Firma digitale: messaggio cifrato e firmato in hash

Il mittente U calcola $h(m)$ e genera la firma:

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

poi cifra separatamente il messaggio per V:

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

infine spedisce a V la tripla (U, c, f).

Osservazioni:

- il messaggio è appesantito con la firma, che però è corta;
- si può cifrare m con un cifrario simmetrico;
- $h(m)$ è veloce da calcolare ed è difficile trovare un messaggio diverso da m con stesso hash per la proprietà claw-free;
- non c'è bisogno di due coppie di chiavi distinte per firma e cifratura.

Decifrazione e verifica

V decifra c:

$$m = D(c, k_V[\text{priv}])$$

calcola separatamente $h(m)$ e controlla che:

$$C(f, k_U[\text{pub}]) = h(m).$$