Internet

Cos’è

Il Web

La posta elettronica

Cos’è

E’ una **RETE** di **RETI**, **pubblica**.

Non è una rete di calcolatori.

I computer che si collegano ad Internet, devono prima essere collegati ad una rete, la quale a sua volta sarà collegata ad un’altra. Per questo motivo si parla di rete pubblica mondiale alla quale chi vi si collega partecipa e la estende

TCP/IP

TCP/IP è il protocollo su cui si basa Internet, ed è colui che consente l'armonizzazione di reti e tecnologie diverse fra loro

Si divide in:

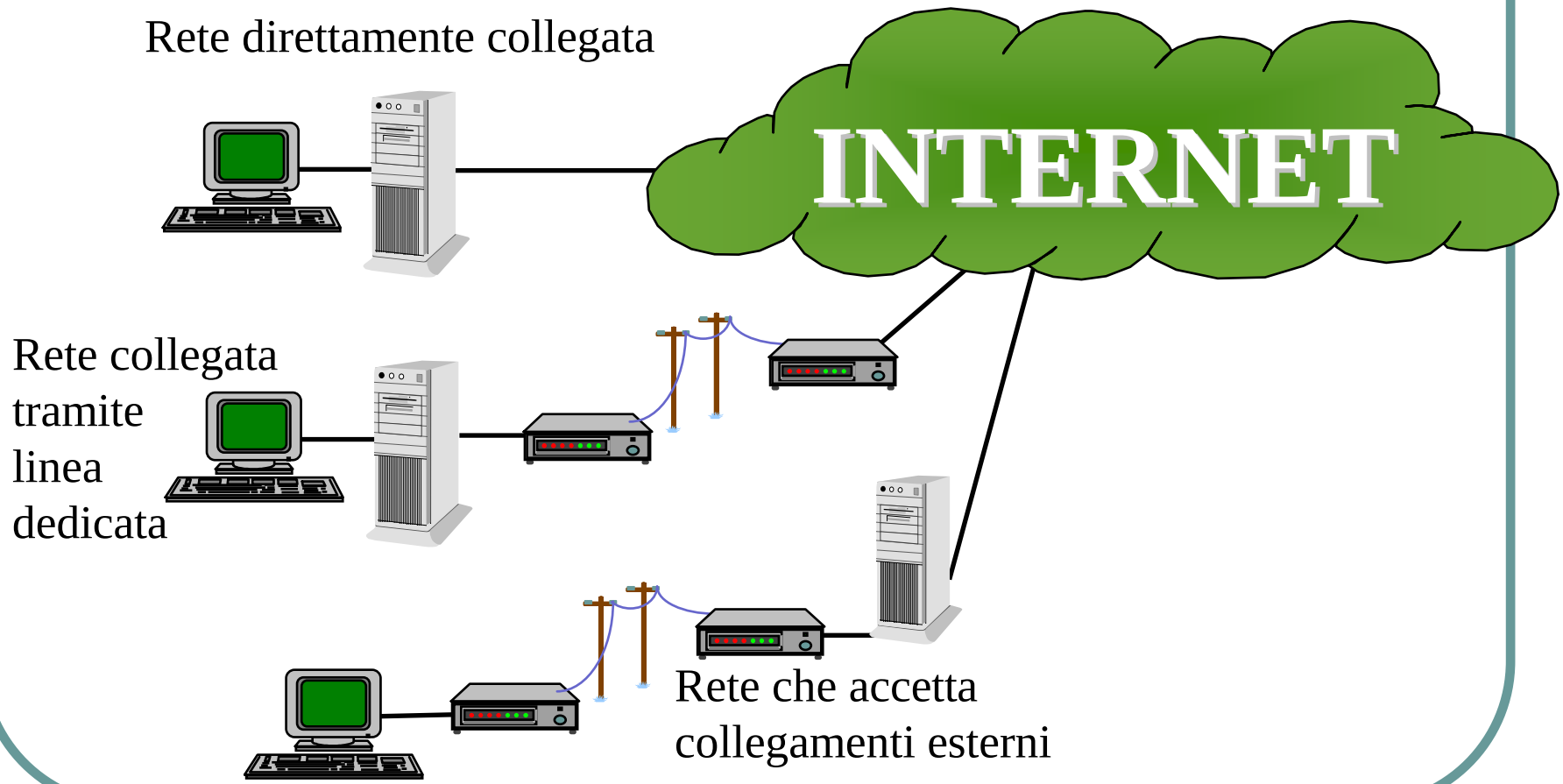
Transmission Control Protocol

- Si occupa della correzione degli errori

Internet Protocol

- Si occupa dell'instradamento delle informazioni e sincronizzazione della trasmissione

Tipi di connessione



Indirizzi Internet

Tutti i computer connessi ad Internet hanno un indirizzo IP (p.e. 151.100.3.45) che consente di renderli univoci

Per comodità vengono associati dei nomi più facilmente memorizzabili

p.e. www.utgroma.it = 213.203.150.67

Il primo da sinistra indica il nome del computer

Il secondo la rete a cui è collegato a seguire

L'ultimo a destra indica la rete principale e può rappresentare anche la tipologia (.com, .net. .gov) oppure la nazionalità (.it, .fr, .uk, .de, au)

I principali servizi

- Email - posta elettronica
- Mailing List - posta circolare
- Newsgroup - bacheche elettroniche
- FTP - cartelle condivise
- Telnet - connessioni a terminali remoti
- Web – ipertesti
- Chat e Videoconferenze
- Streaming audio e video

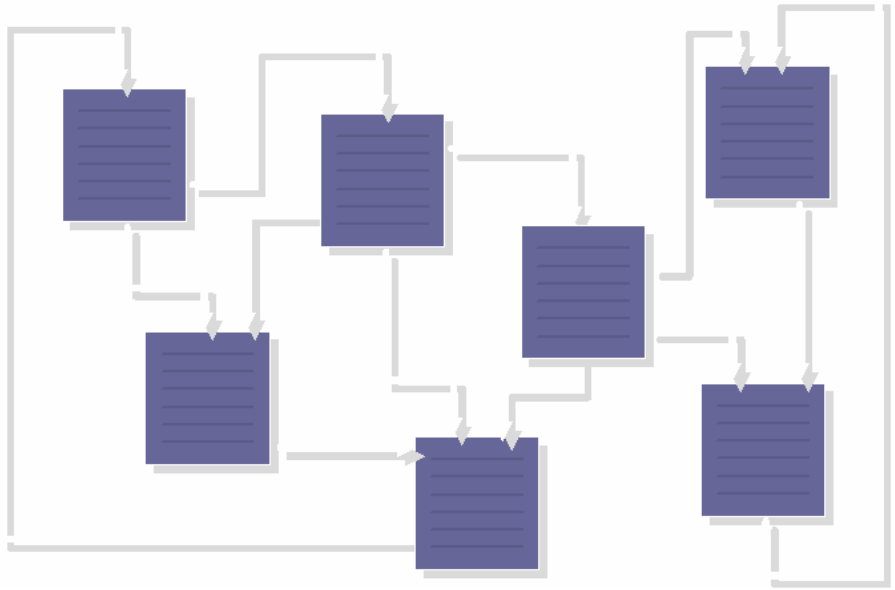
Il Web

Il web è una collezione di sistemi informativi che corrispondono alle seguenti caratteristiche:

- Distribuiti: si possono trovare su più siti posizionati anche in posti diversi
- Collaborativi: si possono scambiare le informazioni in modo automatico
- Eterogenei: possono differire sia come tipologia che caratteristiche tecniche
- Multimediali: possono offrire oggetti e servizi di varia natura

L’Ipertesto per “navigare”

La vera novità introdotta dal Web è la possibilità di “collegare”, attraverso i cosiddetti ***link***, gli oggetti fra loro e, di conseguenza, consentire una consultazione libera e casuale degli stessi



Motori di ricerca

Sono siti che consentono di trovare altri siti attraverso parole chiave oppure tramite ricerche guidate

p.e. www.altavista.com

www.google.com

www.yahoo.com

www.virgilio.it

I Browser

I browser sono i programmi installati sui nostri computer che ci consentono di “navigare” su Internet

I passi per visualizzare una informazione sono:

- L’utente digita o “clicca” l’indirizzo da cercare
- Il nostro browser traduce l’indirizzo alfanumerico in un indirizzo IP (grazie all’aiuto di alcuni server sulla rete detti DNS)
- Il browser ottenuto l’indirizzo IP richiede l’informazione direttamente al server
- Il server, se è raggiungibile e contienel’informazione desiderata, la invia al browser
- Il browser ottenuta l’informazione in forma completa l’interpreta e la visualizza

I Plug-in

Se l'informazione che abbiamo chiesto di visualizzare al nostro browser non è in un formato riconosciuto occorre installare il relativo *plug-in*, ovvero il software che ci consente di decodificare e visualizzare il formato richiesto

p.e. il formato PDF richiede il plug-in

Acrobat Reader scaricabile da Internet

Scaricare?

E’ la traduzione del termine inglese “download”, che spesso il nostro browser ci chiederà di eseguire

Vuol dire che il browser non visualizzerà l’oggetto da noi richiesto, ma ci chiederà di salvarlo semplicemente in una posizione da noi scelta fra le risorse del computer per poi essere utilizzato

Posta elettronica

E’ il servizio di Internet che ci consente di inviare messaggi ad un determinato utente

Ricordiamoci che i messaggi sono sempre dei file, ma con una caratteristica che li contraddistingue dagli altri: oltre al testo del messaggio possono contenere altri file (in allegato)

Cos’è un casella di posta elettronica

E’ una porzione di disco che si trova presso un server, sempre connesso, a cui viene associato un indirizzo di posta elettronica con una password

p.e. vincenzo.calabro@tin.it

Il nome della casella di posta elettronica

Il nome della rete o del server che la ospita

Come si usa la posta elettronica

Si deve configurare il programma di posta elettronica per accedere alla casella con i seguenti parametri:

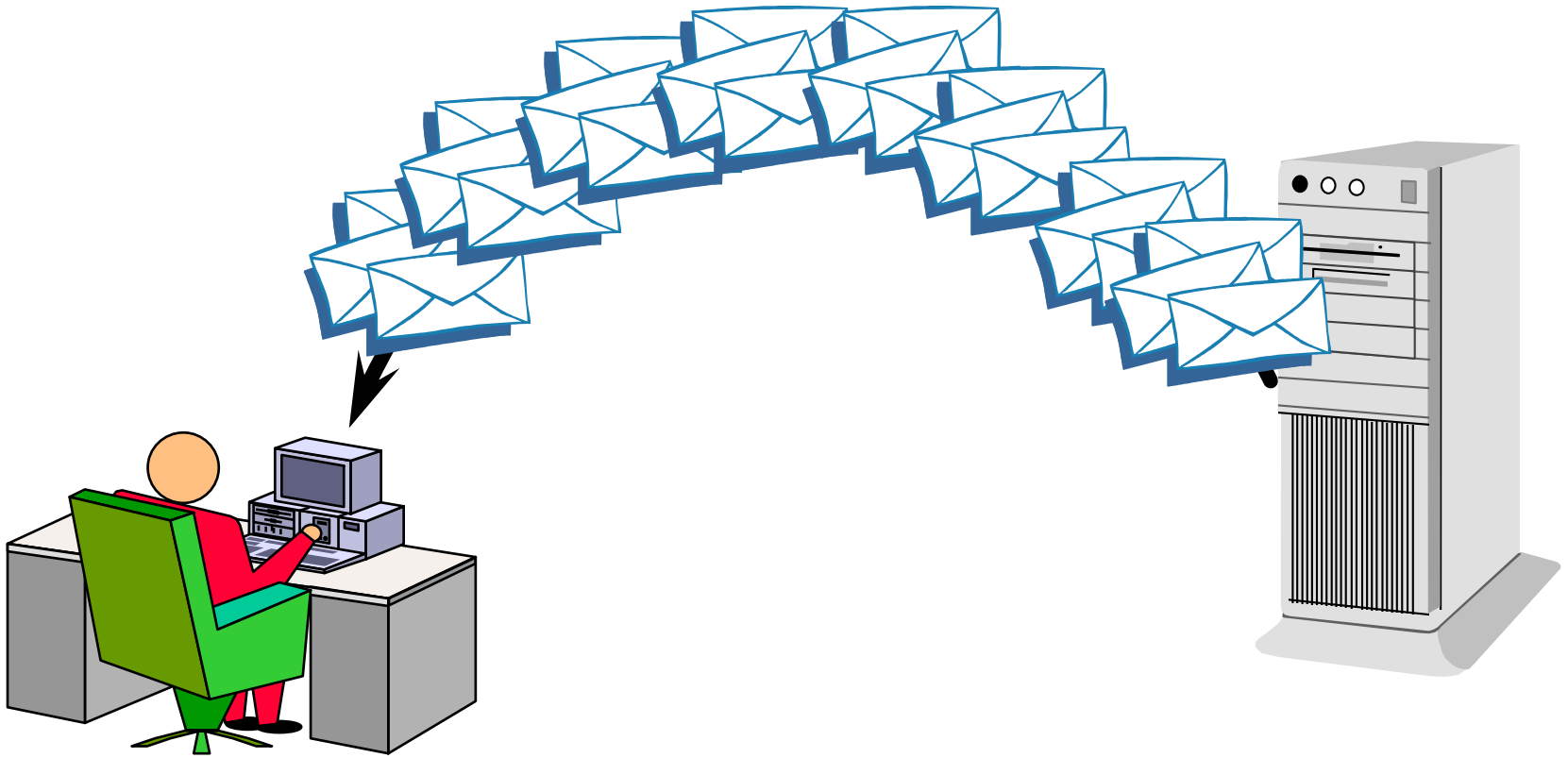
1. Indirizzo server posta in entrata (POP3)
2. Indirizzo server posta in uscita (SMTP)
3. Nome casella di posta
4. Password

Per leggere i messaggi

Si richiede la lettura tramite apposito comando del programma, il quale effettua i seguenti passi:

1. si collega al server
2. si autentica con le credenziali impostate
3. se corrette sposta i messaggi sul nostro computer da cui è possibile successivamente visualizzarli, stamparli e salvarli
4. alla fine si scollega

Lettura dei messaggi



Per scrivere un messaggio

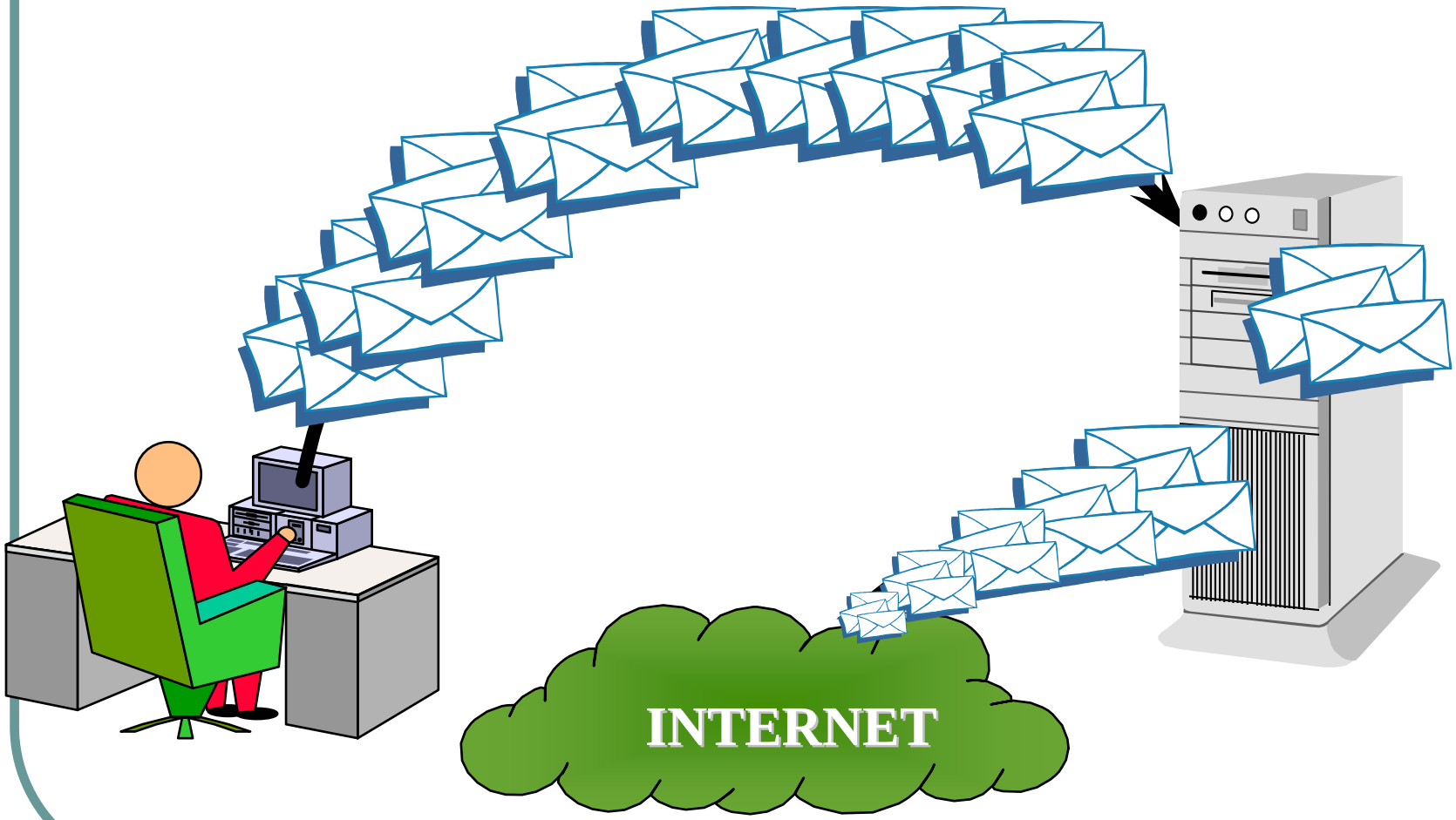
Si apre una finestra che ci chiede le seguenti informazioni:

- L'indirizzo e-mail del/i destinatario/i
- L'oggetto del messaggio
- Il corpo del messaggio
- Eventuali allegati

Dato il comando di invio il nostro programma:

1. Si collega al nostro server di posta in uscita
2. Copia il messaggio nella coda di messaggi in uscita del server e chiude la connessione
3. Il server avrà l'incarico di controllare la casella di posta del destinatario e di inoltrare il messaggio

Spedizione dei messaggi



Virus

- Negli ultimi anni la maggiore diffusione di virus informatici avviene tramite la posta elettronica, sfruttando le potenzialità e gli automatismi offerte dai programmi di posta elettronica
- I nuovi virus utilizzano tali funzionalità per attaccare il computer che li riceve ed allo stesso tempo si diffondono tramite e-mail
- Oltre ad installare un programma antivirus aggiornato, occorre fare attenzione a chi ci scrive e soprattutto al tipo di allegati che troviamo insieme ai messaggi
- E’ consigliabile cancellare sempre i messaggi con allegati sospetti o sconosciuti

Crittografia vs Firma digitale

La crittografia non si deve confondere con il processo di firma. La crittografia è un processo che altera il contenuto originario e leggibile di un testo (*plaintext*) attraverso l'applicazione di algoritmi che trasformano il contenuto leggibile in un contenuto non leggibile o interpretabile (*ciphertext*) senza l'utilizzo di strumenti idonei (conoscenza della *chiave di cifratura*).

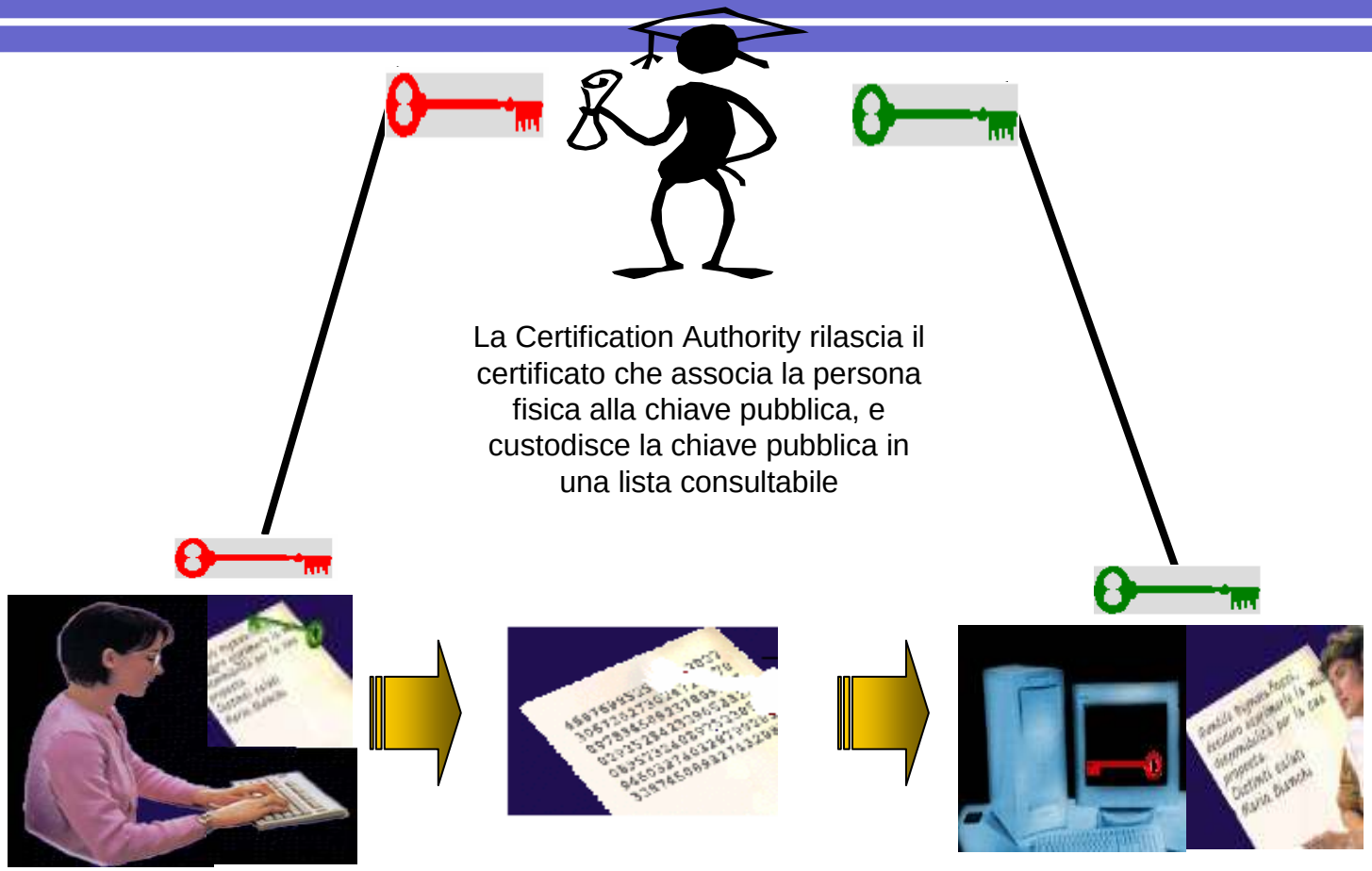
La firma digitale utilizza la crittografia come strumento, ma è un processo che si prefigge:

- autenticità del mittente,
- integrità del documento,
- non ripudio del documento

Strumenti per la Firma digitale

- Algoritmo di crittografia asimmetrico
- Certificato con una coppia di chiavi (chiave pubblica - chiave privata)
- Certification Authority (genera e revoca i certificati)
- Registration Authority (associa il certificato a un soggetto)

Il processo di firma



La Certification Authority rilascia il certificato che associa la persona fisica alla chiave pubblica, e custodisce la chiave pubblica in una lista consultabile

Il mittente firma con la sua chiave privata un documento

Il messaggio firmato, insieme al certificato del mittente rilasciato dalla CA, raggiunge il destinatario

Il destinatario, usando la chiave pubblica del mittente, riesce a determinare l'autenticità dello stesso e l'integrità del messaggio

Possibili scenari

	Obiettivo principale raggiunto
Il mittente codifica il messaggio con la key_{pub} del destinatario	La **riservatezza** del documento in quanto solo il destinatario, che possiede la sua chiave privata può rimetterlo in chiaro.
Il mittente codifica il messaggio con la propria key_{pri}	La **autenticità** del documento in quanto il destinatario, accedendo alla chiave pubblica del mittente può rimetterlo in chiaro.
Il mittente codifica il messaggio con la key_{pub} del destinatario e poi lo firma utilizzando la propria key_{pri}	La **autenticità** e la **riservatezza** del documento in quanto chiunque, accedendo alla chiave pubblica del mittente, può sapere da chi proviene il documento, ma solo il destinatario, può rimetterlo in chiaro.

Azioni lato mittente

- genera l'impronta ($hash_{mittente}$) del documento (una stringa binaria di lunghezza fissa ed univoca dello stesso. (La legge italiana prevede l'algoritmo SHA-1 a 160 bit che ha una resistenza alle collisioni=10^{48} tentativi),
- firma il documento, cioè crittografa con la sua chiave privata l'hash del documento,
- genera l'associazione documento-firma-certificato emesso dalla Certification Authority secondo lo standard PKCS#7 dando vita alla "busta elettronica".

Azioni lato destinatario

- apre la busta elettronica,separa il documento in chiaro dalla firma e calcola l'hash del documento (applicando lo stesso algoritmo mittente) ottenendo l'$hash_{destinatario}$
- utilizza la chiave pubblica del mittente, estratta dal certificato per ottenere l'$hash_{mittente}$,
- confronta $hash_{mittente}$ con $hash_{destinatario}$. Se l'esito è positivo, il messaggio si deve ritenere, integro.

Il Computer nella vita di ogni giorno

- Il Computer al lavoro
  - Office Automation
  - Amministrazione Aziendale
  - Ambito Industriale
  - Servizi (Biglietteria online, home banking)
  - Pubblica Amministrazione
  - Ambito Sanitario
  - Formazione
- Mondo elettronico
  - Posta elettronica
  - Commercio elettronico

Salute, sicurezza e ambiente

- Ergonomia
  - Postazione di lavoro
  - Postura dell'operatore
  - Caratteristiche dell'ambiente
- Salute
  - Disturbi muscolo-scheletrici, affaticamento visivo, affaticamento psichico e stress
- Precauzioni
  - Cavi elettrici
- Ambiente

Sicurezza

- Sicurezza dei dati
  - Proteggere i dati (furto)
  - Proteggere i dati personali (privacy)
  - Misure
    - Autorizzazioni
    - Protezione Password
    - Backup/Salvataggio dei dati
- Virus

Diritto d’autore e aspetti giuridici

- Copyright
  - Licenza d’uso
  - Pirateria
- Legislazione sulla protezione dei dati
- Reati informatici