



---

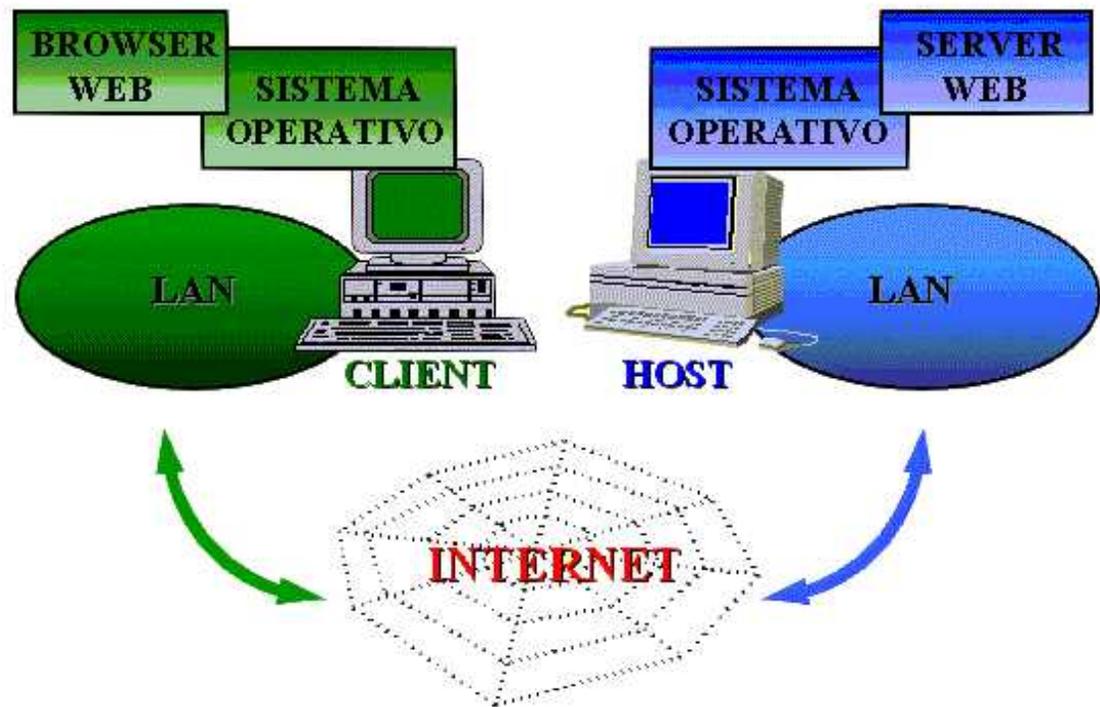
# Sicurezza nell'utilizzo di Internet

# Sicurezza – Definizioni

- Pirati informatici (hacker, cracker): persone che entrano in un sistema informatico senza l'autorizzazione per farlo
- Sicurezza: protezione applicata ad un sistema informatico per garantire il soddisfacimento degli obiettivi di preservazione dell'integrità, disponibilità e confidenzialità delle risorse del sistema

# Sicurezza – Struttura del web

- Elementi da prendere in considerazione nell'analisi della sicurezza (punti deboli)



# Sicurezza - Pericoli

- Cavallo di Troia: programma o documento che contiene software dannoso nascosto da una normale applicazione (es. virus in file o email)
- Hacking: spezzare i meccanismi di autenticazione della password (“intuizione”, furto, generazione automatica di password) per puro diletto, senza fare danni

# Sicurezza - Pericoli

- Mapping: un attacco è spesso preceduto da raccolta di informazioni (IP delle macchine, SO installato, porte e servizi attivi)
- Port scanning: scansione sequenziale delle porte che inviando richieste di servizio classifica e analizza le risposte ricevute)

# Sicurezza - Pericoli

- Sniffing: possibilità di “fiutare” le password attraverso software in grado di monitorare il flusso di pacchetti dati che attraversano la rete
- Spoofing: possibilità di modificare in maniera fraudolenta il contenuto dei pacchetti in circolazione (es. falsificando l'indirizzo IP di provenienza e assumendo indebitamente l'identità altrui)

# Sicurezza - Pericoli

- Phishing: possibilità di indurre ignari utenti a fornire in buona fede le proprie credenziali (es. indirizzandoli tramite link camuffati in email di invito su siti che riproducono siti istituzionali), utilizzate poi fraudolentemente

# Sicurezza - Pericoli

- Attacchi “denial-of-service” (DoS): es. pacchetti con IP “camuffato” possono richiedere allocazione di risorse su di un server (es. SYN flooding) o terminali ignari rispondono a richieste di echo-reply con IP mittente camuffato (che subisce l’attacco)
- Distributed denial-of-service (DDoS):
  - ◆ 1. Si acquisiscono fraudolentemente account e credenziali di utente su terminali diversi
  - ◆ 2. Si installa su tali terminali un programma “slave” per attacchi DoS
  - ◆ 3. Un programma “master” attiva tutti gli slave a lanciare l’attacco ad uno stesso host bersaglio

# Sicurezza - Pericoli

- Hijacking: “dirottamento” es. di una connessione; in un primo tempo la conversazione fra A e B viene “ascoltata”, poi il pirata si può sostituire es. a B (dopo averlo messo temporaneamente fuori uso con DoS) inviando ad A pacchetti con IP di B “camuffato” proseguendo così fraudolentemente a suo vantaggio la conversazione
- .....

# Sicurezza – Cosa fare

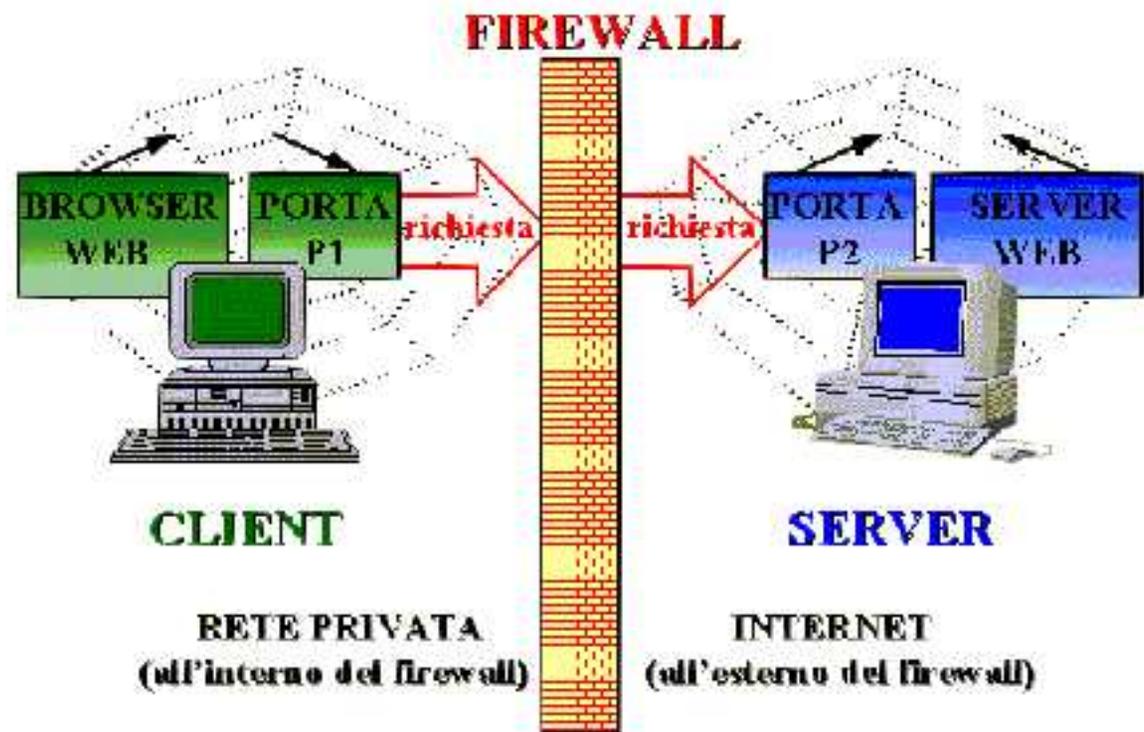
- Limitare gli accessi e usare meccanismi di autenticazione e autorizzazione
- Monitorare i registri e i log che tracciano i tentativi di accesso (tcwrapper in unix)
- Disabilitare i servizi del sistema operativo che non sono necessari
- Separare i servizi (es. Web, email)
- Tenersi informati: newsgroup e pareri del Computer Emergency Response Group (CERT)

# Sicurezza – Cosa fare

- Principio del privilegio minimo: al server Web deve essere assegnata la quantità minima di privilegi di cui ha bisogno
- Limitare l'accesso alle aree CGI, directory in cui sono memorizzati script e programmi eseguibili

# Sicurezza – i Firewall

- Funzioni o apparecchiature che servono a proteggere un dominio o una rete privata



# Sicurezza – i Firewall

- In pratica un Firewall è una combinazione di HW e SW che “isola” una rete privata (es. aziendale) dal resto di Internet operando un filtraggio selettivo dei pacchetti
- Può agire su due livelli:
  - ◆ Firewall a filtraggio di pacchetto (agisce sullo strato di rete in base all’IP)
  - ◆ Gateway a livello di applicazione (gestisce gli accessi in modo più fine, utente per utente, centralizzando le funzioni di autorizzazione e controllo e gestendole a livello di applicazione)

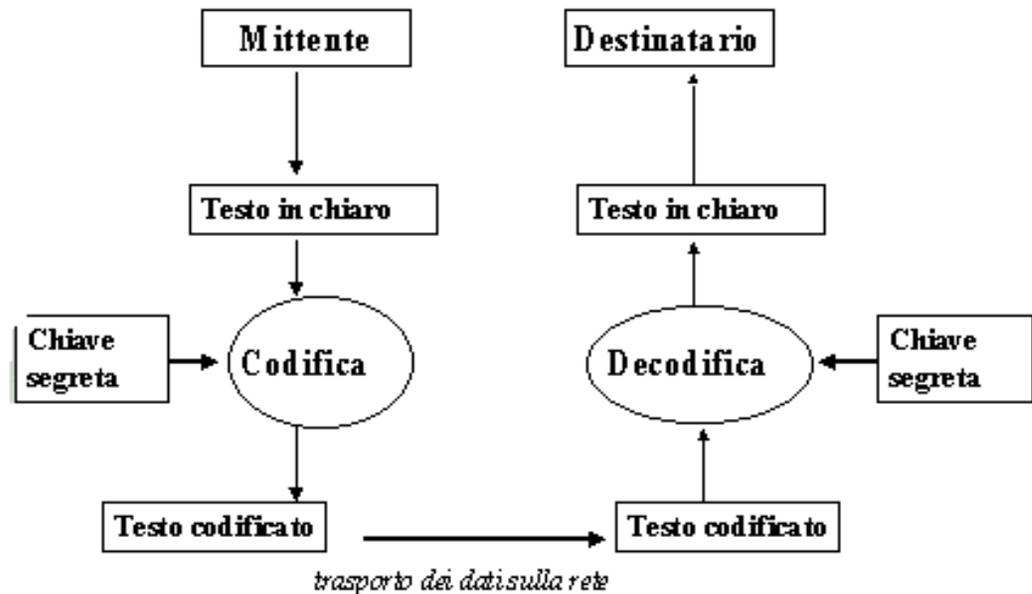
# Crittografia

- La Crittografia si occupa della cifratura e della decifratura dei messaggi
- Crittografia moderna: algoritmi a chiave simmetrica e asimmetrica

# Crittografia - Algoritmi a chiave simmetrica (DES)

- **Data Encryption Standard 1976**
- Messaggio criptato con chiave segreta (nota solo al mittente e al destinatario)

crittografia a chiave simmetrica



# Crittografia – Sistemi a chiave asimmetrica (o a chiave pubblica)

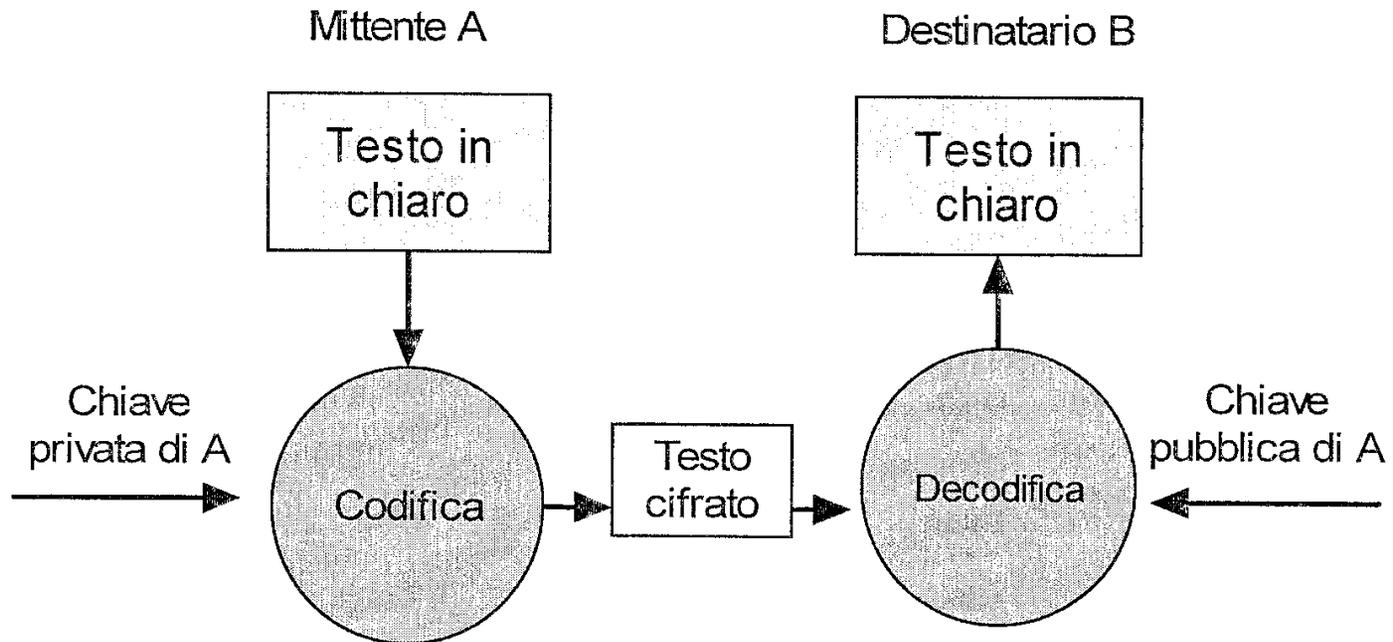
- Ad ogni persona sono assegnate due chiavi (pubblica e privata) legate tra loro ma non riconducibili l'una a l'altra
- Sono necessarie autorità di riferimento per la detenzione delle chiavi pubbliche che siano affidabili (garantiscono l'autenticità)

# Crittografia – Sistemi a chiave asimmetrica (RSA)

- Algoritmo **Rivest, Shamir, Adleman** 1977
  - ◆ scelgo  $p, q$  numeri primi grandi ( $\sim 10^{200}$ )
  - ◆  $n = pq, \quad m = (p-1)(q-1)$
  - ◆ scelgo  $e < m$ ,  $e$  primo rispetto a  $m$
  - ◆ calcolo  $d$  tale che:  $de = 1 \pmod m$   
(inverso di  $e \pmod m$ , es. alg. di Euclide)
  - ◆  $\Rightarrow$  **chiave pubblica** è:  $(e, n)$
  - ◆  $\Rightarrow$  **chiave privata** è :  $(d, n)$
- cifratura:  $C = M^e \pmod n$
- decifratura:  $M = C^d \pmod n$ 
  - ◆ decrittazione: trovare  $d$  noti  $n, e, C$   
(occorre fattorizzare  $n$  in  $pq$  !!)

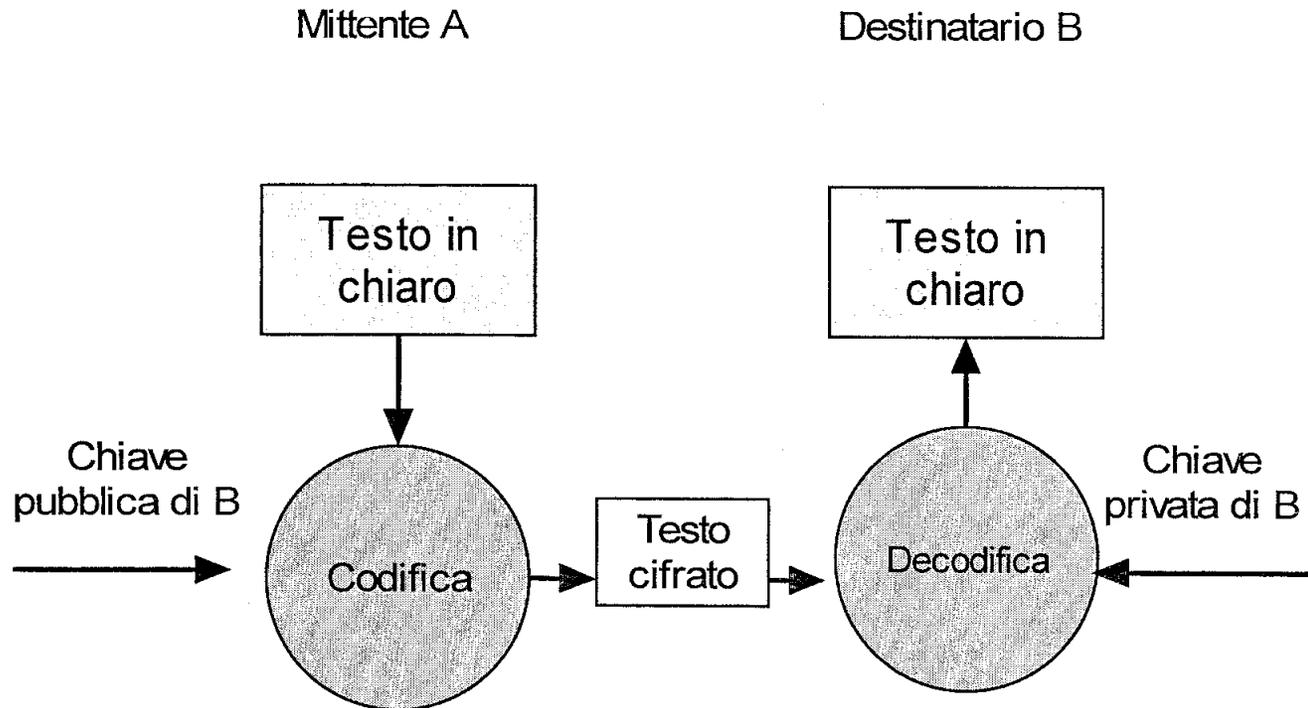
# Crittografia – Sistemi a chiave asimmetrica (RSA)

- Autenticazione del mittente



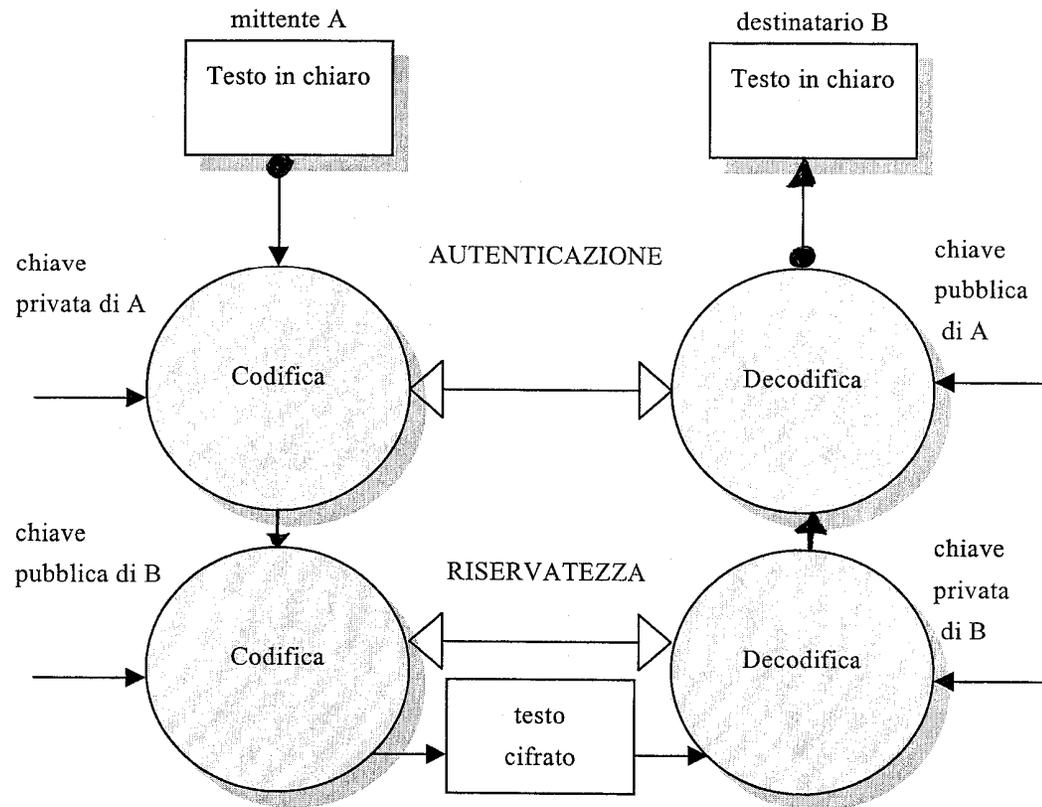
# Crittografia – Sistemi a chiave asimmetrica (RSA)

- Riservatezza e identità del destinatario



# Crittografia – Sistemi a chiave asimmetrica (RSA)

- Certezza del mittente, del destinatario e riservatezza del messaggio



# Sistemi a chiave Asimmetrica

## ■ Vantaggi

- ◆ non richiede scambio di informazione segreta in rete (la chiave)
- ◆ con  $N$  soggetti, richiede  $2N$  chiavi anziché  $N(N-1)/2$
- ◆ garantisce l'autenticità

## ■ Svantaggi

- ◆ usa chiavi molto lunghe e processo criptazione computazionalmente oneroso
- ◆ non cifra alcune strutture del messaggio che possono essere riconosciute e permettere di risalire al messaggio in chiaro

# Uso sinergico dei due sistemi (es. PGP – Pretty Good Privacy)

- Il Messaggio vero e proprio viene codificato con un cifrario simmetrico (+ veloce e sicuro)
- La crittografia a chiave pubblica viene utilizzata per lo scambio della chiave simmetrica:  
la chiave simmetrica viene codificata con la chiave pubblica del destinatario e allegata al messaggio (busta elettronica)

# SSL (protocollo https)

- Privatezza del collegamento: i dati sono crittografati con crittografia simmetrica (RSA)
- Autenticazione: identità autenticata attraverso la crittografia asimmetrica (certificato digitale)
- Affidabilità: il livello di trasporto include un check dell'integrità del messaggio (con firma digitale)

# Firma Digitale

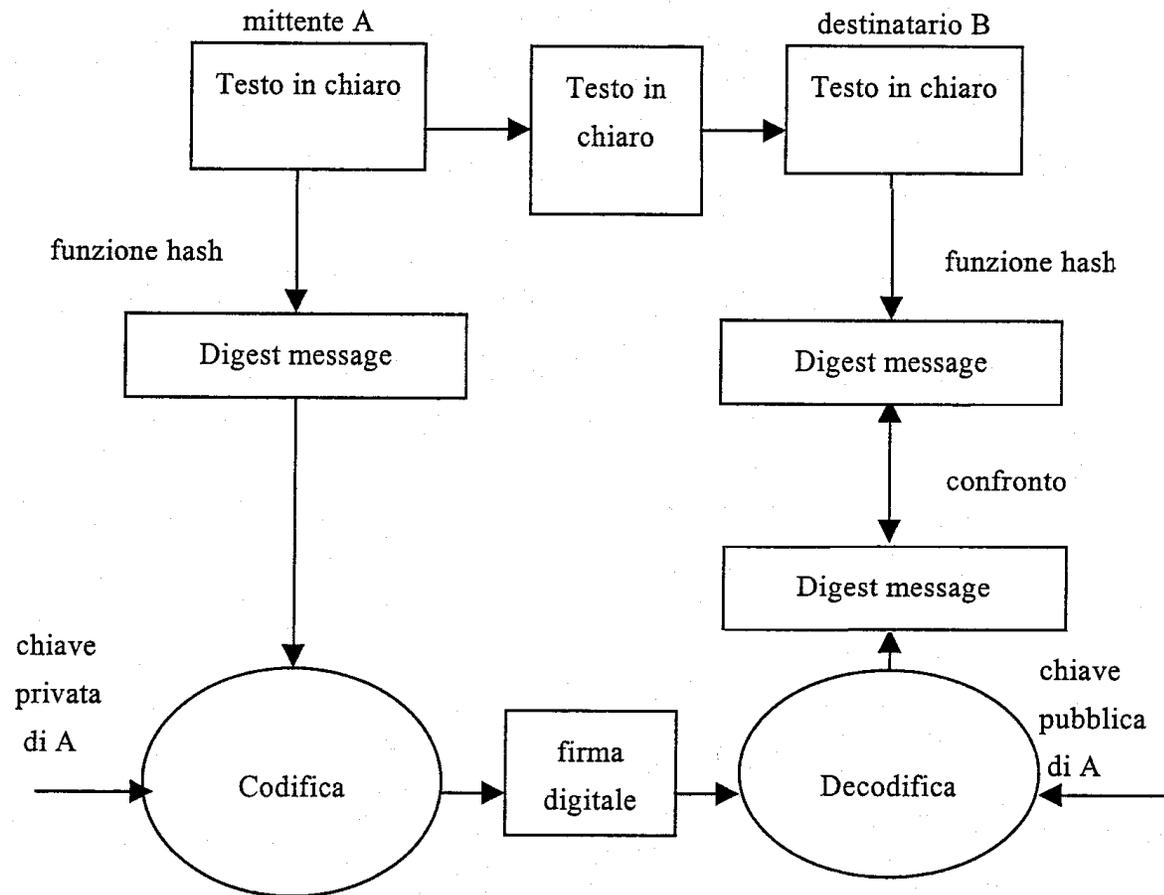
- Il Documento con firma elettronica
  - ◆ è stato realmente prodotto dal proprietario della firma
  - ◆ non può essere stato modificato dopo la firma
  - ◆ non può essere disconosciuto da chi ha firmato
- (proprietà verificabili da chiunque riceva il documento firmato)

# Firma Digitale in Italia

- La sottoscrizione con firma digitale ha valore legale (D.P.R. 512/97 n. 513 e Regolamento attuativo)
  - ◆ ha funzione indicativa  
(identifica l'autore)
  - ◆ ha funzione dichiarativa  
(denota approvazione del contenuto del documento da parte del firmatario)
  - ◆ ha funzione probatoria  
(l'autore si assume la paternità dei contenuti)

# Firma Digitale

## ■ Schema di funzionamento



# Distribuzione e Certificazione delle Chiavi

- Occorrono “intermediari di fiducia” che:
  - ◆ Nel caso di chiave simmetrica agisca come Centro di Distribuzione delle Chiavi (KDC), usando una chiave segreta condivisa
  - ◆ Nel caso di chiave asimmetrica garantiscono che una chiave pubblica appartenga ad una certa entità validandone l'identità (lavorano come Certification Authority)
    - ★ Certificato = credenziali + chiave pubblica di un'entità, firmato dalla CA con la propria chiave privata
    - ★ Se ci si fida della CA, ci si deve fidare anche dell'identità dei proprietari (e delle loro chiavi) da essa certificati

# Commercio Elettronico (e-commerce)

- Un qualunque tipo di operazione commerciale (vendita/acquisto beni e servizi) in cui gli attori interagiscono per via elettronica piuttosto che con scambi fisici e contatti diretti
- Tipologie:
  - ◆ B2B - Business to Business (93%)
  - ◆ B2C - Business to Consumer (7%)

# Commercio Elettronico

- Transazione Commerciale:  
inoltro dell'ordine dall'acquirente  
al negozio virtuale (Internet)
- Transazione Finanziaria:  
inoltro istruzioni di pagamento  
da parte dell'acquirente
  - ◆ off-line (es. via telefono o fax)
  - ◆ on-line - pagamento elettronico

# Pagamento elettronico

- Metodi “hardware”
  - ◆ borsellino elettronico (smart-card)
- Metodi “software”
  - ◆ debit-based (assegni elettronici)  
Netchex, Redi-check, Netchegue, Banknet, FSTC
  - ◆ credit-based (uso di carte di credito)  
CyberCash, FirstVirtual, STT-SEPP, TelePay, SET
  - ◆ token-based (moneta virtuale)  
Millicent, Netbill, E-Cash, DigiCash, PayPal, WebMoney, cashU..

# Il Sistema SET - Secure Electronic Transaction

- Nato da accordo Visa-Mastercard (GTE, IBM, Microsoft, Netscape)
- Non prevede connessione sicura (non opera a livello di pacchetto come SSL) ma gestisce la transazione di pagamento a livello di applicazione
- Basato su crittografia (RSA + DES) e certificati digitali (standard X.509)

# SET - Attori

- Il possessore di carta di credito (il compratore)
- Il venditore
- Un'Autorità di Certificazione, garante dell'identità delle parti coinvolte (es. VeriSign)
- Un Payment Gateway (l'intermediario)
- La rete di pagamento delle istituzioni finanziarie

# SET - Fasi operative

- **User Registration:**  
l'utente si registra presso un'autorità e ottiene un certificato
- **Purchase Request:**  
l'utente invia l'ordine di acquisto
- **Payment Authorization:**  
il venditore richiede al gateway l'autorizzazione e provvede alla consegna del bene o servizio
- **Payment Capture:**  
avviene il trasferimento della somma

# SET - User Registration (1)

- **Initiate Request**  
invio (non protetto) richiesta di registrazione all'authority
- **Initiate Response**  
l'authority risponde includendo il proprio certificato e autenticandolo apponendo la propria firma digitale
- **Registration Form Request**  
il richiedente fa le verifiche, memorizza il certificato ad uso futuro, e chiede il form appropriato (c/c bancario, diverse carte credito) usando la chiave pubblica dell'authority
- **Registration Form**  
l'authority fa le verifiche e invia all'utente il form richiesto (al solito con con certificato firmato)

# SET - User Registration (2)

- **Cardholder Certification Request**

il richiedente fa le verifiche sul form, se non già disponibili il sw genera una coppia di chiavi simmetriche per l'utente; questi compila il form (es. con dati carta di credito), che viene cifrato con una chiave simmetrica, posta in busta elettronica sigillata con la chiave pubblica dell'authority e inviata alla stessa

- **Cardholder Certificate**

l'authority apre la busta, legge la chiave con cui decifra il form, prende una decisione sul rilascio dell'autorizzazione; in caso positivo genera il certificato per l'utente, lo firma digitalmente e lo invia in messaggio protetto

- **Certificate**

il richiedente decifra il certificato, fa le verifiche del caso e registra il suo certificato per usi futuri

# SET - Purchase Request

## ■ Initiate Request

invio (non protetto) del proprio certificato al venditore

## ■ Initiate Response

il venditore assegna alla transazione un identificatore (ID) univoco e lo pone, assieme ai certificati proprio e del payment gateway in un messaggio firmato digitalmente che invia in modo protetto al compratore

## ■ Purchase Request

il compratore verifica i certificati inviati, genera order information (OI) e payment instructions (PI) in cui è inserito il TI; OI non contiene dati riservati e viene semplicemente firmato, PI viene cifrato con chiave simmetrica e posto in busta che solo il payment gateway potrà aprire; infine PI e OI sono inviati al venditore

## ■ Purchase Response

il venditore verifica il certificato del compratore e l'ID in OI e invia richiesta di approvazione al gateway; avuta la risposta la invia al compratore apponendo la propria firma ("ricevuta" della transazione per il compratore)

# SET - Payment Authorization

## ■ Authorization Request

il gateway riceve dal venditore la richiesta di autorizzazione contenente PI cifrato con chiave simmetrica e posti in busta digitale dal compratore, le informazioni riguardanti la transazione cifrati con chiave simmetrica posti in busta digitale dal venditore e i certificati di compratore e venditore

## ■ Authorization Response

il gateway riceve la richiesta di autorizzazione, controlla i certificati, apre le buste digitali ricavandone le chiavi simmetriche di compratore e venditore con cui decifra PI e richiesta di autorizzazione; se le informazioni inviate da compratore e venditore corrispondono, la richiesta di autorizzazione viene inoltrata all'istituto finanziario (es. su rete interbancaria); se la transazione è approvata, il gateway invia un messaggio al venditore contenente un capture token che verrà usato in seguito per l'accredito

# SET - Payment Capture

- **Capture Request**

il venditore crea un messaggio di richiesta, lo firma e lo cifra usando una chiave simmetrica; il messaggio cifrato viene poi inserito in una busta indirizzata al payment gateway cui viene inviato assieme al capture token e ai certificati di compratore e venditore

- **Capture Response**

il payment gateway controlla i certificati, apre la busta digitale ed estrae la chiave simmetrica a lui destinata con cui decifra le informazioni e controlla la firma digitale; superati i controlli il gateway invia il capture token all'istituto finanziario affinché venga eseguito il trasferimento di fondi; se è tutto OK, il gateway invia un messaggio di conferma al venditore in busta digitale, assieme al proprio certificato.

# Firma alla cieca (blind signature)

- Necessaria per proteggere la privacy in settori quali e-commerce (sistemi di pagamento) ed e-governement (sistemi di voto)
- Nel caso di gestione pagamenti garantisce:
  - ◆ Incapacità di terze parti a determinare identità del pagatore, momento e importo dei pagamenti fatti da un individuo
  - ◆ Capacità per un individuo di fornire prove di pagamento o di determinare l'identità del pagatore in circostanze eccezionali (controversie)
  - ◆ Capacità di bloccare le transazioni per mezzi di pagamento risultati rubati o contraffatti

# Firma alla cieca (1)

- Metodo base (Chaum 1998) con RSA
- Un attore A vuole farsi firmare un messaggio M da un validatore V senza che V possa leggerlo
- V ha chiave pubblica  $(e,n)$  e chiave privata  $(d,n)$
- A utilizza una funzione di blinding nota solo a lui con cui “occulta” il messaggio da firmare  $M' = f(M)$

# Firma alla cieca (2)

- A genera un numero casuale  $r$  (blinding factor) coprimo con  $n$
- A calcola  $M' = M r^e \bmod n$ , e lo spedisce a V (dato che  $r$  è casuale anche  $M'$  risulta casuale)
- V lo firma con la propria chiave privata  $(d, n)$  generando  $S' = (M')^d \bmod n$ , e lo invia ad A
- A calcola  $S = S' / r \bmod n$
- Per la relazione  $r^{ed} = r \bmod n$ , si ha che  $S = (M r^e)^d / r \bmod n = M^d \bmod n$
- Quindi  $S$  è il messaggio  $M$  di A firmato dal validatore  $V$  alla cieca, senza conoscerne il contenuto (a  $V$  è noto  $M'$  non  $M$ )

# Firma alla cieca (3)

- M' equivale alla spedizione di M dentro una busta chiusa contenente carta carbone
- V firma M alla cieca, apponendo la propria firma senza aprire la busta, grazie alla carta carbone
- A apre la busta chiusa S' restituitagli da V dentro la quale trova M con la firma di V
- A può quindi utilizzare S (validato da V) in rapporti con terze parti

# Firma alla cieca – Esempio d'uso

- A è un acquirente di un bene e M è la fattura relativa al pagamento (contenente la descrizione del bene e i dati del venditore ma non quelli di A)
- V è la banca che riceve M' da A, addebita l'importo sul conto di A, quietanza la fattura e la restituisce ad A come S'
- A estrae S da S' (verifica che contenga M) e lo invia al venditore X come prova di pagamento
- Il venditore X riceve S (verifica che contenga M) e lo invia alla banca, che lo inserisce nell'archivio dei pagamenti completati e provvede ad accreditare l'importo sul conto di X e a notificargli l'accredito
- Il venditore X conferisce il bene all'acquirente A