## da chi proviene un messaggio?

- in un crittosistema simmetrico solo Alice e Bob conoscono la chiave
- se Bob riceve un messaggio di Alice e la decifratura del messaggio ha senso, il messaggio proviene certamente da Alice
- in un crittosistema a chiave pubblica, chiunque può scrivere un messaggio cifrato a Bob affermando di essere Alice
- serve una firma digitale

## firma "manuale"

- associa un documento a un utente firmatario
- la firma fa fisicamente parte del documento
- la firma viene verificata confrontandola con una firma campione depositata
- dovrebbe essere difficile da falsificare
- è vincolante dal punto di vista legale (contratti etc.)

## firma digitale - differenze

- deve sempre associare un utente a un documento - tramite una stringa digitale
- c'è bisogno di un metodo che leghi la firma al documento
- ci vuole un algoritmo pubblico di verifica – previene la falsificazione
- una copia di un documento digitale è uguale all'originale – bisogna evitare che una firma sia riutilizzabile

## signature scheme

- Alice firma un messaggio da mandare a Bob
- ci sono due componenti: un algoritmo sig per firmare e un algoritmo ver per verificare
- quello per firmare dev'essere privato (solo Alice può firmare)
- quello per verificare dev'essere pubblico (Bob - e chiunque altro - può verificare che viene da Alice)
- per firmare il messaggio $x$ Alice usa l'alg $\text{sig}_k$ che dipende da una chiave $k$, e calcola $\text{sig}_k(x) = y$ (lo stesso messaggio può avere diverse firme)
- data una coppia $(x, y)$ dove $x$ è il messaggio e $y$ la firma, l'algoritmo $\text{ver}_k(x, y)$ dà in output vero se $y$ è una firma valida di $x$, falso altrimenti
- in questo momento, non si chiede che $(x, y)$ sia cifrato

## 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 $\text{sig}_k \in \mathcal{S}$ e un corrispondente algoritmo di verifica $\text{ver}_k \in \mathcal{V}$.
5. $\text{sig}_k : \mathcal{P} \to \mathcal{A}$ e $\text{ver}_k : \mathcal{P} \times \mathcal{A} \to \{V, F\}$ sono funzioni tali che $\forall x \in \mathcal{P}$ e $\forall y \in \mathcal{A}$ vale

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

## procedura di firma usando un PKCS

- l'algoritmo per firmare $\text{sig}_k$ dev'essere privato (solo Alice può firmare)
- l'algoritmo per verificare $\text{ver}_k$ dev'essere pubblico (Bob - e chiunque altro - può verificare che viene da Alice)
- idea: usare un CS a chiave pubblica (deterministico)
- Alice ha la chiave $k_A$, $e_{k_A}$ è pubblica e $d_{k_A}$ è privata
- Alice firma il messaggio $x$ ponendo $\text{sig}_{k_A}(x) = y = d_{k_A}(x)$ (è l'unica che può decifrare)
- invia la coppia $(x, y)$
- Bob (e chiunque altro) calcola $e_{k_A}(y)$
- se $x = e_{k_A}(y)$, allora $\text{ver}_{k_A}(x, y) = V$

## 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
- $\text{sig}_k(x) \equiv x^d \pmod{N}$
- $\text{ver}_k(x, y) = V \iff x \equiv y^e \pmod{N}$

## esempio

- la chiave RSA di Alice è $k_A = (N_A, p_A, q_A, d_A, e_A) = (2773, 47, 59, 17, 157)$, $\phi(N_A) = 2668$
- Alice vuole firmare e trasmettere il messaggio $x = 920$
- usa la chiave privata $d_A = 17$ e calcola $\text{sig}_{k_A}(920) = 920^{17} \equiv 948 \pmod{2773}$
- la coppia (messaggio, firma) è quindi $(920, 948)$
- Bob riceve $(x, y) = (920, 948)$
- verifica la firma usando la chiave pubblica di Alice $e_A = 157$ $948^{157} \equiv 920 \pmod{2773} \Rightarrow \text{ver}_{k_A}(920, 948) = V$