# Firma digitale: messaggio in chiaro e cifrato

Protocollo proposto da Diffie e Hellman. La firma di un messaggio è quel messaggio cifrato con la chiave *privata* di un cifrario asimmetrico.

La firma dell'utente $U$ con chiave privata $k_{\text{priv}}$ sul messaggio $m$ è:

$$f = D(m, k_{\text{priv}}).$$

$U$ spedisce la tripla $(U, m, f)$, che può essere verificata controllando che:

$$C(f, k_{\text{pub}}) = m.$$

La specifica di $U$ permette al destinatario di selezionare la chiave pubblica.

Si può utilizzare un qualsiasi cifrario che consente di utilizzare $C$ e $D$ in ordine inverso, ovvero $C$ e $D$ devono essere commutative:

$$C(D(m)) = D(C(m)) = m,$$

che vale per RSA.

Caratteristiche:

- autentica e non falsificabile: $k_{\text{priv}}$ è nota solo a $U$, per falsificare la firma è necessario conoscerla, ed è difficile da ricavare se il cifrario è sicuro;
- $m$ non può essere alterato, altrimenti $f$ non è coerente con $m$;
- non ripudiabile: solo $U$ può produrre $f$;
- non riutilizzabile: dipende da $m$;
- la verifica non richiede di conoscere informazioni private, quindi può essere fatta da chiunque.

Svantaggi:

- raddoppia la lunghezza del messaggio;
- non permette di cifrare $m$: può essere sempre ricavato tramite l'operazione di verifica della firma.