Fabio Burroni

Dipartimento di Ingegneria dell'Informazione

Università degli Studi di Siena

burronif@unisi.it

Sistemi e tecnologie per la multimedialità e telematica

La Sicurezza delle Reti

La presentazione è scaricabile da http://www.ltt.dii.unisi.it/benelli.htm

La Sicurezza delle Reti

Il modello OSI



Il software delle reti

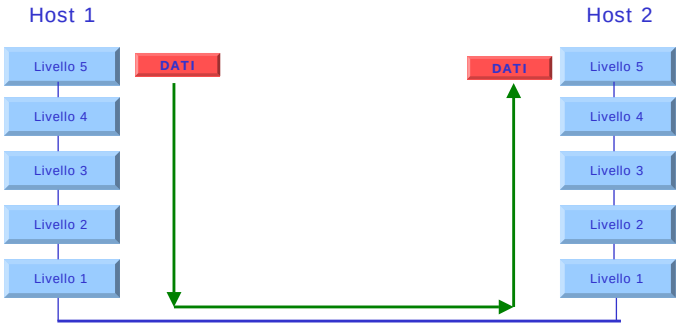
Esempio Architettura a 5 livelli



Il software delle reti

Supponiamo che l'Host 1 deve mandare dei dati all'Host 2.

I dati fisicamente fluiscono dal livello più alto a quelli inferiori, fino al livello più basso, che li trasmette nel mezzo fisico di trasmissione. Raggiunto l'host destinatario i dati risalgono tutti i livelli fino a quello più alto.



Il software delle reti

Ogni livello offre un servizio al livello superiore. Quindi, ad esempio, il livello 4 offre un servizio al livello 5. Per realizzare il servizio il livello 4 appende ai dati ricevuti dal livello 5 delle informazioni aggiuntive. Tali informazioni sono dette **Header**, o intestazione.



Il livello 5 genera i dati (**pacchetto**).

Il livello 4 appende l'header e passa tutto il pacchetto (H4 + dati) al livello 3.

Il livello 3 riceve il pacchetto (H4 + dati) dal livello 4 appende l'header e passa tutto il pacchetto (H3 + H4 + dati) al livello 2.

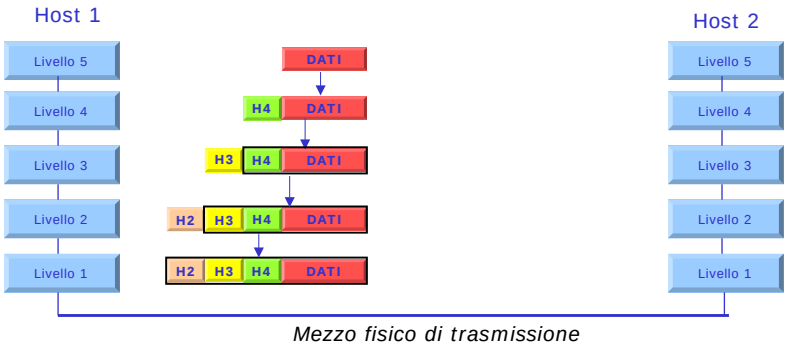
E così via....

L'Header aggiunto da livello 4 contiene, in generale, informazioni, su come devono essere trattati i dati. Tali informazioni saranno interpretate dal livello 4 (paritetico) dell'host destinatario.

L'header può contenere: numero di sequenza del pacchetto, priorità del pacchetto, campi di controllo degli errori, time stamp, ecc.

Il software delle reti

Trasmissione

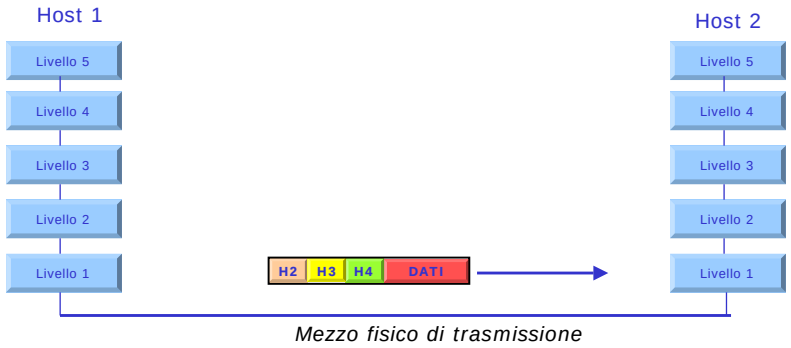


Questo meccanismo si chiama "**incapsulamento**".

Il livello 1 non appende nessun header. Si limita a trasmettere l'intero pacchetto ricevuto dal livello 2 sul mezzo fisico di trasmissione.

Il software delle reti

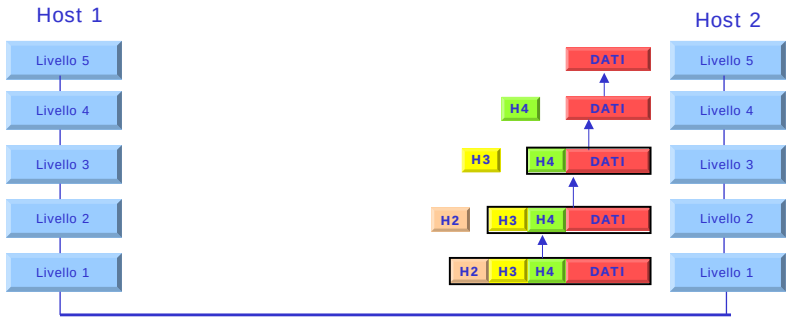
Trasmissione



L'intero pacchetto, realizzato mediante il meccanismo di "**incapsulamento**", percorre il mezzo fisico di trasmissione e raggiunge il livello 1 dell'host destinatario.

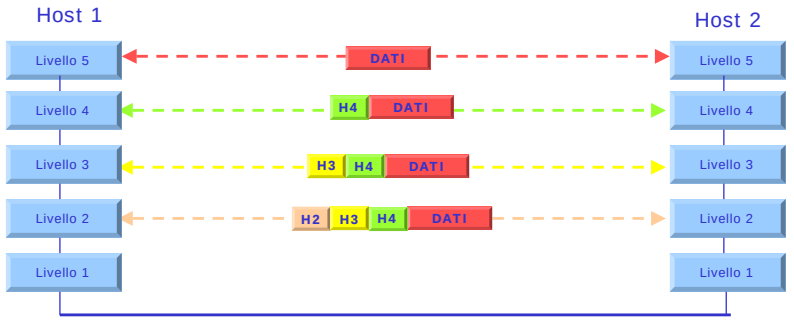
Il software delle reti

Ricezione



Il livello 1 passa il pacchetto al livello 2.
Il livello 2 rimuove l'Header 2, interpreta le informazioni contenute in H2 ed agisce in base ad esse, quindi passa il pacchetto al livello 3.
In definitiva il livello 5 dell'host 2, riceve i dati così come sono stati trasmessi.

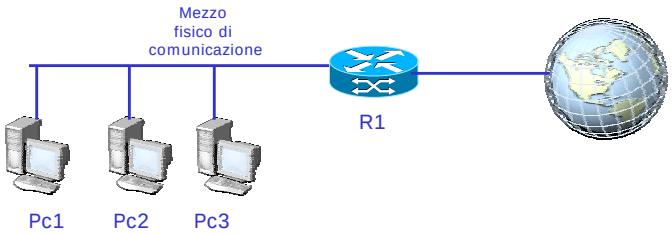
Il software delle reti



In sostanza, con il meccanismo di incapsulamento, livelli paritetici su host distinti si sono scambiati delle informazioni, quindi hanno stabilito una comunicazione. Si parla in questo caso di "**comunicazione virtuale**".

Debolezze delle reti locali.

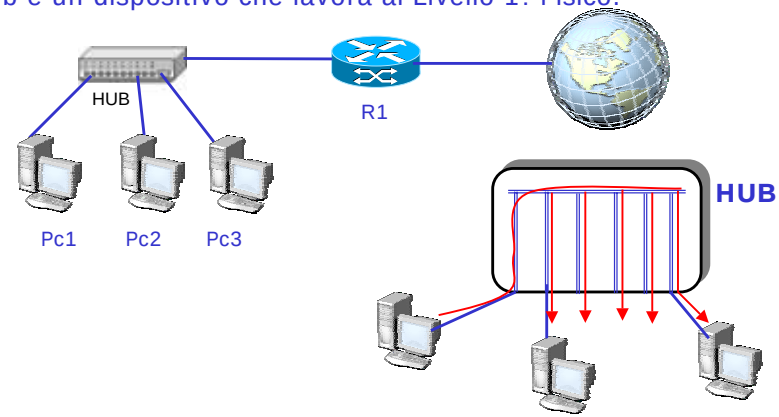
Le reti locali sono fondamentalmente reti Broadcast e questo costituisce un punto debole dal punto di vista della sicurezza. Vediamo un esempio:
Consideriamo la seguente rete Lan Ethernet:



Il mezzo fisico di comunicazione (cavo) è condiviso da tutti gli host. In realtà le moderne reti locali hanno una configurazione diversa: a **stella.**

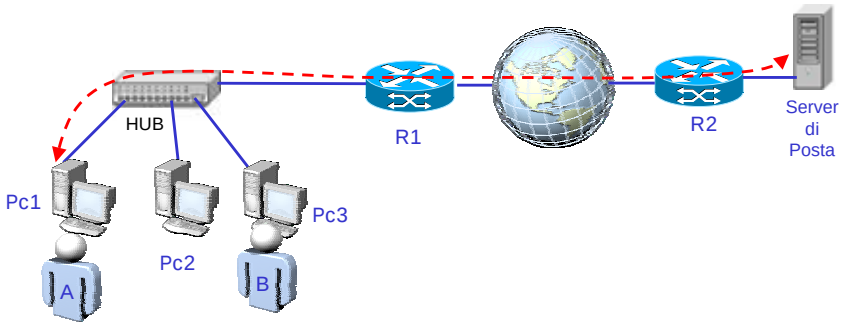
Debolezze delle reti locali.

L'**Hub** sostituisce il "cavo" condiviso da tutti gli host. In gergo si dice che il cavo è collassato all'interno dell'Hub. La funzione dell'Hub è quella di amplificatore. In sostanza amplifica il segnale proveniente da una porta e lo ritrasmette a tutte le altre porte.
L'Hub è un dispositivo che lavora al Livello 1: Fisico.



Debolezze delle reti locali.

Supponiamo che l'utente **A** stia scaricando la propria posta elettronica.
L'utente **B** sta utilizzando un **Packet Sniffer**.



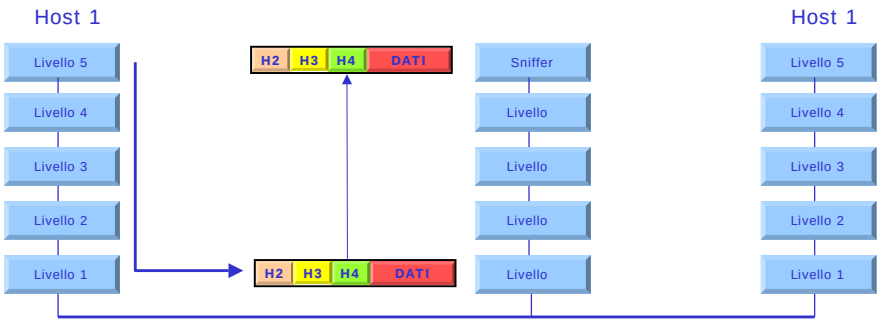
Debolezze delle reti locali.

Cosa è un "packet sniffer" ?

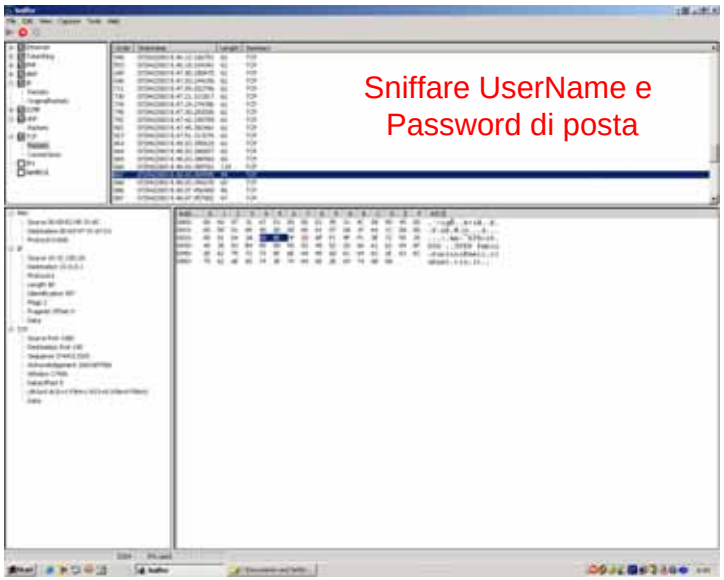
Un packet sniffer è un programma in grado di analizzare tutti i pacchetti che circolano su una rete locale.

Un packet sniffer nasce come programma di diagnostica delle reti, in sostanza cattura, analizza e decodifica tutti i pacchetti in transito. Permette quindi di cercare errori di trasmissione e di conoscere lo stato della rete. In realtà è ampiamente utilizzato dagli **Hacker**.

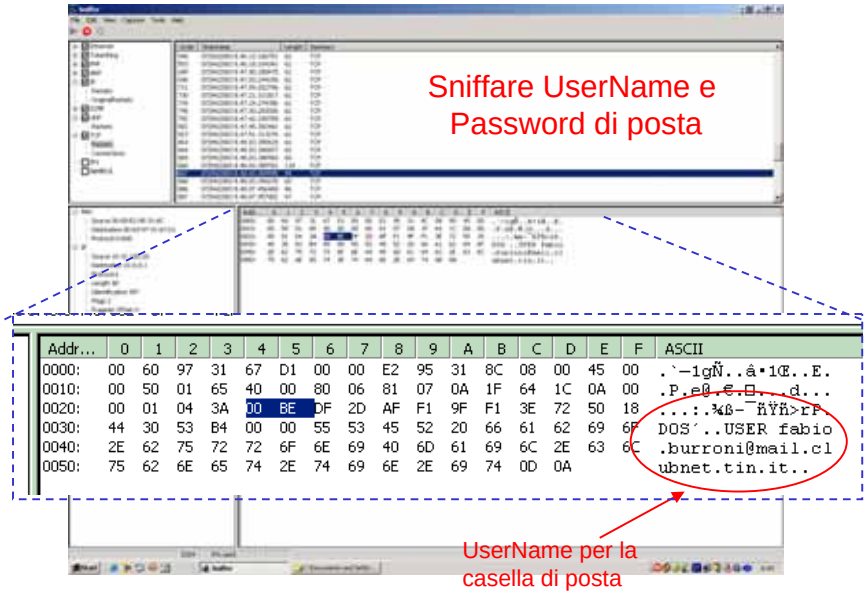
Cosa è un "packet sniffer" ?



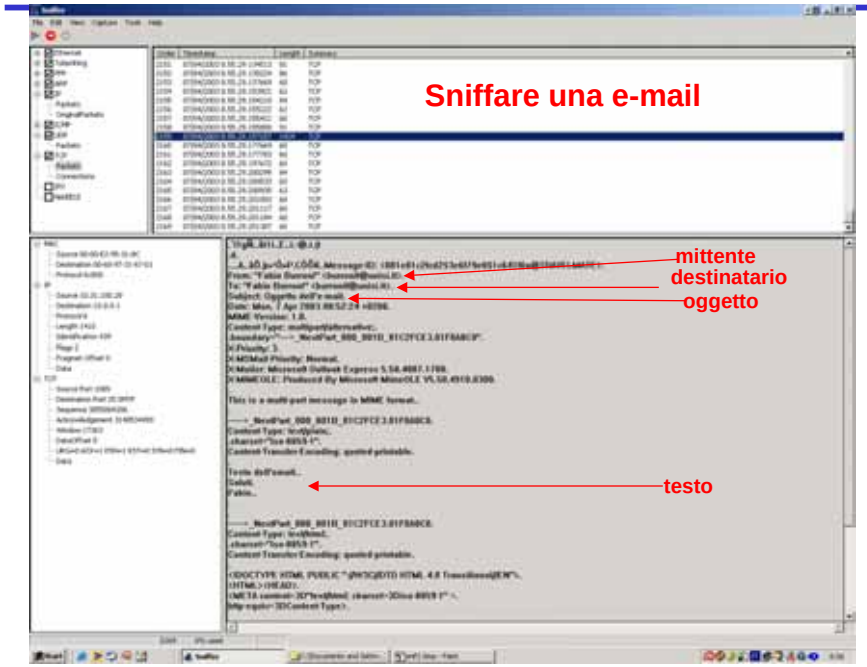
Sniffer in azione sull'Host PC3



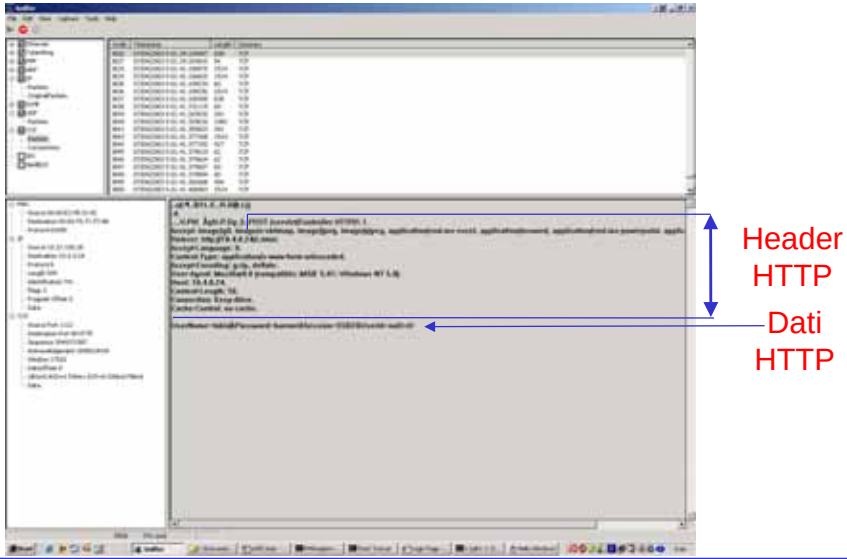
Sniffer in azione sull'Host PC3



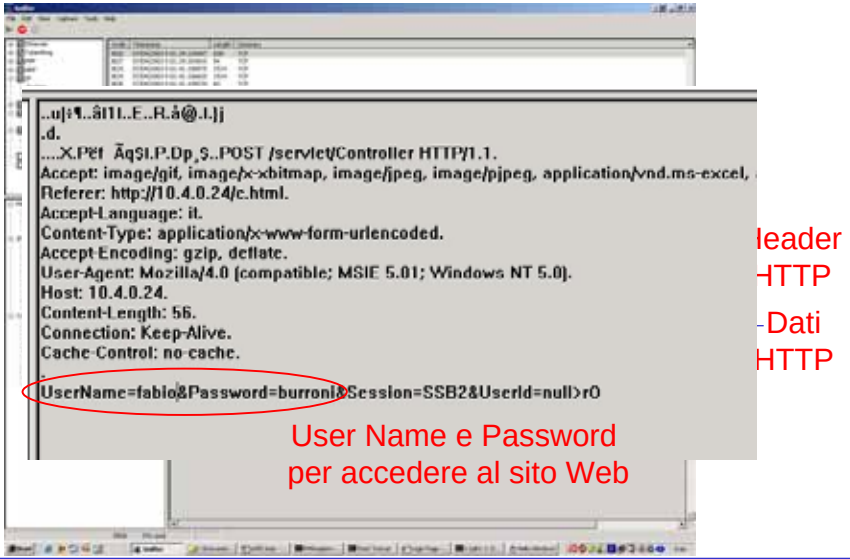
Sniffare una e-mail



Sniffare credenziali di autenticazione.



Sniffare credenziali di autenticazione.



Soluzioni

Al fine di proteggere le informazioni trasmesse su Internet è necessario implementare "**meccanismi**" di sicurezza.

Un "**meccanismo**" di sicurezza ha il compito di **rilevare**, **prevenire** o **porre rimedio** agli effetti di qualunque azione che comprometta la sicurezza delle informazioni.

Attacchi

Gli attacchi vengono normalmente suddivisi in **attivi** e **passivi**.

Attacchi **Passivi**.

Con gli attacchi **passivi** ci si limita ad "ascoltare" il traffico che attraversa una rete al fine di carpire informazioni importanti.

Sniffing: l'attaccante ascolta le comunicazioni per entrare in possesso di dati riservati quali: password, numeri di carta di credito, ecc..

Analisi del Traffico: è un attacco più sottile dello sniffing. Nel caso in cui le trasmissioni siano protette con meccanismi di cifratura, si possono ottenere ugualmente importanti informazioni come: tipologia dei messaggi trasmessi, identità degli host in comunicazione, lunghezza e frequenza di messaggi scambiati. Queste informazioni possono essere utilizzate per apportare altri tipi di attacchi.

Attacchi

Attacchi **Attivi**.

Gli attacchi attivi sono spesso i più pericolosi poiché hanno lo scopo di modificare le informazioni trasmesse o di creare un falso flusso informativo.

Masquerade. L'attaccante finge di essere qualcun altro: un utente autorizzato; quindi ottiene accesso a risorse protette.

Replay. L'attaccante intercetta passivamente i messaggi e li ritrasmette al fine di generare un effetto non autorizzato.

Modifica dei Messaggi. Alcune porzioni di un messaggio vengono modificate.

Negazione del Servizio. Si impedisce il normale utilizzo delle funzioni di comunicazione.

Servizi di sicurezza

Un **Servizio di Sicurezza** ha lo scopo di contrastare gli attacchi.

I servizi di sicurezza possono essere classificati nel seguente modo:

Servizi di sicurezza

Un **Servizio di Sicurezza** ha lo scopo di contrastare gli attacchi.

I servizi di sicurezza possono essere classificati nel seguente modo:

Riservatezza. Consiste nel proteggere i dati trasmessi da attacchi passivi. Per proteggere i dati dallo sniffing si utilizzano tecniche crittografiche.

Servizi di sicurezza

Un **Servizio di Sicurezza** ha lo scopo di contrastare gli attacchi.

I servizi di sicurezza possono essere classificati nel seguente modo:

Riservatezza. Consiste nel proteggere i dati trasmessi da attacchi passivi. Per proteggere i dati dallo sniffing si utilizzano tecniche crittografiche.

Autenticazione. Ha lo scopo di garantire l'autenticità delle informazioni. Il destinatario di un messaggio deve avere la garanzia che il messaggio è stato spedito dalla sorgente dichiarata. Un servizio di autenticazione deve poter contrastare gli attacchi di spoofing.

Servizi di sicurezza

Un **Servizio di Sicurezza** ha lo scopo di contrastare gli attacchi.

I servizi di sicurezza possono essere classificati nel seguente modo:

Riservatezza. Consiste nel proteggere i dati trasmessi da attacchi passivi. Per proteggere i dati dallo sniffing si utilizzano tecniche crittografiche.

Autenticazione. Ha lo scopo di garantire l'autenticità delle informazioni. Il destinatario di un messaggio deve avere la garanzia che il messaggio è stato spedito dalla sorgente dichiarata. Un servizio di autenticazione deve poter contrastare gli attacchi di spoofing.

Integrità. Assicura che i messaggi siano ricevuti come sono stati spediti, senza modifiche, duplicazioni e repliche.

Come sviluppare Servizi di sicurezza.

La Crittografia

Il denominatore comune della maggior parte dei servizi di sicurezza è costituito dalle tecniche crittografiche. La **cifratura** delle informazioni rappresenta lo strumento più importante per la sicurezza delle comunicazioni e dei sistemi informatici.

Le tecniche crittografiche vengono attualmente utilizzate in molti sistemi e servizi di comunicazione. Si possono cifrare pacchetti IP, dati scambiati tra applicazioni client-server, conversazioni telefoniche (GSM e UMTS), file. Si può firmare digitalmente un'applicazione (Applet Java), un documento.

Principi di Crittografia

I sistemi di cifratura si dividono in due tipologie: **Cifratura Convenzionale** (simmetrica) e **Cifratura a Chiave Pubblica** (asimmetrica).

Gli elementi per la **Cifratura Convenzionale**

Testo in chiaro: è il messaggio o il dato che deve essere cifrato. Costituisce uno degli ingressi dell'algoritmo di cifratura.

Algoritmo di cifratura: è un algoritmo che effettua trasformazioni sul testo in chiaro.

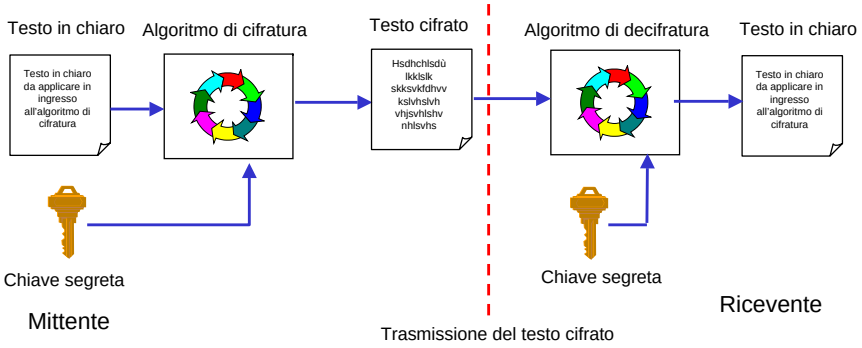
Chiave segreta: è una sequenza di byte che viene data in ingresso all'algoritmo di cifratura e dalla quale dipendono le trasformazioni apportate al testo in chiaro.

Testo cifrato: è il risultato dell'applicazione dell'algoritmo di cifratura al testo in chiaro e alla chiave.

Algoritmo di decifratura: si tratta dell'inverso dell'algoritmo di cifratura. Prende in ingresso il testo cifrato e la chiave segreta e restituisce il testo in chiaro.

Principi di Crittografia

Cifratura convenzionale



Requisiti:

L'algoritmo di cifratura deve essere "**robusto**", cioè possedendo numerosi testi cifrati ed i corrispondenti testi in chiaro non si deve essere in grado di scoprire la chiave.
Mittente e ricevente devono condividere la stessa chiave. Devono aver ottenuto la chiave in modo sicuro e mantenerla riservata.

Cifratura a chiave pubblica

La crittografia a chiave pubblica trova la sua massima applicazione per scopi di autenticazione dei messaggi e per la distribuzione delle chiavi.

La cifratura a chiave pubblica fa uso di **due** chiavi distinte: una è **Pubblica**, quindi nota a tutti, l'altra è **Privata**, nota solo al proprietario, quindi va mantenuta segreta.



Chiave Pubblica



Chiave Privata

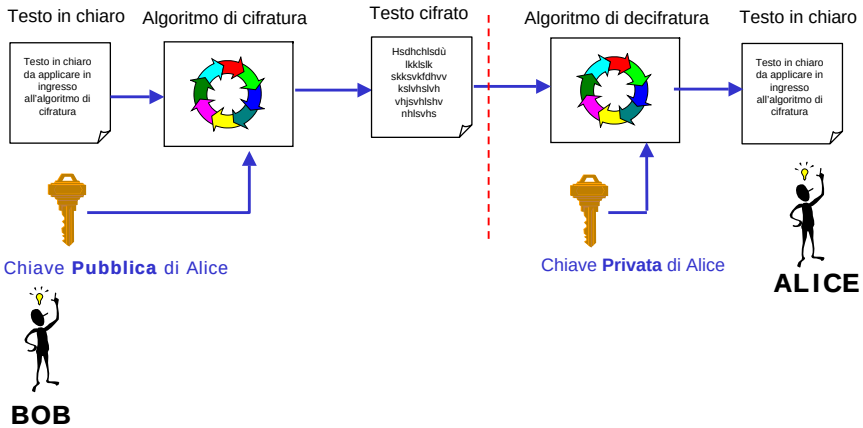
Principio: un messaggio cifrato con la chiave **Pubblica** può essere decifrato solo con la corrispondente chiave **Privata**. Un messaggio cifrato con la chiave **Privata** può essere decifrato solamente con la corrispondente chiave **Pubblica**.

Cifratura a chiave pubblica

Cifratura a chiave pubblica

BOB vuole mandare un messaggio riservato ad Alice, quindi vuole usare la cifratura.

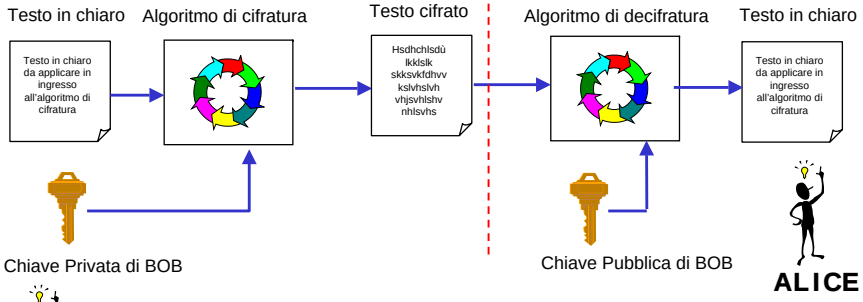
Cifratura per ottenere **Riservatezza**.



Cifratura a chiave pubblica

Bob vuole mandare un messaggio ad Alice garantendo l'autenticità della provenienza, quindi usa l'autenticazione.

Cifratura per ottenere **Autenticazione**.



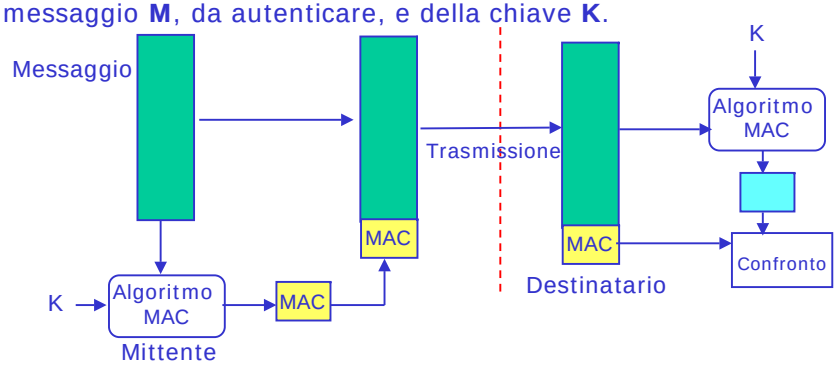
1. BOB cifra il messaggio con la propria chiave **Privata**;
2. Alice decifra il messaggio ricevuto da Bob con la chiave **Pubblica** di BOB. Alice è certa che il messaggio è stato inviato da BOB, in quanto BOB è l'unico a conoscere la propria chiave **Privata**.

Autenticazione dei messaggi

Un messaggio, un file, un documento è autentico quando non è stato alterato e proviene dalla sorgente dichiarata.

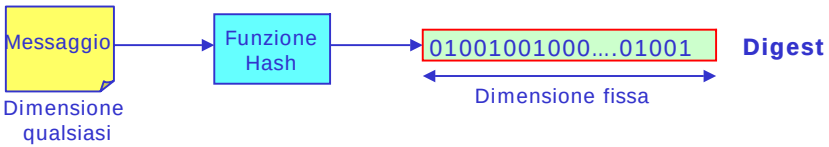
Codice di Autenticazione di Messaggio (**MAC**)

Viene generato un piccolo blocco di dati (**MAC**) e accodato al messaggio. Le parti in comunicazione devono condividere una stessa chiave **K**. Il blocco di dati è ottenuto come funzione del messaggio **M**, da autenticare, e della chiave **K**.



Funzione Hash Unidirezionale.

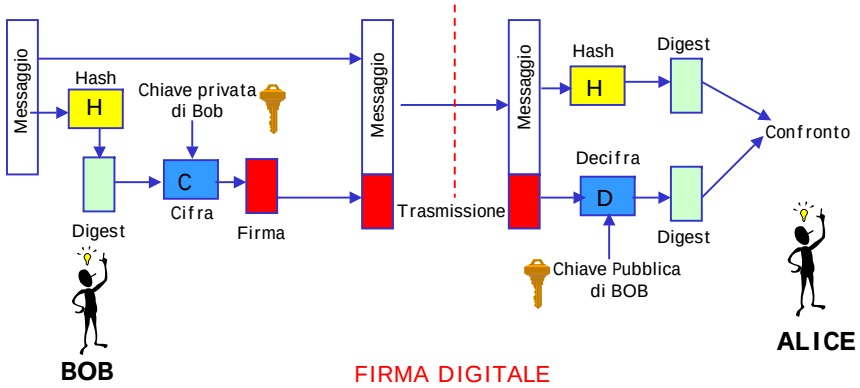
L'obiettivo di una funzione hash, H, è produrre una "impronta" del messaggio, del file, di un blocco di dati.
Le funzioni Hash non usano chiavi segrete !



Firma digitale

La cifratura a chiave pubblica insieme alle funzioni di Hash può essere utilizzata per Firmare Digitalmente un documento e quindi garantirne l'autenticità e l'integrità.
La Firma digitale non garantisce la riservatezza.

Firma digitale



FIRMA DIGITALE

La distribuzione delle chiavi

I certificati digitali

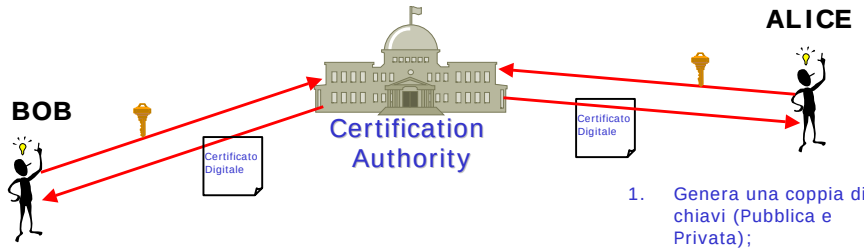
Con gli algoritmi di cifratura Asimmetrici, per la distribuzione delle chiavi, viene spesso utilizzata una terza parte fidata, denominata **Autorità di Certificazione** (*Certification Authority*). Il compito fondamentale della CA è di garantire l'appartenenza di una data chiave pubblica ad un determinato soggetto.

A tale scopo la CA è responsabile della emissione dei **Certificati Digitali**.

La presenza della CA comporta che ogni utente richieda alla CA una certificazione della Chiave Pubblica.

La distribuzione delle chiavi

I certificati digitali

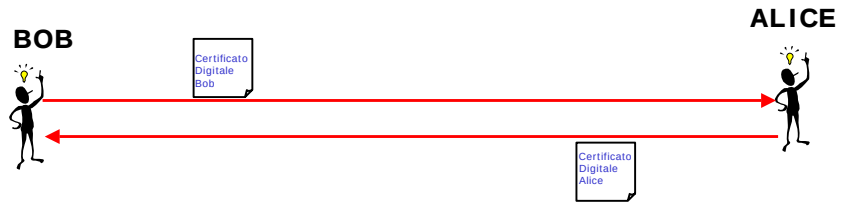


1. Genera una coppia di chiavi (Pubblica e Privata);
2. Invia la chiave pubblica alla CA;
3. Riceve il certificato digitale.

1. Genera una coppia di chiavi (Pubblica e Privata);
2. Invia la chiave pubblica alla CA;
3. Riceve il certificato digitale.

La distribuzione delle chiavi

I certificati digitali



Una volta ricevuta la certificazione Bob e Alice possono istaurare una comunicazione riservata.
Prima di effettuare la comunicazione è necessario che le due parti si scambino i certificati.

La distribuzione delle chiavi

Contenuto del Certificato Digitale

Versione: serve per distinguere le varie versioni del certificato che sono state definite nei vari anni. La prima versione è del 1988.
Numero di Serie: è un valore intero univoco per la CA che emette il certificato.
Identificatore dell'algoritmo di firma: specifica l'algoritmo di firma utilizzato per firmare il certificato.
Nome di chi emette: nome della CA che ha creato e firmato il certificato.
Periodo di validità: è costituito da due date che specificano la fascia temporale di validità del certificato.
Nome del Soggetto: indica il nome dell'utente al quale si riferisce il certificato. Il certificato "certifica" la chiave pubblica del soggetto che detiene la corrispondente chiave privata.

La distribuzione delle chiavi

Contenuto del Certificato Digitale

Informazioni sulla chiave pubblica: contiene la chiave pubblica del soggetto è l'identificatore dell'algoritmo con cui tale chiave può essere utilizzata.
Identificatore unico di chi emette il certificato: stringa di bit che permette di identificare in modo univoco la CA. Questo è un campo opzionale.
Identificatore del soggetto: campo opzionale. E' una stringa di bit che rappresenta univocamente il soggetto.
Estensioni: Le estensioni fanno parte dello standard X.509 versione 3. Contengono parametri aggiuntivi.
Firma: viene calcolata su tutti i campi del certificato. E' costituita dal codice hash degli altri campi, cifrato con la chiave privata della CA. Inoltre contiene anche l'identificatore dell'algoritmo di firma utilizzato.

Applicazione della Crittografia

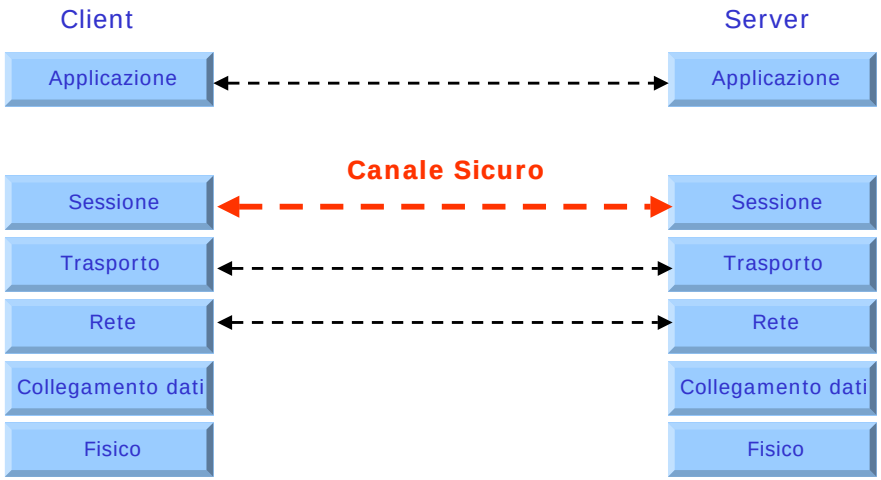
Lo standard più diffuso per la protezione dei Servizi offerti tramite internet è Secure Socket Layer (SSL).

SSL offre i seguenti servizi di sicurezza:

- Autenticazione delle parti in comunicazione;
- Integrità dei dati;
- Riservatezza delle Comunicazioni.

Secure Socket Layer

SSL offre un "Canale Sicuro" a livello di Sessione.



Secure Socket Layer



Tutti i dati trasmessi dal Client al Server, e viceversa vengono “cifrati” usando un algoritmo Simmetrico.

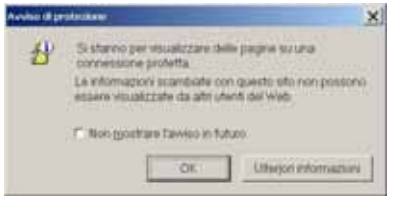
L’autenticazione delle parti in comunicazione avviene tramite l’utilizzo dei certificati digitali.

L’integrità dei dati è garantita con l’utilizzo di Codici di Autenticazione di messaggio (MAC).

Secure Socket Layer

Utilizzo di SSL

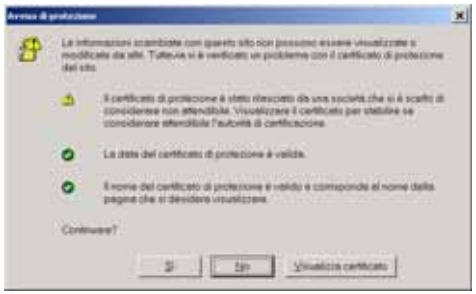
Quando un client, Browser Web, tenta di accedere ad una risorsa protetta con SSL viene visualizzato il seguente messaggio.



Questo messaggio è generato dal Browser WEB.

Secure Socket Layer

Utilizzo di SSL



Il Browser Web, ricevuto il certificato dal Server, permette all’utente di visualizzarlo.

Utilizzo di SSL

Certificato digitale del Server



Secure Socket Layer

Installazione Certificati



Secure Socket Layer

Installazione Certificati

Viene attivata la procedura guidata per l'installazione dei certificati.



Fabio Burroni

Dipartimento di Ingegneria dell'Informazione

Università degli Studi di Siena

burronif@unisi.it