito di possibili firme
3. $\mathcal{K}$, lo spazio delle chiavi, è un insieme finito di possibili chiavi
4. $\forall k \in \mathcal{K}$ c'è un algoritmo di firma $\mathrm{sig}_k \in \mathcal{S}$ e un corrispondente algoritmo di verifica $\mathrm{ver}_k \in \mathcal{V}$.
5. $\mathrm{sig}_k : \mathcal{P} \to \mathcal{A}$ e $\mathrm{ver}_k : \mathcal{P} \times \mathcal{A} \to \{V, F\}$ sono funzioni tali che $\forall x \in \mathcal{P}$ e $\forall y \in \mathcal{A}$ vale

$$\mathrm{ver}_k(x, y) = \begin{cases} V & \text{se } y = \mathrm{sig}_k(x), \\ F & \text{se } y \neq \mathrm{sig}_k(x) \end{cases}$$

schema di firma RSA

- Sia $N = pq$, p, q primi. Sia $\mathcal{P} = \mathcal{A} = \mathbb{Z}_N$.
- Lo spazio delle chiavi è

$$\mathcal{K} = \{(N, p, q, d, e) \mid ed \equiv 1 \pmod{\phi(N)}\}.$$

- N e e sono la chiave pubblica, p, q, d sono la chiave privata
- Se $k = (N, p, q, d, e)$ è una chiave, poniamo
- $\mathrm{sig}_k(x) \equiv x^d \pmod{N}$
- $\mathrm{ver}_k(x, y) = V \iff x \equiv y^e \pmod{N}$

falsificazione

- dato $x \in \mathcal{P}$, dev'essere computazionalmente difficile per chi non è Alice calcolare una firma y tale che $\text{ver}_{k_A}(x, y) = V$
- una coppia (x,y) tale che $\text{ver}_{k_A}(x, y) = V$ che non è stata prodotta da Alice (ma da Eve, per esempio) si dice una falsificazione
- usando lo schema RSA (e anche usando un altro PKCS deterministico)
- è difficile, dato il messaggio x produrre una falsificazione (x, y)
- è però facile data y produrre una falsificazione (x, y)

- Eve può falsificare la firma di Alice
- sceglie y e pone $x = e_{k_A}(y)$
- la coppia (x, y) passa la verifica "per costruzione"
- $\text{ver}_k(x, y) = V \quad \Longleftrightarrow \quad x = e_{k_A}(y)$
- una falsificazione di questo tipo si chiama falsificazione esistenziale (existential forgery)
- Eve non può scegliere il messaggio x e produrre una firma valida y (una falsificazione di questo tipo si chiama falsificazione scelta (selective forgery))

- Eve vuole ottenere la firma di Alice su un messaggio x da lei scelto
- Alice non firmerebbe mai x
- Eve trova x_1, x_2 tali che $x \equiv x_1 \cdot x_2 \pmod{N}$
- chiede a Alice di firmare x_1 e x_2, e ottiene y_1, y_2
- per le proprietà moltiplicative dell'RSA si ha che

$$\text{ver}_k(x_1 x_2 \bmod N, y_1 y_2 \bmod N) = V$$

funzione hash

- per evitare falsificazioni, si usano schemi di firma insieme a funzioni hash
- molto informalmente, una funzione hash $h : \mathcal{P} \to \mathcal{D}$ è una funzione unidirezionale
- h(x) si dice digest del messaggio x
- può/deve avere molte altre proprietà che non discutiamo

schemi di firma e funzioni hash

- Alice deve firmare il messaggio x
- calcola $h(x)$
- firma il message digest $h(x)$, non x: $y = \mathrm{sig}_{k_A}(h(x))$
- Bob riceve (x, y) – per prima cosa, calcola $h(x)$
- poi controlla che $\mathrm{ver}_{k_A}(h(x), y) = V$
- "intuitivamente" questo impedisce le falsificazioni
- Eve sceglie y, calcola $e_{k_A}(y)$ - per produrre una coppia valida, deve trovare $h^{-1}(e_{k_A}(y))$
- lo schema RSA viene sempre usato insieme a una funzione hash

falsificazioni e funzioni hash

- le proprietà delle funzioni hash impediscono le falsificazioni esistenziali
- Eve sceglie y, calcola $e_{k_A}(y)$ - per produrre una coppia valida, deve trovare x tale che $h(x) = e_{k_A}(y)$, quindi $x = h^{-1}(e_{k_A}(y))$
- difficile perché h è preimage resistant
- in un altro attacco Eve ha un messaggio firmato (x, y), $y = \mathrm{sig}_{k_A}(h(x))$
- calcola $z = h(x)$, cerca un $\bar{x} \neq x$ con $h(\bar{x}) = h(x)$
- se ci riesce, ha la falsificazione (esistenziale) $(\bar{x}, y)$
- una proprietà della funzioni hash è che deve essere difficile, dato x, trovare $\bar{x} \neq x$ con $h(\bar{x}) = h(x)$
- h deve essere second preimage resistant
- altro possibile attacco: se Eve ha x e $\bar{x}$ tali che $h(\bar{x}) = h(x)$,
- convince Alice a firmare x ottenendo y, e ha la falsificazione $(\bar{x}, y)$
- h deve essere collision resistant