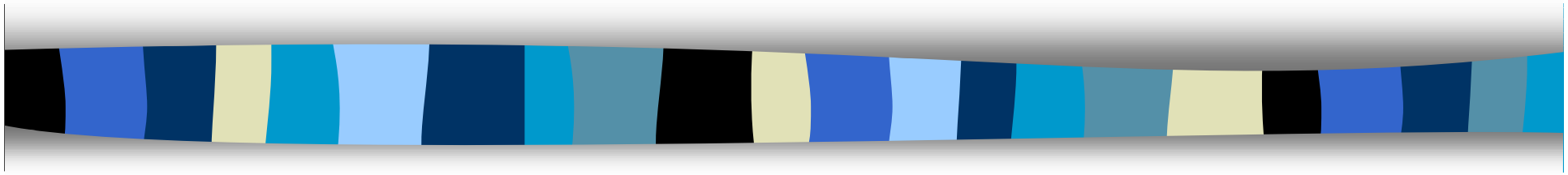
INFORMATICA



Prof. MARCO CASTIGLIONE
ISTITUTO TECNICO STATALE TITO ACERBO - PESCARA

Sicurezza Informatica

1. ASPETTI GENERALI

1. Sicurezza - Aspetti Generali

DEFINIZIONI

- **Sicurezza di un sistema informatico**

  Per sicurezza si intende la salvaguardia dei seguenti aspetti:
  - affidabilità;
  - integrità;
  - riservatezza;
  - autenticità;
  - non ripudio.

- **Sistema sicuro**

  Quando le informazioni vengono garantite contro le violazioni degli aspetti di sopra con sistemi e misure di sicurezza opportunamente predisposti.

1. Sicurezza - Aspetti Generali

DEFINIZIONI

- **Affidabilità dei dati**

  Proprietà dei dati per essere sempre accessibili o disponibili agli utenti autorizzati.
  - Mancanza di fornitura elettrica.
  - Malfunzionamenti hardware/software.

- **Integrità dei dati**

  Proprietà che garantisce la corruzione dei dati, nella trasmissione e nella memorizzazione.
  - Cancellazione e modifica non autorizzate di dati e file.

1. Sicurezza - Aspetti Generali

DEFINIZIONI

- **Riservatezza**

  Proprietà che rende i dati accessibili in lettura solo dai legittimi destinatari.
  - Intercettazione dati durante la trasmissione.
  - Accesso non riservato ad un server.

- **Autenticazione o autenticità**

  Proprietà che garantisce la certezza della sorgente, della destinazione del contenuto dei dati.
  - Furti di identità in una e-mail.

1. Sicurezza - Aspetti Generali

DEFINIZIONI

- **Non ripudio**

  Certezza che chi trasmette (non ripudio del mittente) e chi riceve (non ripudio del destinatario) non possano negare di aver ricevuto e trasmesso rispettivamente i dati.
  - Ricevuta di ritorno (raccomandata) per il destinatario.
  - Firma autenticata per il mittente.

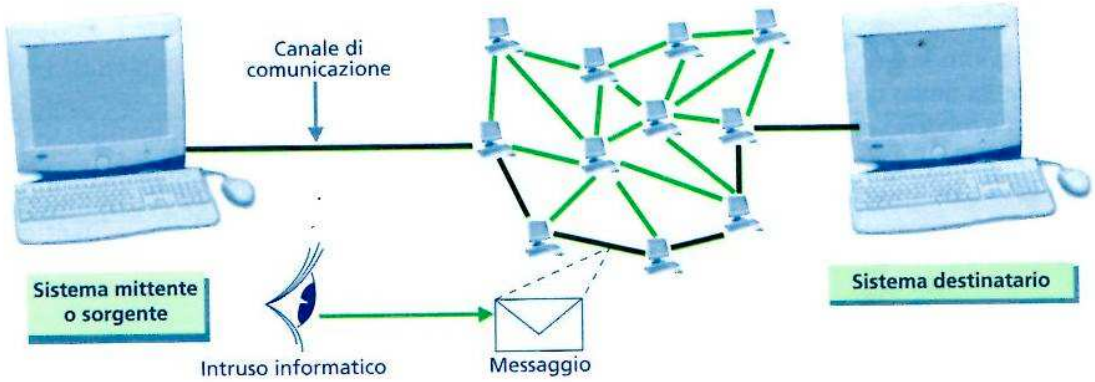
- **Accesso non autorizzato ad un sistema informatico**
  Violazione di domicilio.
- **Copiatura di dati e programmi**
  Violazione del diritto d'autore.

1. Sicurezza - Aspetti Generali

SICUREZZA IN RETE

- **Internet**

  E' sempre possibile interporsi fisicamente tra mittente e destinatario dei dati per intercettare i singoli pacchetti.
  - Intercettare e-mail.
  - Intercettare numeri carte di credito.



- **Sistema aperto**

  La rete Internet è nata senza affrontare le problematiche legate alla sicurezza delle informazioni.

1. Sicurezza - Aspetti Generali

VIOLAZIONI DELLA SICUREZZA

- **Attacco ai sistemi informatici**

  Qualsiasi agente accidentale o intenzionale finalizzato a superare le misure di sicurezza.

- **Agente attivo o passivo**
  Attivo se viola tutti gli aspetti di sicurezza.
  Passivo se viola solo l'aspetto della riservatezza.
- **Agente non umano**
  Può essere catastrofico (terremoto, ...) o frequente (corrente elettrica, …)
- **Agente umano**
  Può essere intenzionale (crimine informatico) o non intenzionale (cancellazioni casuali, …)

1. Sicurezza - Aspetti Generali

STRUMENTI DI VIOLAZIONE

- **Hacker, Cracker, pirati o criminali informatici**
  Coloro che commettono crimini informatici.

- **Sniffing**
  Ascoltare e catturare dati che viaggiano in rete.
- **Spoofing**
  Invio di pacchetti camuffandone l'indirizzo del mittente.
- **E-mail bombing**
  Invio di una enorme quantità di messaggi ad un utente con lo scopo di provocare il crash del server.
- **Spamming**
  Invio di posta non desiderata.

1. Sicurezza - Aspetti Generali

STRUMENTI DI VIOLAZIONE

- **Codice malefico o malware**

  Qualsiasi programma che riesce ad introdursi in un sistema all'insaputa degli utenti e a compiere operazioni più o meno dannose.

- **Cavallo di troia**

  Codice che si nasconde all'interno di un programma o documento e si attiva occasionalmente.

- **Virus**

  Programma autonomo capace di replicarsi.

- **Worm**

  Programmi che occupano la memoria libera per saturare il sistema. Nella trasmissione occupano la banda disponibile.

Sicurezza Informatica

2. CRITTOGRAFIA

2. Sicurezza - Crittografia

DEFINIZIONE

- **Crittografia**
  E' una branca della matematica che studia i metodi per trasformare un messaggio in modo da renderlo visibile solo ad un ristretto gruppo di persone (mittente e destinatario).

- **Caratteristiche**
  Un sistema di crittografia è in grado di garantire riservatezza, integrità, autenticazione e non ripudio.

2. Sicurezza - Crittografia

SISTEMI DI CRITTOGRAFIA

- **Codice di Cesare**
  - Chiave N compreso tra 1 e 25.
  - Algoritmo: sostituzione di ciascuna lettera con l'N-esima successiva.

  ESEMPIO N=3
  - lettera a sostituita con la lettera d;
  - lettera b con lettera e ….
  "ciao" => "fldr"

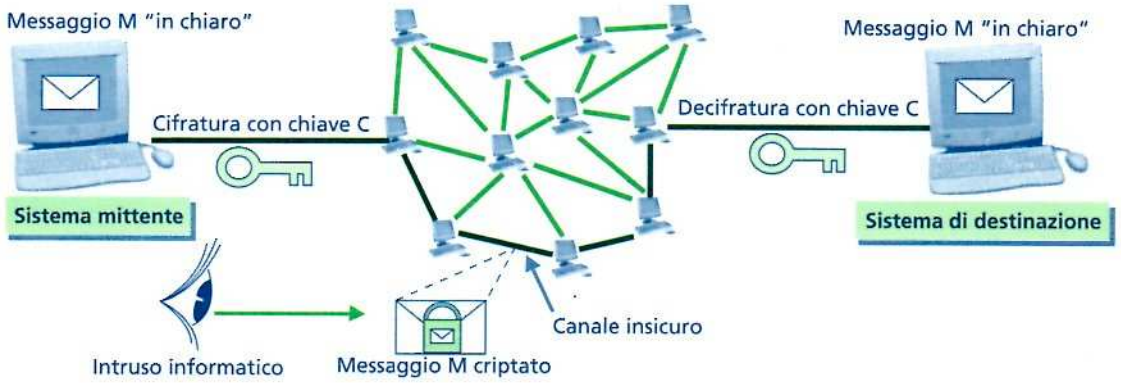
  INAFFIDABILE
  E' forzato dopo pochi tentativi!

2. Sicurezza - Crittografia

SISTEMI DI CRITTOGRAFIA

- **Crittografia simmetrica (a chiave provata)**
  Si utilizza una sola chiave, definita cifrario, per cifrare e decifrare i messaggi. La chiave deve essere conosciuta dal mittente e dal destinatario.

  - Funzione E_c = algoritmo di cifratura
  M -> (cifratura) -> $E_c(M)$ -> (invio sul canale)
  -> (decifratura) -> $E_c^{-1}(Ec(M)) = M$



2. Sicurezza - Crittografia

SISTEMI DI CRITTOGRAFIA

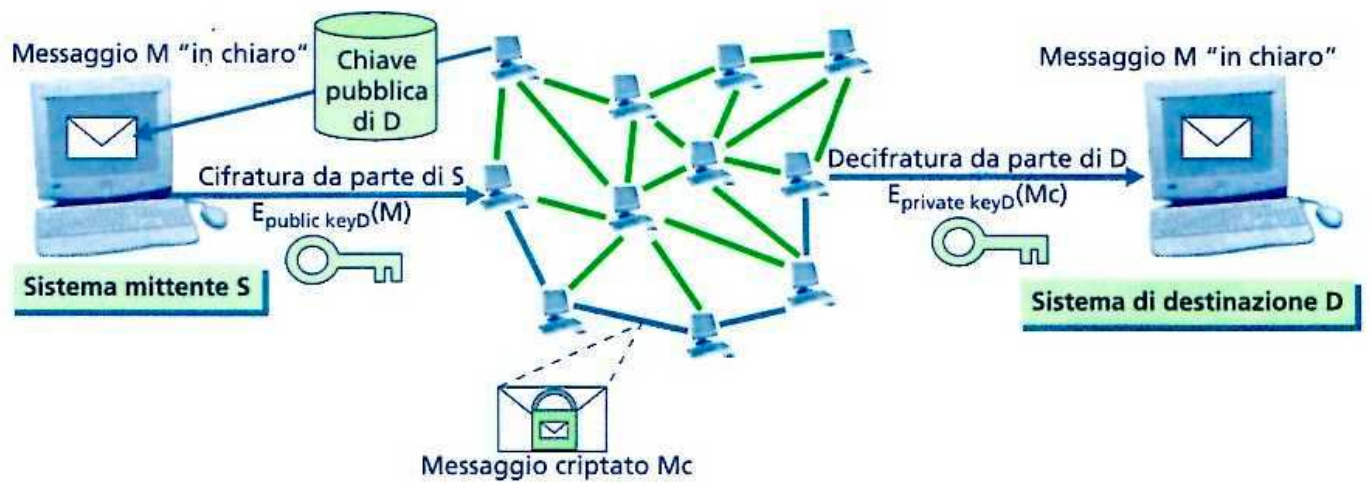
- **Crittografia asimmetrica (a chiave pubblica)**

  - 1976 Diffie e Hellmann.
  - Coppia di chiavi legate da una relazione matematica.
  - Chiave pubblica nota a tutti.
  - Chiave privata a disposizione del mittente.
  - Le chiavi possono essere utilizzate indifferentemente per cifrare e decifrare.
  - Dalla chiave pubblica non è possibile ricavare la chiave privata.

2. Sicurezza - Crittografia

CRITTOGRAFIA ASIMMETRICA

- **Autenticazione destinatario e riservatezza messaggio**

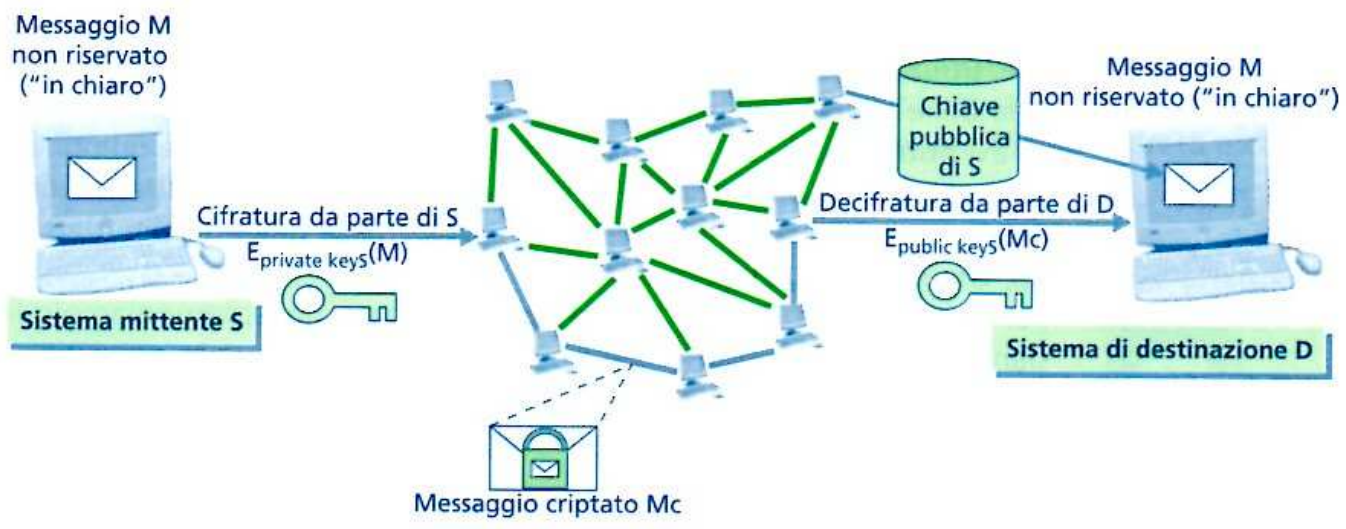


- Trasmissione da S utilizzando la pubKD:
$M_C = E_{pubKD}(M)$.
- Decifratura da parte di D unico a conoscere la priKD:
$M = E_{priKD}(M_C)$.

2. Sicurezza - Crittografia

CRITTOGRAFIA ASIMMETRICA

- **Autenticazione sorgente**

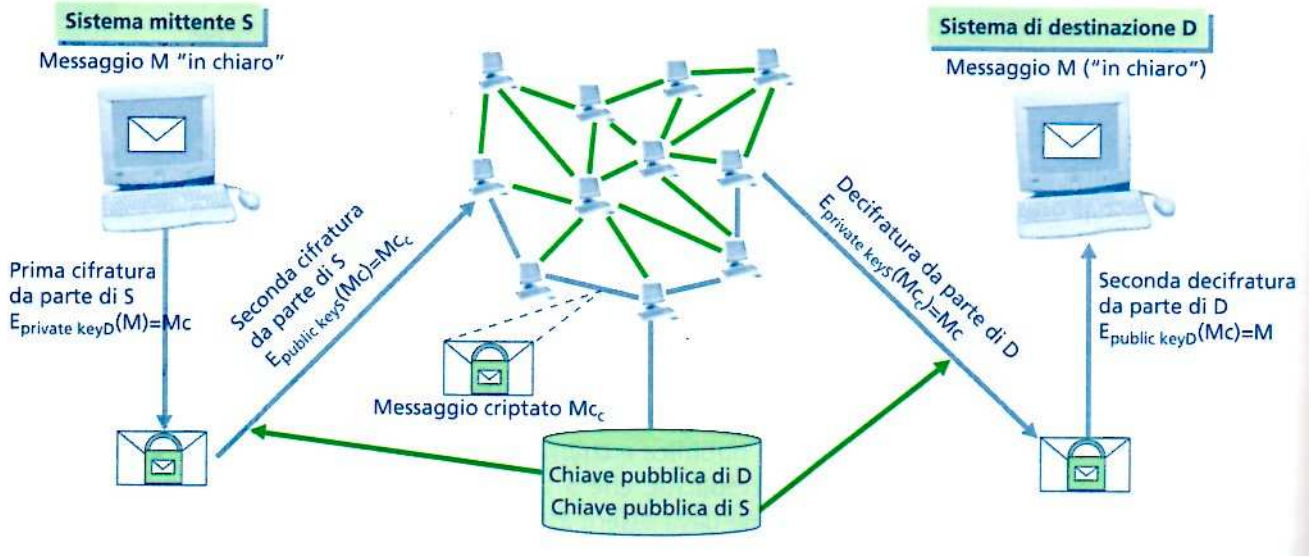


- Trasmissione da S utilizzando la priK ed unico a conoscerla:
$M_C = E_{priKS}(M)$.
- Decifratura da parte di D con la pubK:
$M = E_{pubKS}(M_C)$.

2. Sicurezza - Crittografia

CRITTOGRAFIA ASIMMETRICA

- **Autenticazione sorgente e destinazione, riservatezza**



- Trasmissione da S con due cifrature pubKD e priKS:

$M_C = E_{pubKD}(M)$ $M_{CC} = E_{preKS}(M_C)$.

- Decifratura da parte di D con la pubKS e priKD:

$M_C = E_{pubKS}(M_{CC})$ $M = E_{priKD}(M_{CC})$.

2. Sicurezza - Crittografia

FIRMA DIGITALE

- Vengono applicati i principi della crittografia asimmetrica

  - S genera l'**impronta digitale**.
  - Crittografare l'impronta digitale con chiave asimmetrica priKS per ottenere la **firma digitale**.
  - Invio del messaggio con in allegato la firma digitale.
  - Destinatario decrittografa con chiave pubKS.
  - Confronta l'impronta ottenuta con quella calcolata.
  - Integrità, autenticazione, non ripudio.

2. Sicurezza - Crittografia

FIRMA DIGITALE - NORMATIVA

- **Legge n. 59 del 15.03.1997 (Legge Bassanini)**
  - Atti, dati e documenti formati con strumenti informatici e telematici … sono validi e rilevanti ad ogni effetto di legge.

- **DPR n. 445 del 28.12.2000 (TUDA)**
  - Definizione di documento informatico.
  - Stabilisce le regole per la formazione, trasmissione, conservazione, riproduzione e validazione dei documenti informatici da aggiornare ogni due anni.
  - Stessa validità tra documento informatico e riproduzione meccanica di un documento.

2. Sicurezza - Crittografia

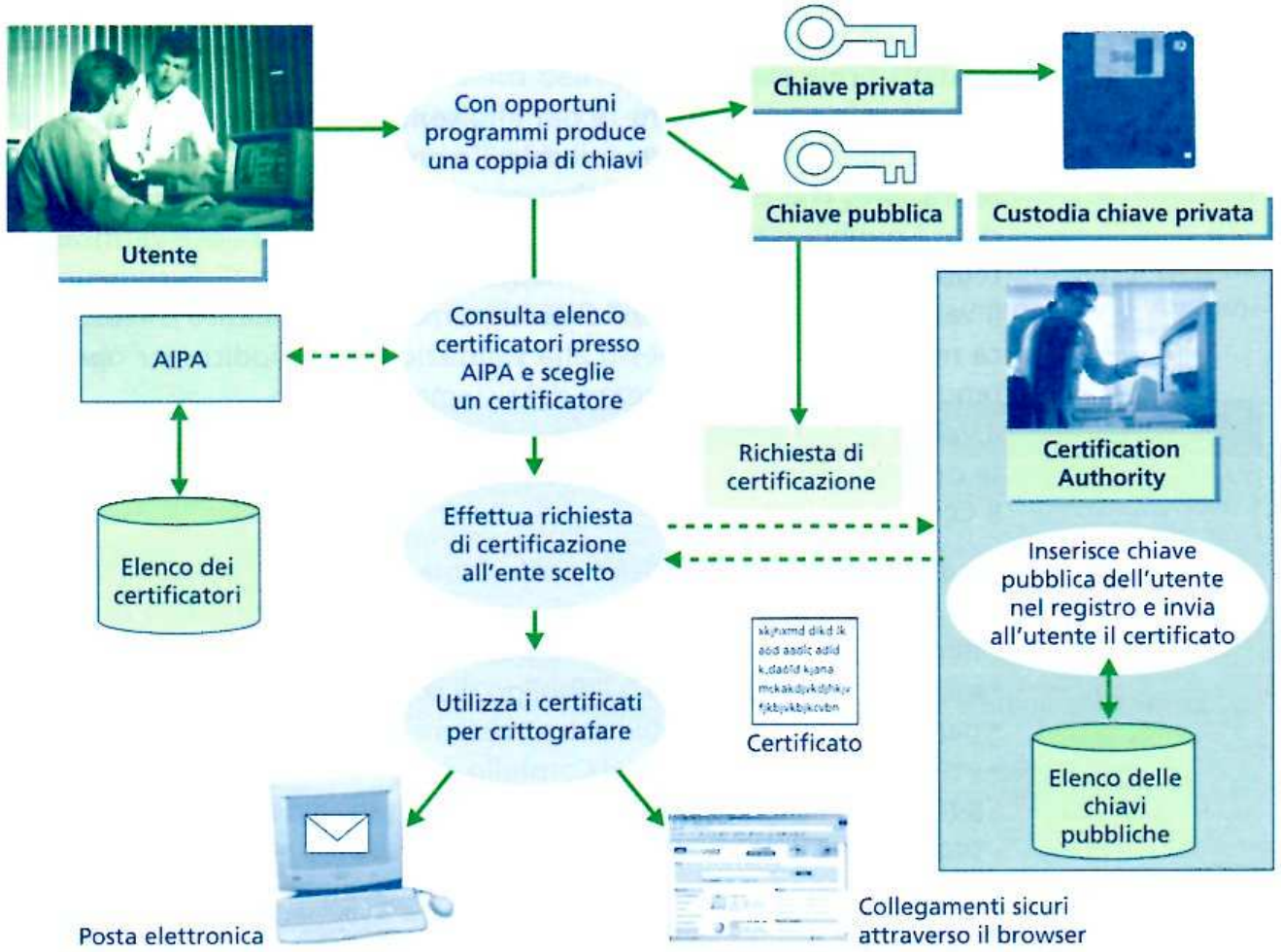
FIRMA DIGITALE - NORMATIVA

- **D.Lgs. N. 82 del 07.03.2005**

  Riorganizzazione della PA nell'utilizzazione di strumenti informatici e telematici.
  - Regole tecniche per la firma digitale.
  - Obbligo di consentire il pagamento in modalità informatica.
  - Garantire l'interoperabilità tra i sistemi informatici della PA.
  - Promozione per lo sviluppo della società dell'informazione.

2. Sicurezza - Crittografia

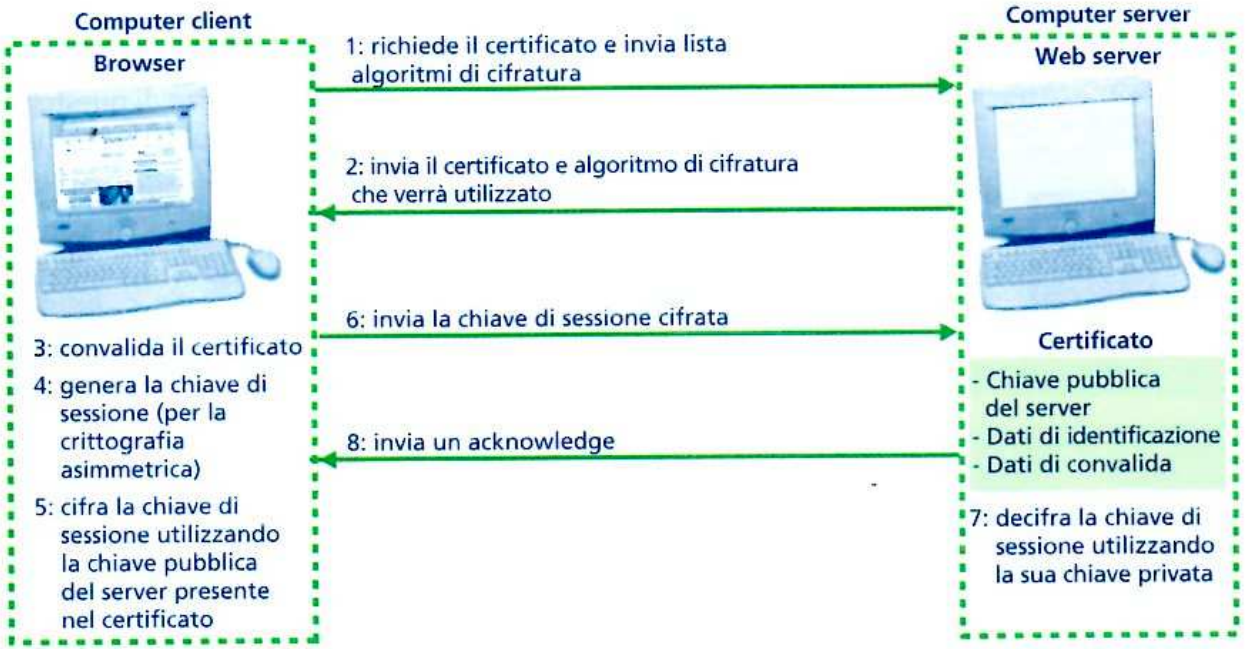
FIRMA DIGITALE - CERTIFICATORI



2. Sicurezza - Crittografia

COLLEGAMENTI SICURI

- **Protocolli SSL e HTTPS**
  - Secure Socket Layer sviluppato da Netscape per garantire privacy, autenticazione e affidabilità nelle trasmissioni in Internet.



Sicurezza

BIBLIOGRAFIA

- Piero Gallo, Fabio Salerno, ***Informatica generale***, vol. 3 Editore Minerva Italica, Milano, 2006.