Firma digitale: messaggio cifrato e firmato

U genera la firma:

$$f = D(m, k_U[\text{priv}]),$$

poi la cifra con la chiave pubblica del destinatario V:

$$c = C(f, k_V[\text{pub}]),$$

e spedisce la coppia (U, c) a V.

Per verificare, V decifra c per ottenere f, da cui ricava m attraverso un'operazione di cifratura:

$$\begin{aligned} f &= D(c, k_V[\text{priv}]) \\ m &= C(f, k_U[\text{pub}]) \end{aligned}$$

Se m è significativo V conclude che è autentico.

È necessario che $n_U \leq n_V$ affinché $f < n_V$ e f possa essere cifrata correttamente; ciò impedisce a V di inviare a U messaggi firmati e cifrati. Per questo motivo ogni utente ha una coppia di chiavi per la firma e una per la cifratura, e tutte le chiavi di firma hanno $n < H$, quelle di cifratura $n > H$ (e.g. $H = 2^{1024}$).
TODO non verificabile da terzi?

Attacco

Supponiamo che il sistema di U risponda automaticamente ad ogni messaggio m (cifrato e firmato come sopra) che riceve inviando un ack composto dal crittogramma della firma di U su m. Il crittoanalista X può decifrare m con un attacco attivo:

- X intercetta il crittogramma c firmato inviato da V a U e lo rispedisce a U facendogli credere che sia stato inviato da X;
- U risponde automaticamente con un ack c' a X:

  $$\begin{aligned} f &= D(c, k_U[\text{priv}]) \\ m' &= C(f, k_X[\text{pub}]) \\ f' &= D(m', k_U[\text{priv}]) \\ c' &= C(f', k_X[\text{pub}]) \end{aligned}$$

  $m' \neq m$ è privo di senso perché è stato calcolato con la chiave pubblica di X anziché quella di V, quindi verrà scartato, ma solo dopo aver inviato l'ack;
- X usa l'ack, la propria chiave privata e le chiavi pubbliche di U e V per risalire a m in tempo polinomiale:

  $$\begin{aligned} f' &= D(c', k_X[\text{priv}]) \\ m' &= C(f', k_U[\text{pub}]) \\ f &= D(m', k_X[\text{priv}]) \\ m &= C(f, k_V[\text{pub}]) \end{aligned}$$

Soluzione:

- mandare l'ack solo se il messaggio decifrato ha senso;
- protocolli di firma basati su hash (non si firma mai direttamente il messaggio).