Identificazione, autenticazione, firma digitale

identificazione accertare l'identità di un utente di un servizio;

autenticazione accertare l'identità del mittente di un messaggio e l'integrità del crittogramma ricevuto;

firma digitale obiettivo:

- il mittente non deve poter negare di aver inviato il messaggio m;
- il destinatario deve essere in grado di autenticare il messaggio;
- il destinatario non deve poter sostenere che $m' \neq m$ è il messaggio inviato dal mittente.

Tutto questo deve poter essere verificato da una terza parte.

L'impiego di una firma garantisce l'autenticazione, che garantisce l'identificazione. Permettono di contrastare attacchi attivi.

Esempi

identificazione password UNIX (canale sicuro), cifratura di un numero casuale con chiave privata (canale insicuro), Fiat-Shamir;

autenticazione MAC;

firma messaggio in chiaro e cifrato, firmato e cifrato, cifrato e firmato in hash, e cifrato e firmato in hash con certificato.