Firma digitale: messaggio cifrato, firmato in hash e certificato

Il mittente U si procura il certificato cert_V (verificandone la firma) del destinatario V, calcola $h(m)$ e genera la firma

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

poi cifra m:

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

e spedisce la tripla (cert_U, c, f), dove cert_U contiene $k_U[\text{pub}]$ e un'indicazione della funzione hash utilizzata.

Decifrazione e verifica

V verifica l'autenticità di cert_U, estrae $k_U[\text{pub}]$, decifra il crittogramma:

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

e controlla che:

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