CAP 9 : IDENTIFIAZIONE AUTENTICAZIONE E FIRMA DIGITALE

- **Identificazione**: un sistema accerta l'identità di un utente che richiede di accedere ai suoi servizi. U utente mette la pw e il sistema associa ad U due sequenze binarie S seme del generatore e Q immagine con funzione one way. Ogni volta che l'utente si connette il sistema risale ad S e lo concatena con la pw di U se coincide con Q allora l'identificazone ha avuto successo. Essendo difficile ricavre la password da Q il metodo è sicuro dagli attacchi. Fasi:
  - Quando U vuole accedere a s S genera un numero casuale r<n e lo invia in chiaro a U
  - Udecifra r e calcola fr^d mod n con la sua chiave pubblica di U composta dalla coppa <e,n> calcola f^e mod n e controlla che r sia il risultato
  - se coincide allora l'utente che ha chiesto l'identificazione è U
- **Autenticazione**: il destinatario di un msg deve accertare l'identità del mittente e la completezza del crittogramma ricevuto.
  Il processo di autenticazione viene descritto attraverso la copia A(m,k) che genera un iformazione : MAC, quale oltre a garantire l'integrità del messaggio, è proprio allegato a esso. Il MAC è uno strumento potente perche consente il controllo di integrità e permete di indivuduare errori malizioni e infine visto che deve essere molto piu piccolo dello spazio dei msg allora A non è iniettiva quindi non è invertibile.
  Il MAC è un immagine breve del messaggio che puo essere generata solo da mittente conosciuto dal Dest. L'impiego di un qls cifrario in modalità CBC permette di creare un MAC
- **Firma digitale**:E' necessaria se mittente e destinatario non si fidano l'uno dell'altro. Ha 3 requisiti: 1) il mittente non deve negare si aver mandato un msg a Destinatario 2)il destinatario di un msg deve accertare l'identità del mittente e la completezza del crittogramma ricevuto 3) il destiatario non deve sostenere di aver ricevuto dal mittente un msg diverso da quello effettivamente mandato.
  Requisiti
  - LA firma è autentica e non falsificabile
  - La firma non è riutilizzabile
  - il documento firmato non è alterabile
  - la firma non puo essere ripudiata da chi l'ha apposta

- **funzione hash one way:** una funzione hash f:X-->Y definita per un dominio X e un codominio Y tc:
  - per ogni x appartenente a X è computazionalmente facile calcolare f(x)
  - sapendo y è computazionalmente difficile trovare una x appartenente a X tc f(x)=y
  - è computazionalmente diffcile trovare x1 e x2 tc f(x1)=f(x2)
- esempi di funzoni hash one way sono
  - MD5 usata per controllare l'integrità dei messaggi nelle linee insicure
  - SHA funzione crittograficamente sicura soddsfa tutti e tre i requisiti e genera immagini diverse per sequenze molto simili

- **PROTOCOLLO 1 : Messaggio m in chiaro e firmato**
  - firma : l'utente u genera la firma f=D(m,Ku[priv]), il messaggio è spedito a V come tripla <U,m,f>
  - verifica: l'utente V riceve la tripla <U,m,f> e verifica l'autenticità calcolando C(f, ku[pub]) e controlando che questo valore sia uguale a m.
  - NB: il protocollo 1 soddisfa i 3 requsiti
- **PROTOCOLLO 2: Messaggio m in cifrato e firmato**
  - firma e cifratura: U genera la firma del messaggio m come f=m^du mod nu esegue la cifratura della firma con la chiave pubblica del destinatario c=f^ev mod nv e spedisce la coppia <U,c>
  - decifrazione e verifica: Ricevuta la coppia <U,c> eseguo la decifrazione di C cn la chiave privata del destinatario. V calcola c^dv mod nv=f. Decifra poi f con la chiave pubblica del mittente f^eu mod nu=m. Se m è un messaggio significativo allora è autentico.
- **PROTOCOLLO 3 : messaggio n cifrato e firmato in hash**
  - firma e cifratura . Il mittente U calcola h(m) e genera f=D(h(m), k[priv]) calcola separatamente il