


Fabio Burroni

Università degli Studi di Siena

**burronif@unisi.it**

Sistemi e Tecnologie di Rete

# 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

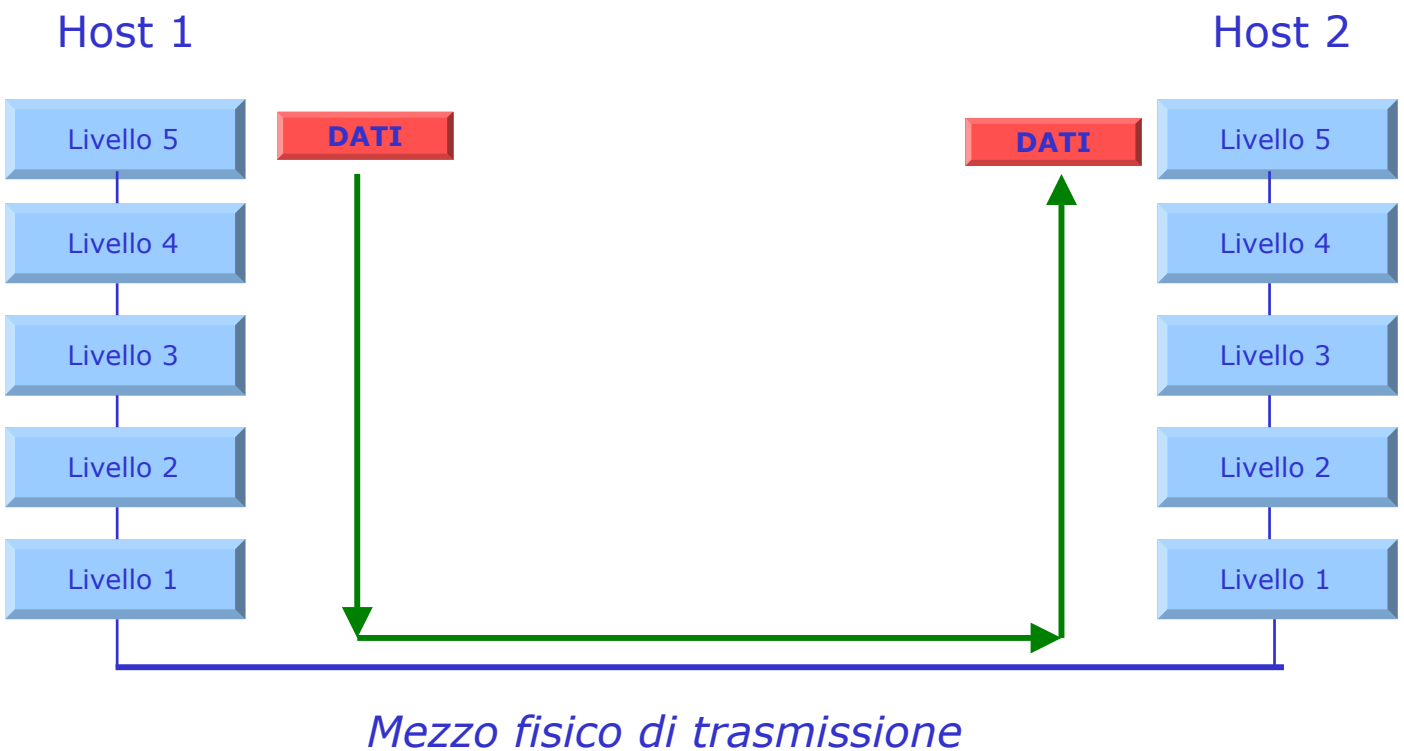
Esempio Architettura a 5 livelli



# Il software delle reti

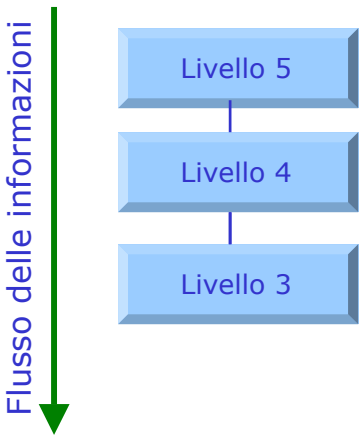
Supponiamo che l'Host 1 deve mandare dei dati all'Host 2.

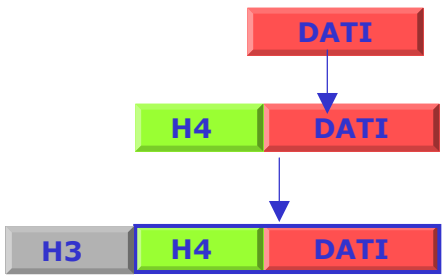
I dati fisicamente fluiscono dal livello più alto a quelli inferiori, fino al livello più basso, che li trasmette nel mezzo fisico di trasmissione. Raggiunto l'host destinatario i dati risalgono tutti i livelli fino a quello più alto.



# 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.

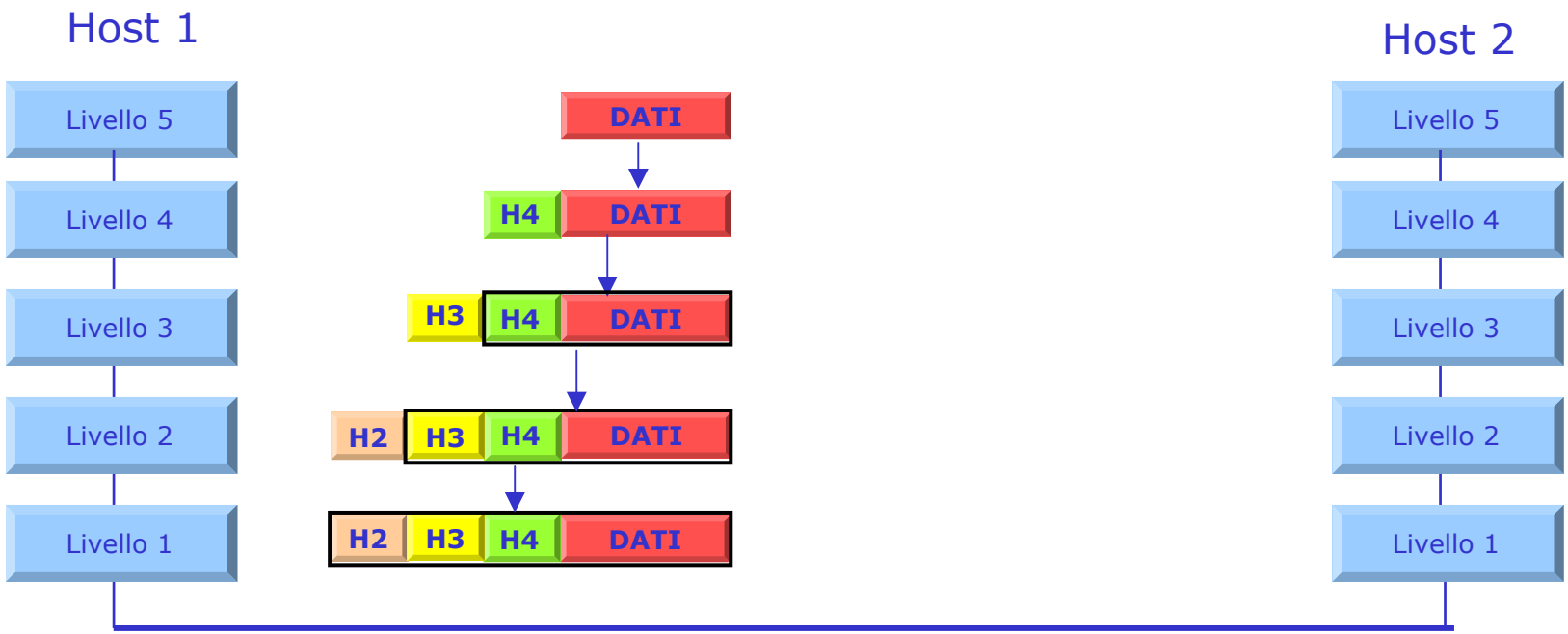
E così via….

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

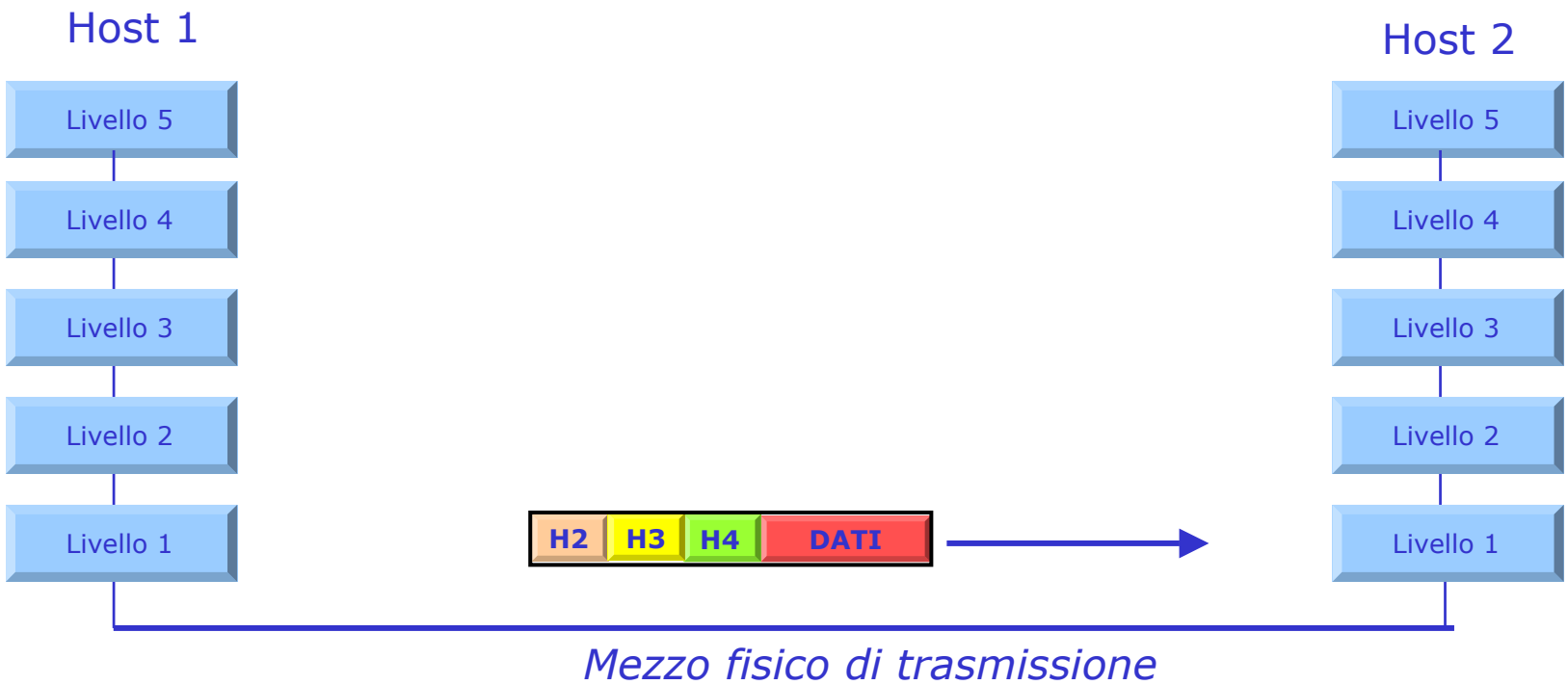



Questo meccanismo si chiama "**incapsulamento**".

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

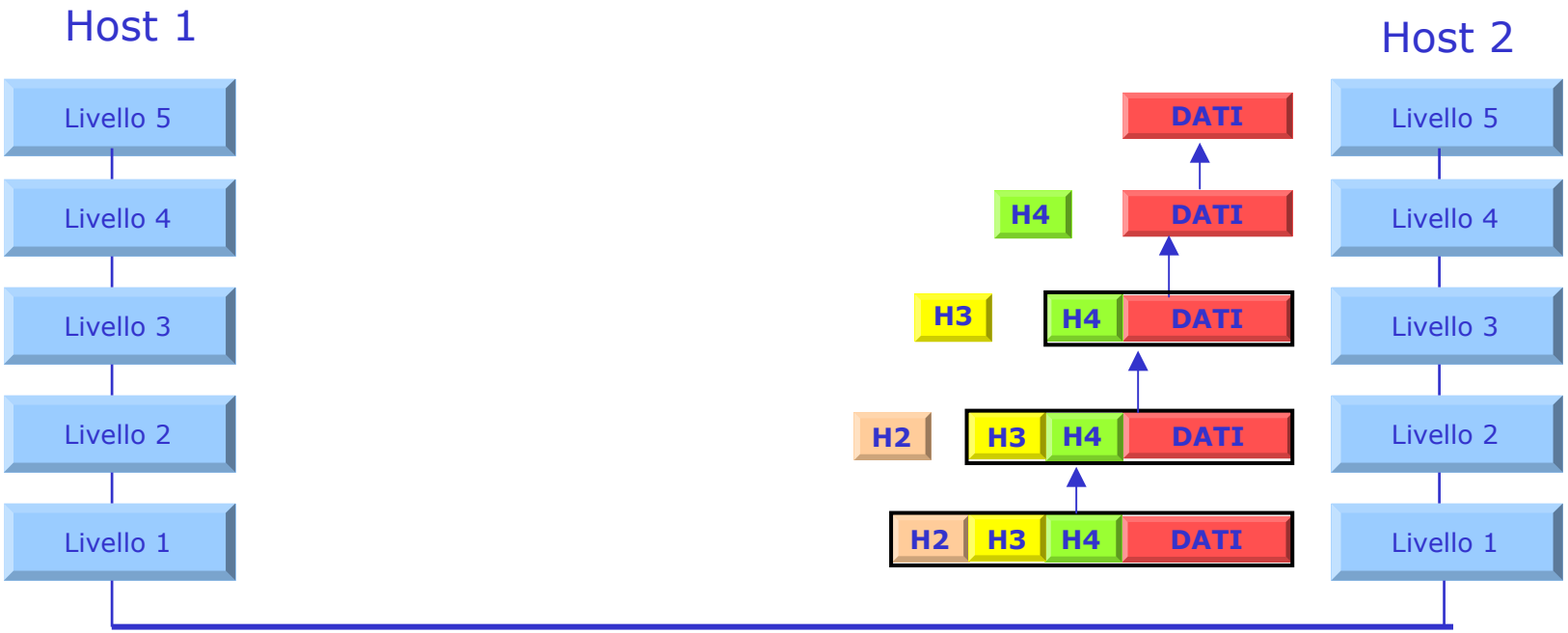
## Trasmissione




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

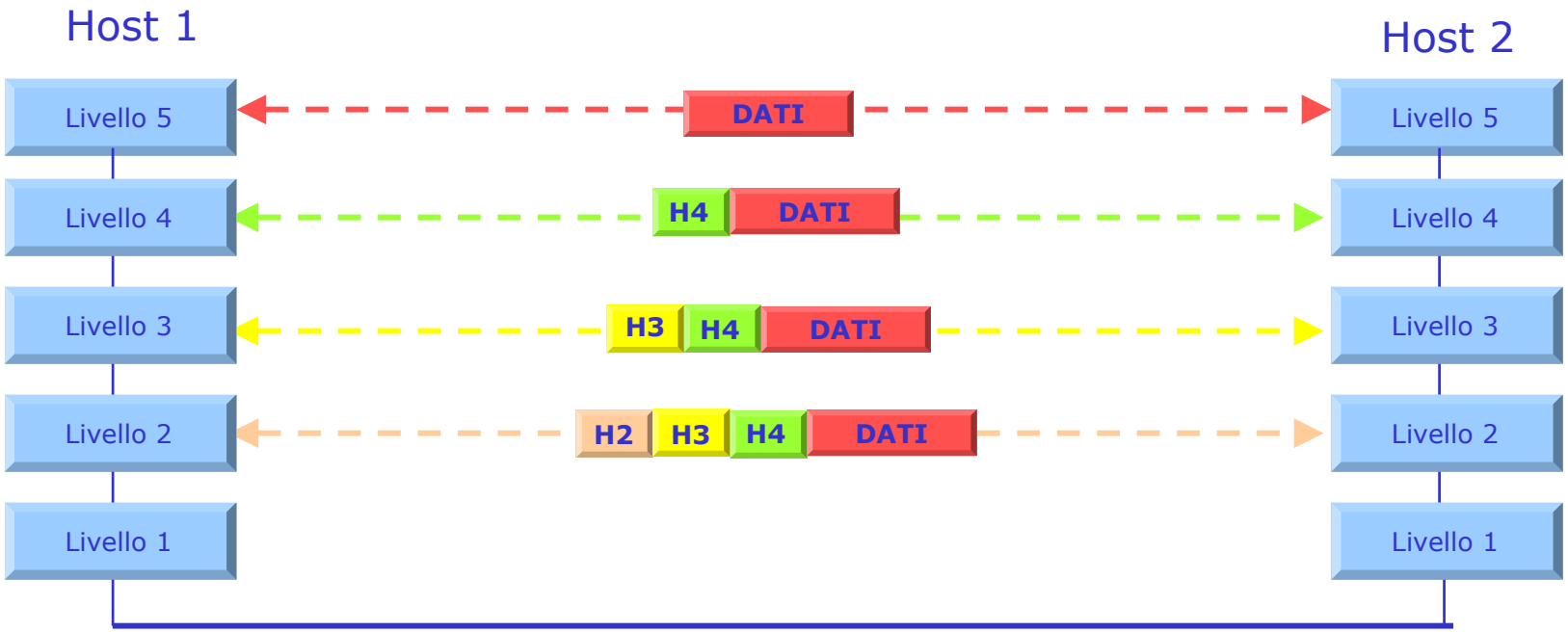
# Il software delle reti

## 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.

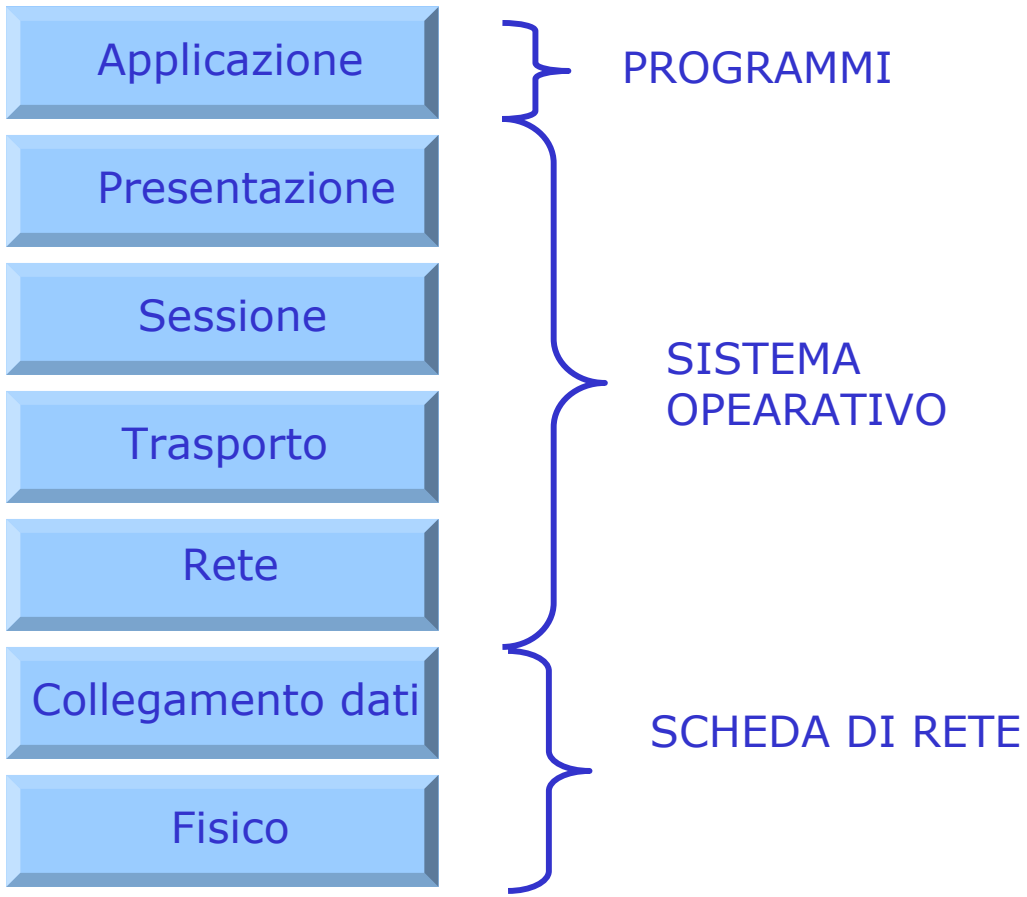
# Il software delle reti




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**".

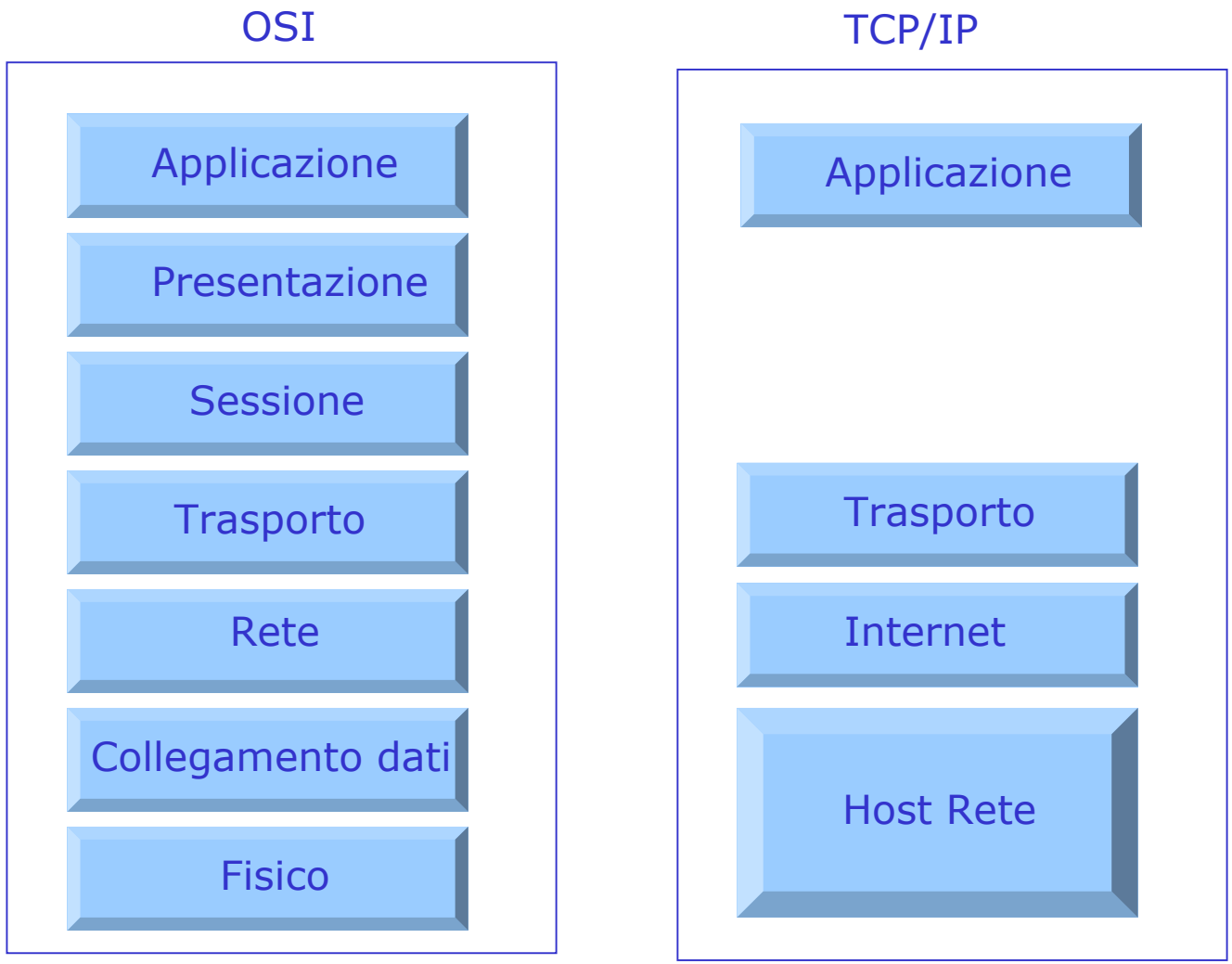
# Il software delle reti

## Il Modello OSI



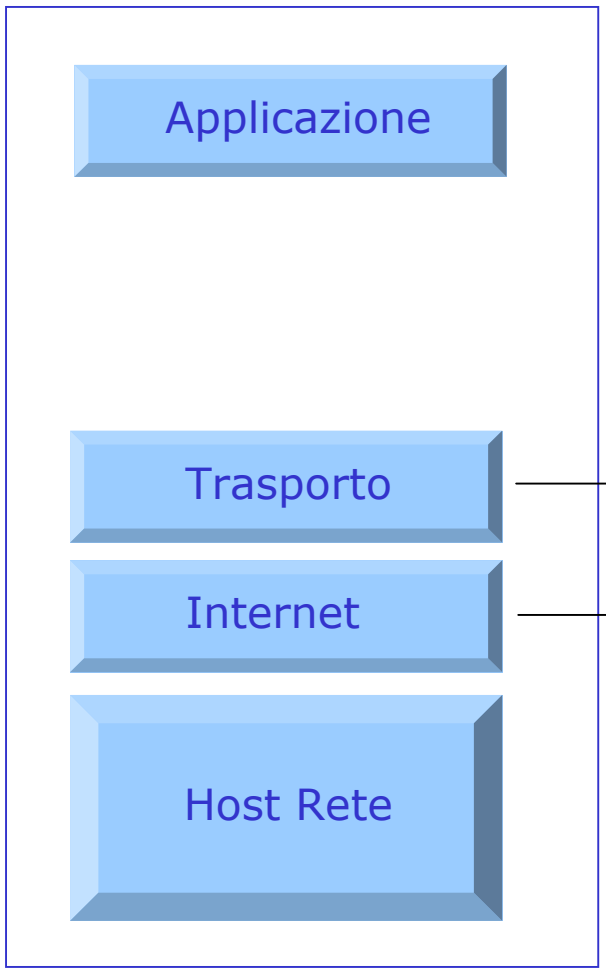
# Il software delle reti

## Il TCP/IP



# Il software delle reti

## Gli indirizzi



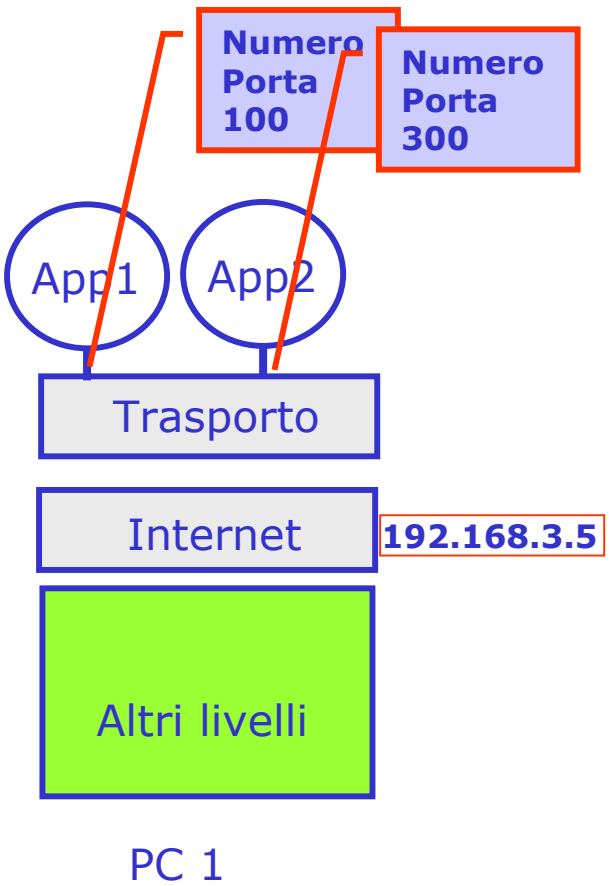

<u>Regole generali</u>: ogni host possiede un indirizzo univoco, ogni applicazione di un host possiede un numero di porta univoco.

Trasporto → Definizione del numero di porta, es **80**.

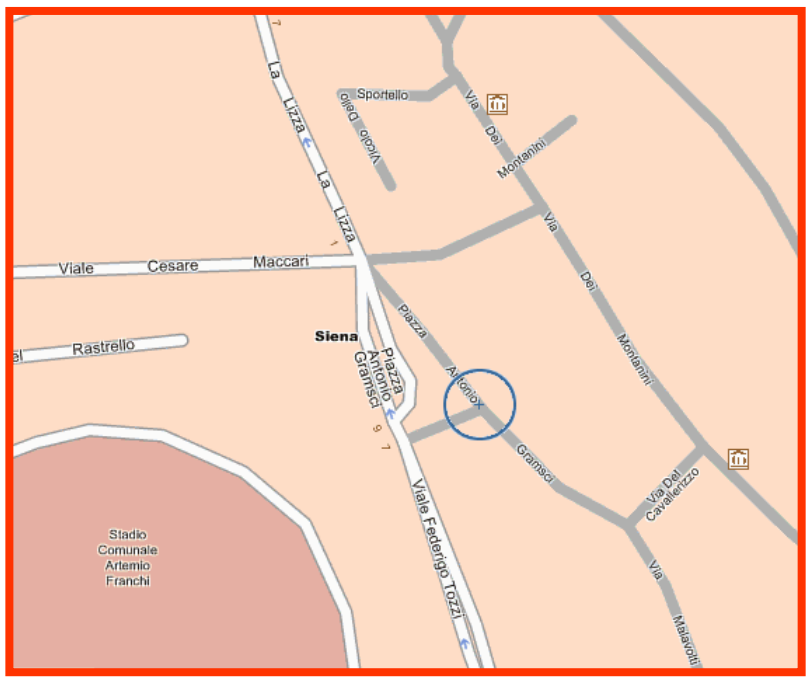
Internet → Definizione di un indirizzo univoco, detto indirizzo IP es. **192.168.3.5**

# Il software delle reti

## Gli indirizzi



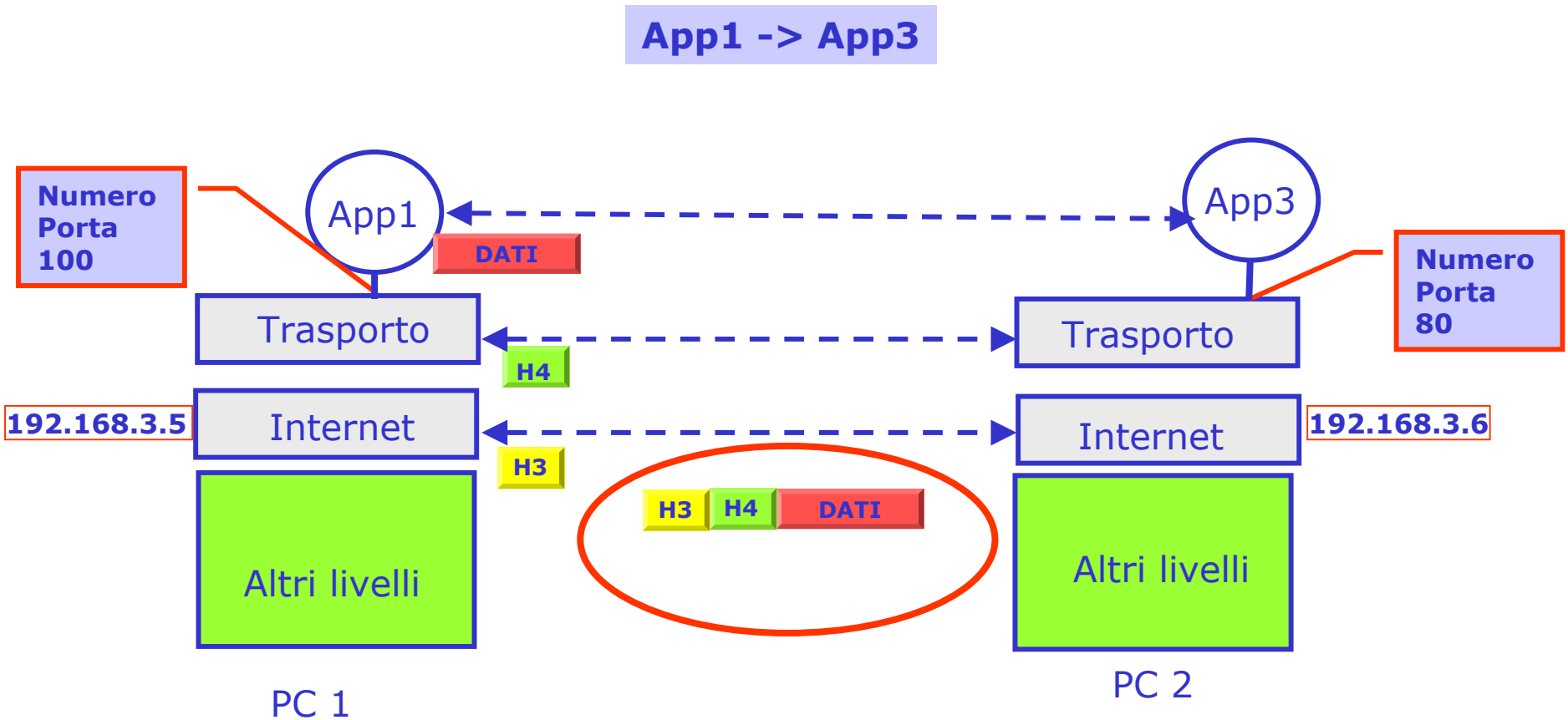

L'indirizzo IP è la via, la porta è il numero civico.



# Il software delle reti

## Il TCP/IP

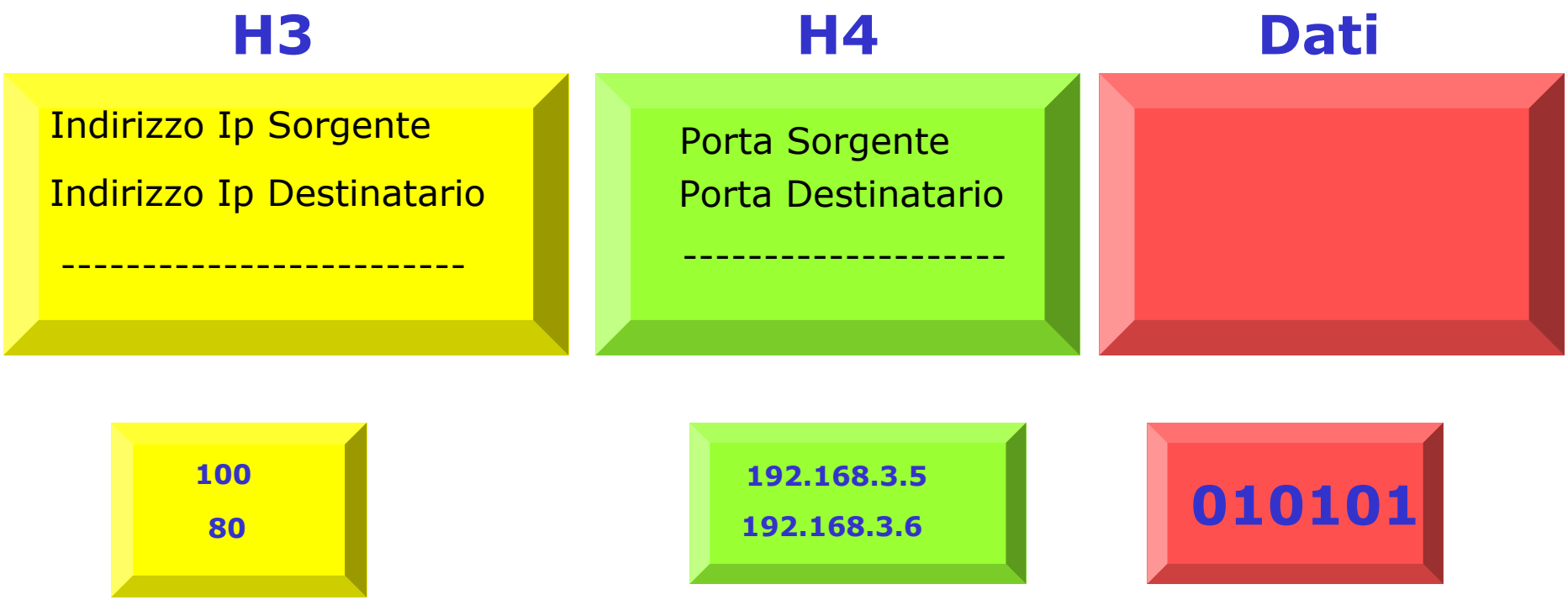
### La comunicazione tra due **applicazioni**



# Il software delle reti

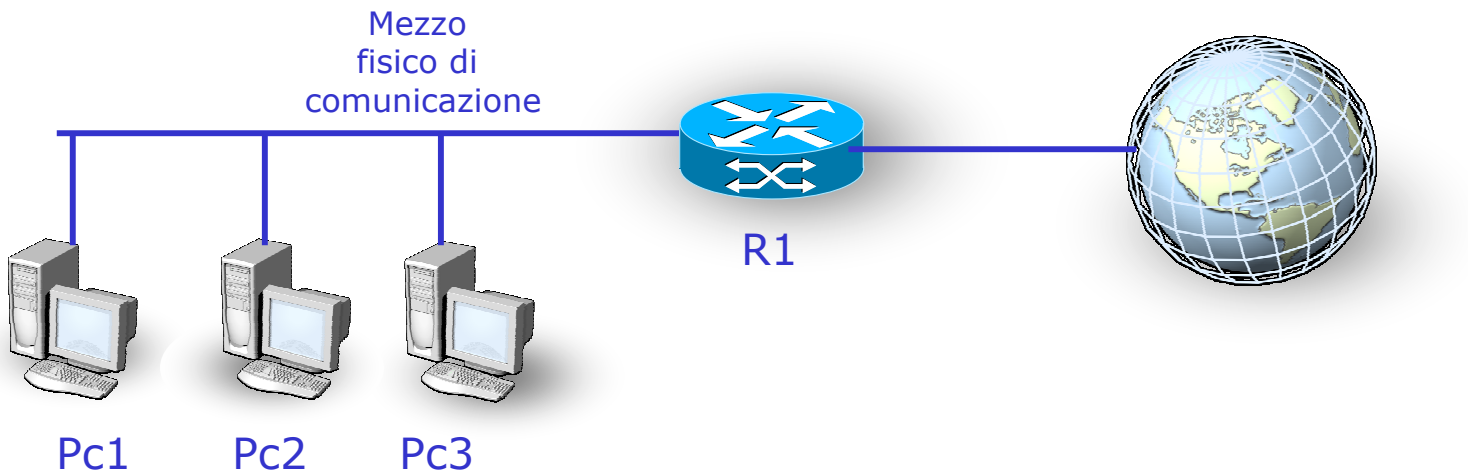
## Il TCP/IP

La comunicazione tra due **applicazioni**



# Debolezze delle reti locali.

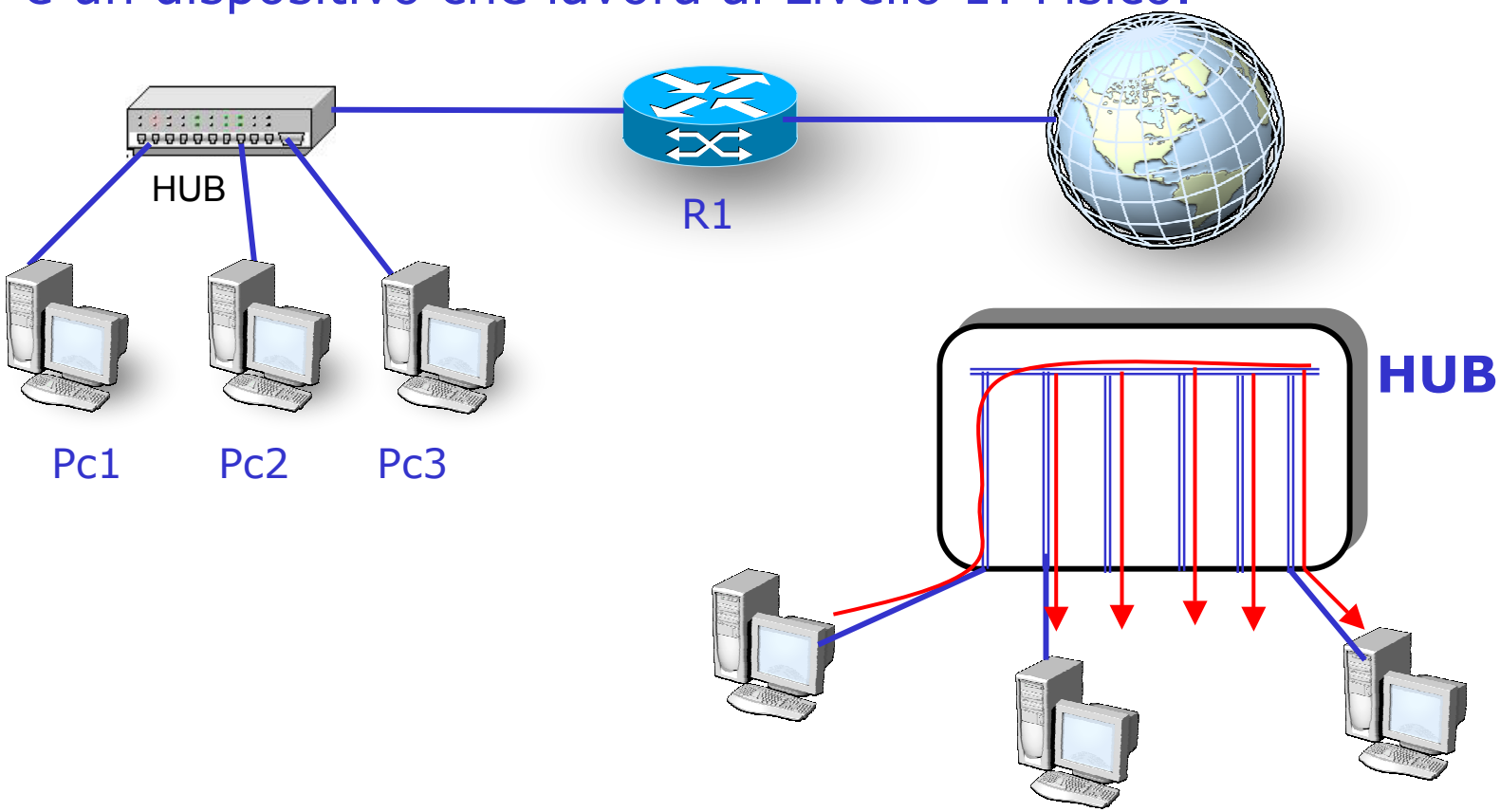
Le reti locali sono fondamentalmente reti Broadcast e questo costituisce un punto debole dal punto di vista della sicurezza. Vediamo un esempio:
Consideriamo la seguente rete Lan Ethernet:




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

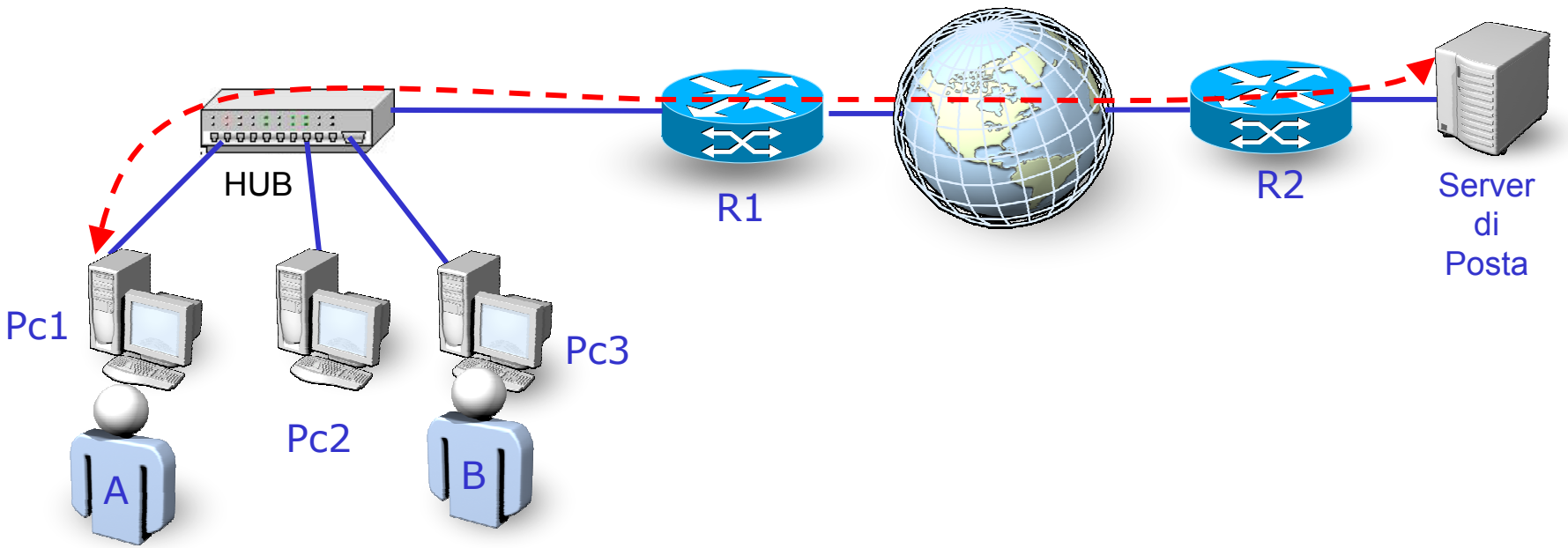
# Debolezze delle reti locali.

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**.



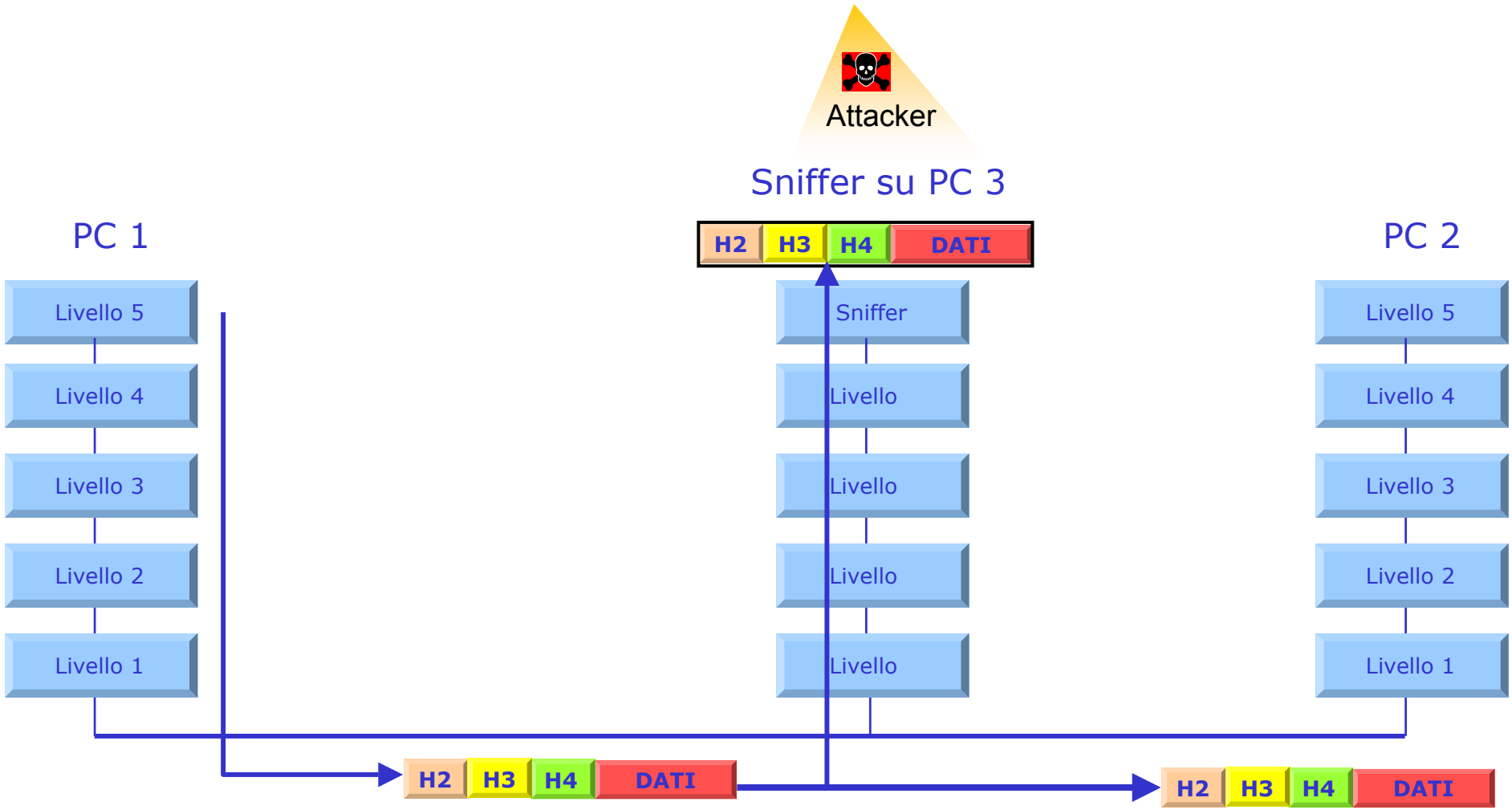
# Debolezze delle reti locali.

## Cosa è un “packet sniffer” ?

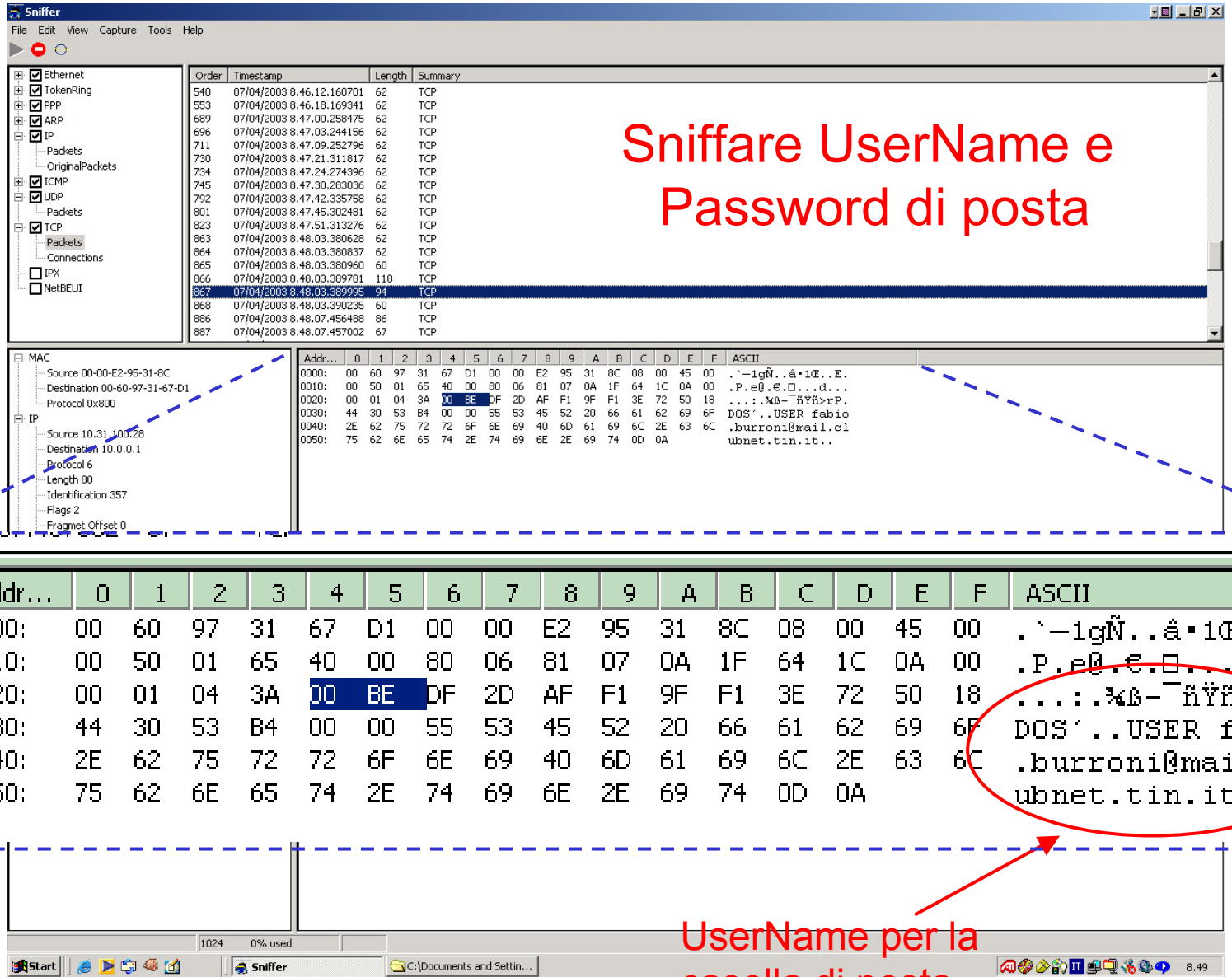
Un packet sniffer è un programma in grado di analizzare tutti i pacchetti che circolano su una rete locale.

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” ?

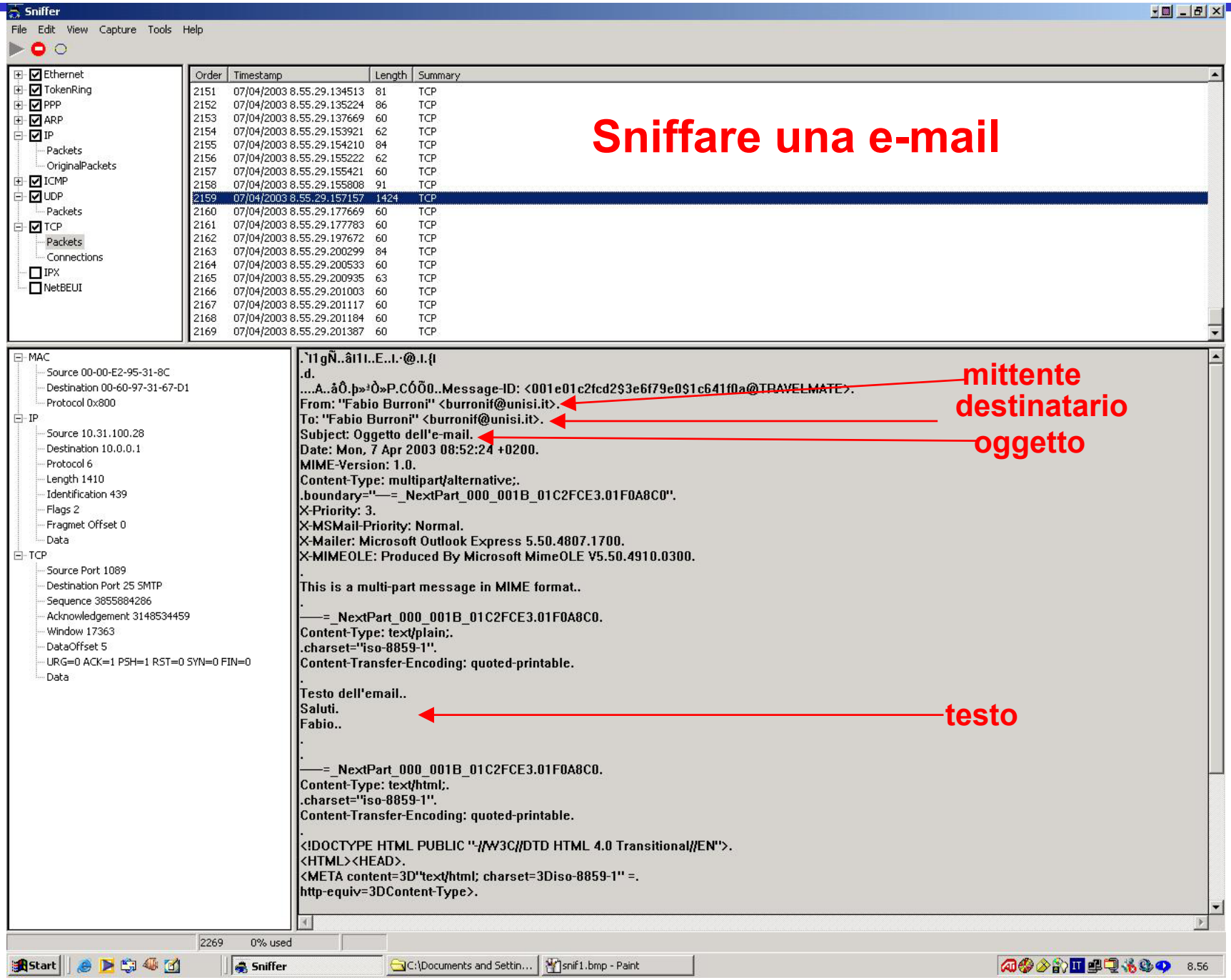


# Sniffer in azione sull'Host PC3

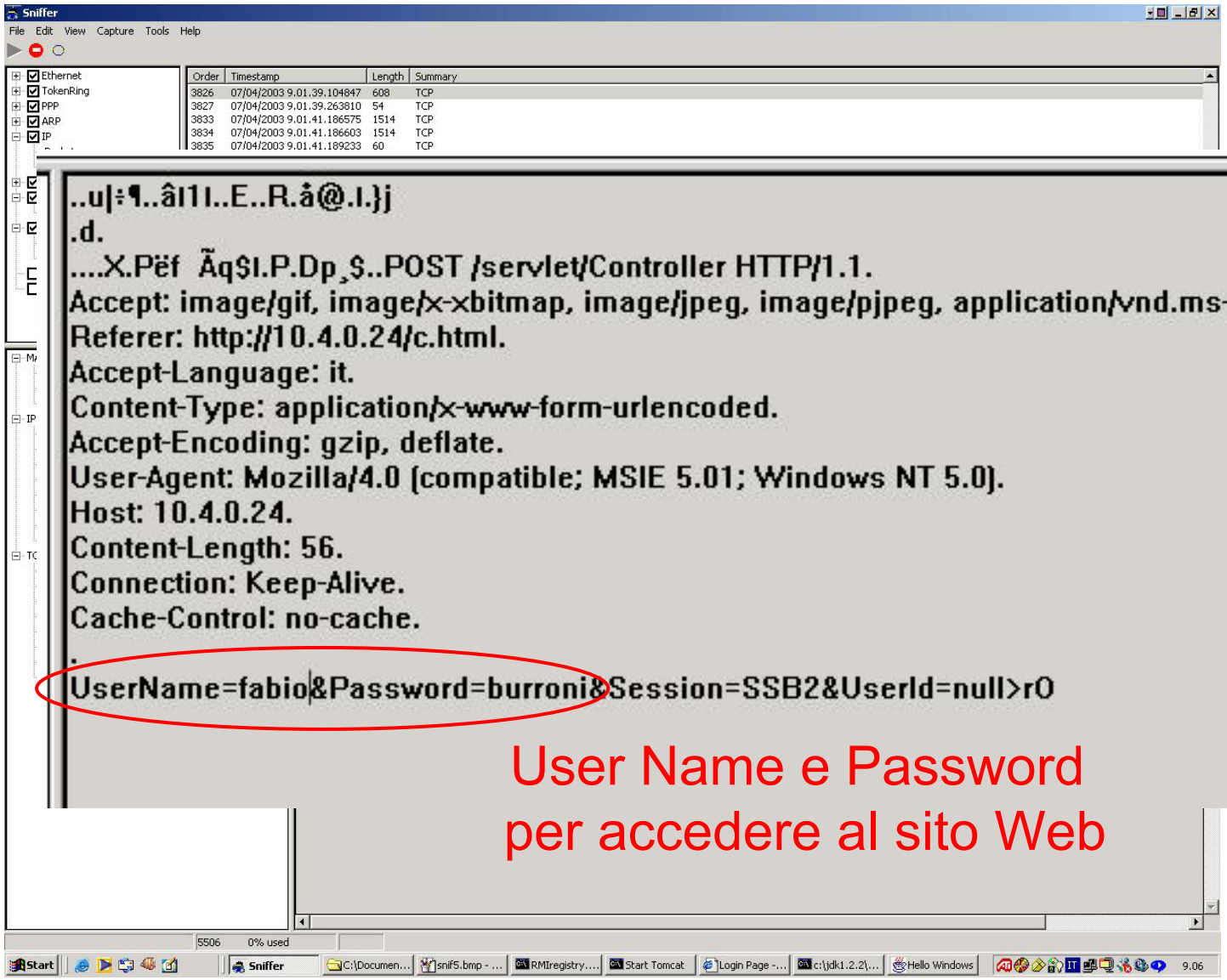



Sniffare UserName e Password di posta

UserName per la casella di posta elettronica.


Sniffer
File Edit View Capture Tools Help
Ethernet
TokenRing
PPP
ARP
IP
Packets
OriginalPackets
ICMP
UDP
Packets
TCP
Packets
Connections
IPX
NetBEUI
Order Timestamp Length Summary
2151 07/04/2003 8.55.29.134513 81 TCP
2152 07/04/2003 8.55.29.135224 86 TCP
2153 07/04/2003 8.55.29.137669 60 TCP
2154 07/04/2003 8.55.29.153921 62 TCP
2155 07/04/2003 8.55.29.154210 84 TCP
2156 07/04/2003 8.55.29.155222 62 TCP
2157 07/04/2003 8.55.29.155421 60 TCP
2158 07/04/2003 8.55.29.155808 91 TCP
2159 07/04/2003 8.55.29.157157 1424 TCP
2160 07/04/2003 8.55.29.177669 60 TCP
2161 07/04/2003 8.55.29.177783 60 TCP
2162 07/04/2003 8.55.29.197672 60 TCP
2163 07/04/2003 8.55.29.200299 84 TCP
2164 07/04/2003 8.55.29.200533 60 TCP
2165 07/04/2003 8.55.29.200935 63 TCP
2166 07/04/2003 8.55.29.201003 60 TCP
2167 07/04/2003 8.55.29.201117 60 TCP
2168 07/04/2003 8.55.29.201184 60 TCP
2169 07/04/2003 8.55.29.201387 60 TCP
Sniffare una e-mail
MAC
Source 00-00-E2-95-31-8C
Destination 00-60-97-31-67-D1
Protocol 0x800
IP
Source 10.31.100.28
Destination 10.0.0.1
Protocol 6
Length 1410
Identification 439
Flags 2
Fragmet Offset 0
Data
TCP
Source Port 1089
Destination Port 25 SMTP
Sequence 3855884286
Acknowledgement 3148534459
Window 17363
DataOffset 5
URG=0 ACK=1 PSH=1 RST=0 SYN=0 FIN=0
Data
.`ì1gÑ..âÌ1ì..E..ì.·@.ì.{ì
.d.
....A..åÔ.þ»³Ò»P.CÓÕ0..Message-ID: <001e01c2fcd2$3e6f79e0$1c641f0a@TRAVELMATE>.
From: "Fabio Burroni" <burronif@unisi.it>.
To: "Fabio Burroni" <burronif@unisi.it>.
Subject: Oggetto dell'e-mail.
Date: Mon, 7 Apr 2003 08:52:24 +0200.
MIME-Version: 1.0.
Content-Type: multipart/alternative;.
.boundary="—=_NextPart_000_001B_01C2FCE3.01F0A8C0".
X-Priority: 3.
X-MSMail-Priority: Normal.
X-Mailer: Microsoft Outlook Express 5.50.4807.1700.
X-MIMEOLE: Produced By Microsoft MimeOLE V5.50.4910.0300.
.
This is a multi-part message in MIME format..
.
——=_NextPart_000_001B_01C2FCE3.01F0A8C0.
Content-Type: text/plain;.
.charset="iso-8859-1".
Content-Transfer-Encoding: quoted-printable.
.
Testo dell'email..
Saluti.
Fabio..
.
.
——=_NextPart_000_001B_01C2FCE3.01F0A8C0.
Content-Type: text/html;.
.charset="iso-8859-1".
Content-Transfer-Encoding: quoted-printable.
.
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">.
<HTML><HEAD>.
<META content=3D"text/html; charset=3Diso-8859-1" =.
http-equiv=3DContent-Type>.
mittente
destinatario
oggetto
testo
2269 0% used
Start
Sniffer
C:\Documents and Settin...
snif1.bmp - Paint
8.56

# Sniffare credenziali di autenticazione.




leader
HTTP

-Dati
HTTP

User Name e Password
per accedere al sito Web

# 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:

**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.

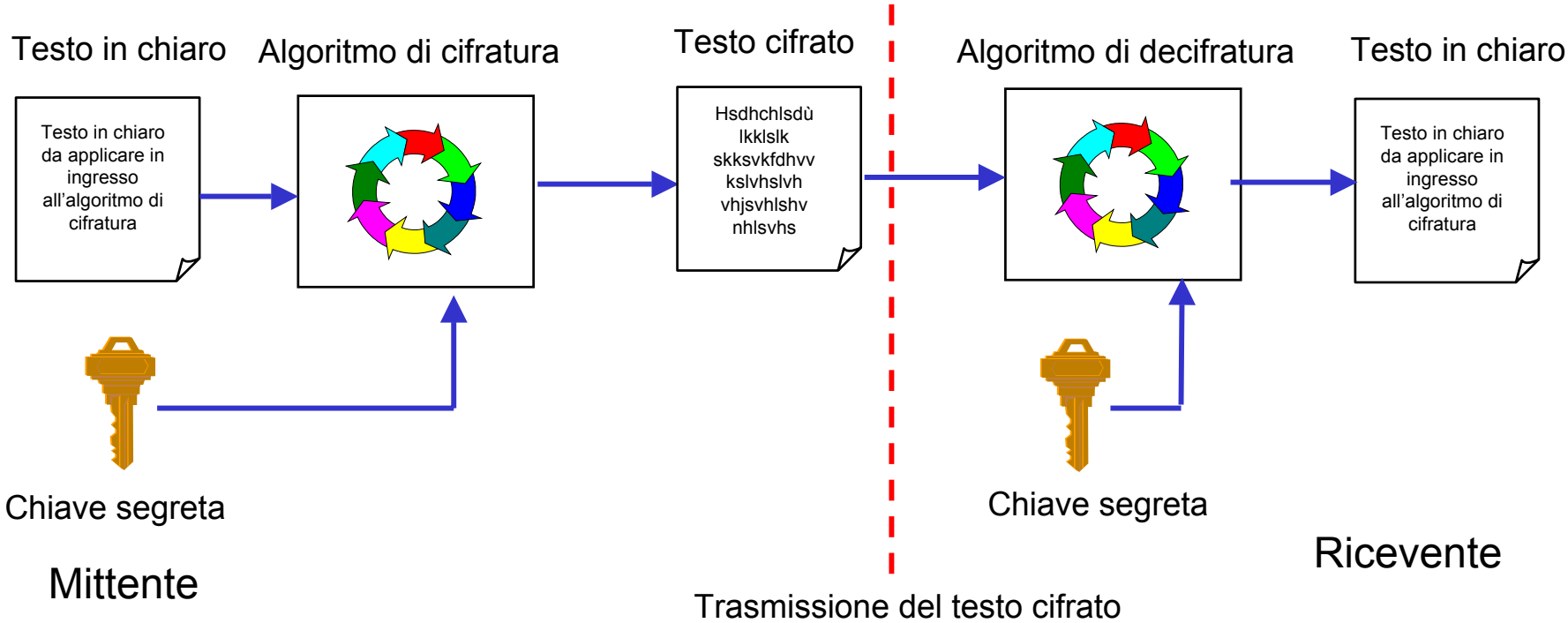
**Chiave segreta**: è una sequenza di byte che viene data in ingresso all'algoritmo di cifratura e dalla quale dipendono le trasformazioni apportate al testo in chiaro.

**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

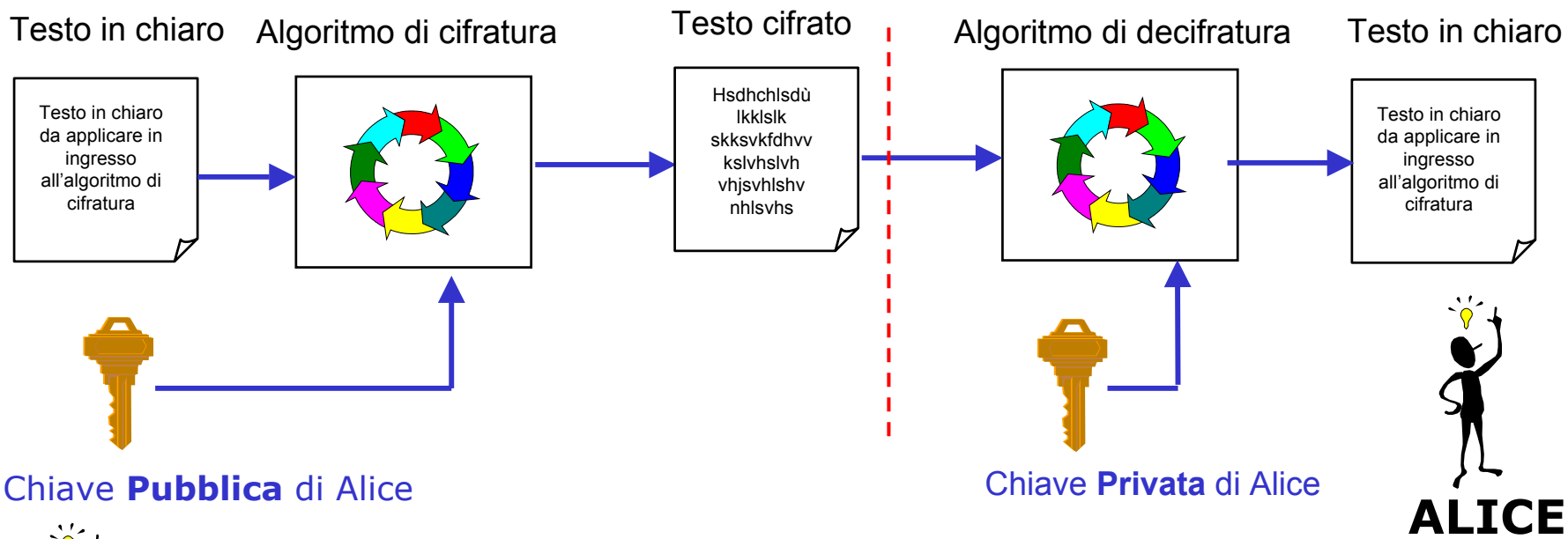
**Principio**: un messaggio cifrato con la chiave **Pubblica** può essere decifrato solo con la corrispondente chiave **Privata**. Un messaggio cifrato con la chiave **Privata** può essere decifrato solamente con la corrispondente chiave **Pubblica**.

# Cifratura a chiave pubblica

## Cifratura a chiave pubblica

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

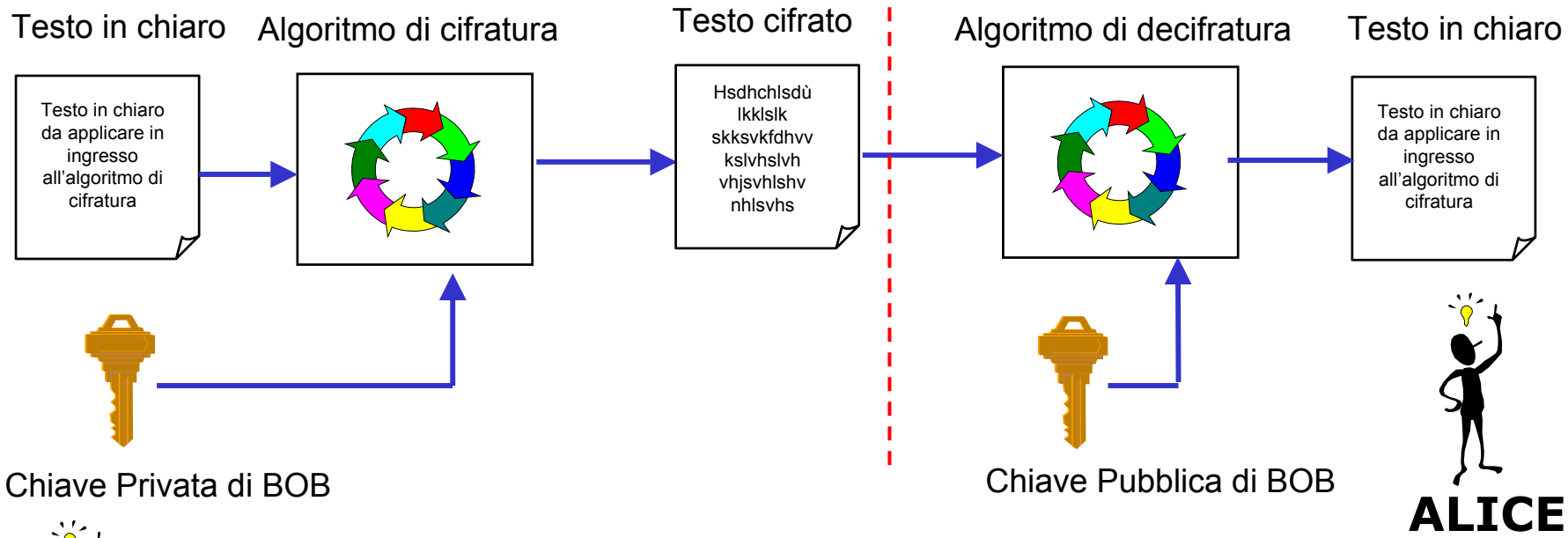
Cifratura per ottenere **Riservatezza**.



# Cifratura a chiave pubblica

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

## Cifratura per ottenere **Autenticazione**.



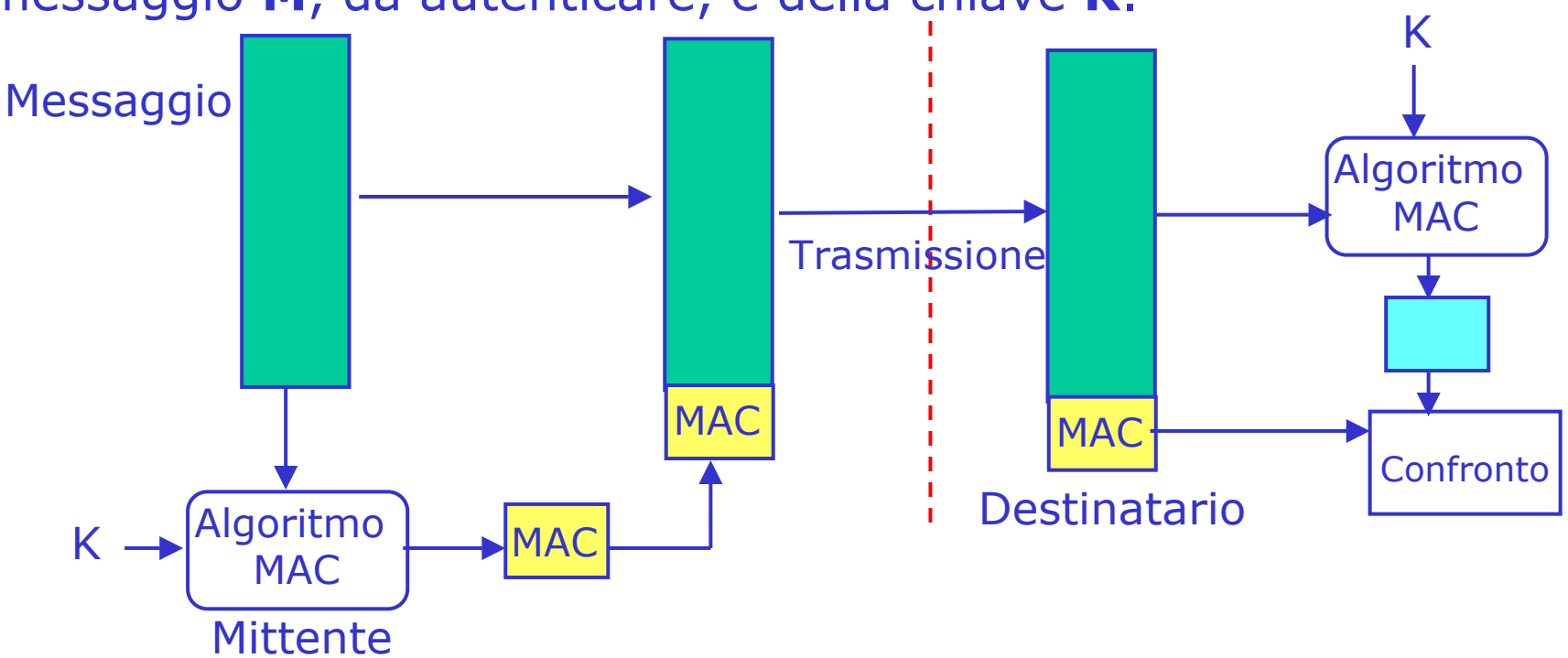

1. BOB cifra il messaggio con la propria chiave **Privata**;
2. Alice decifra il messaggio ricevuto da Bob con la chiave **Pubblica** di BOB. Alice è certa che il messaggio è stato inviato da BOB, in quanto BOB è l'unico a conoscere la propria chiave **Privata**.

# Autenticazione dei messaggi

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

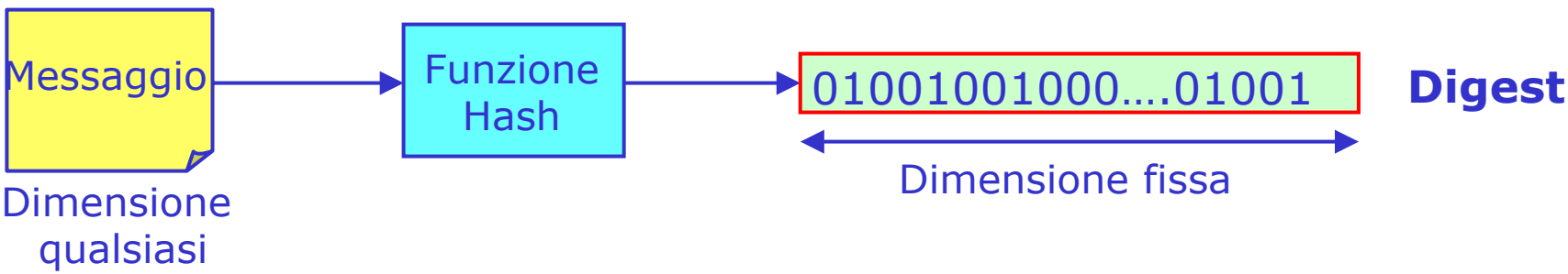
## Codice di Autenticazione di Messaggio (**MAC**)

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.

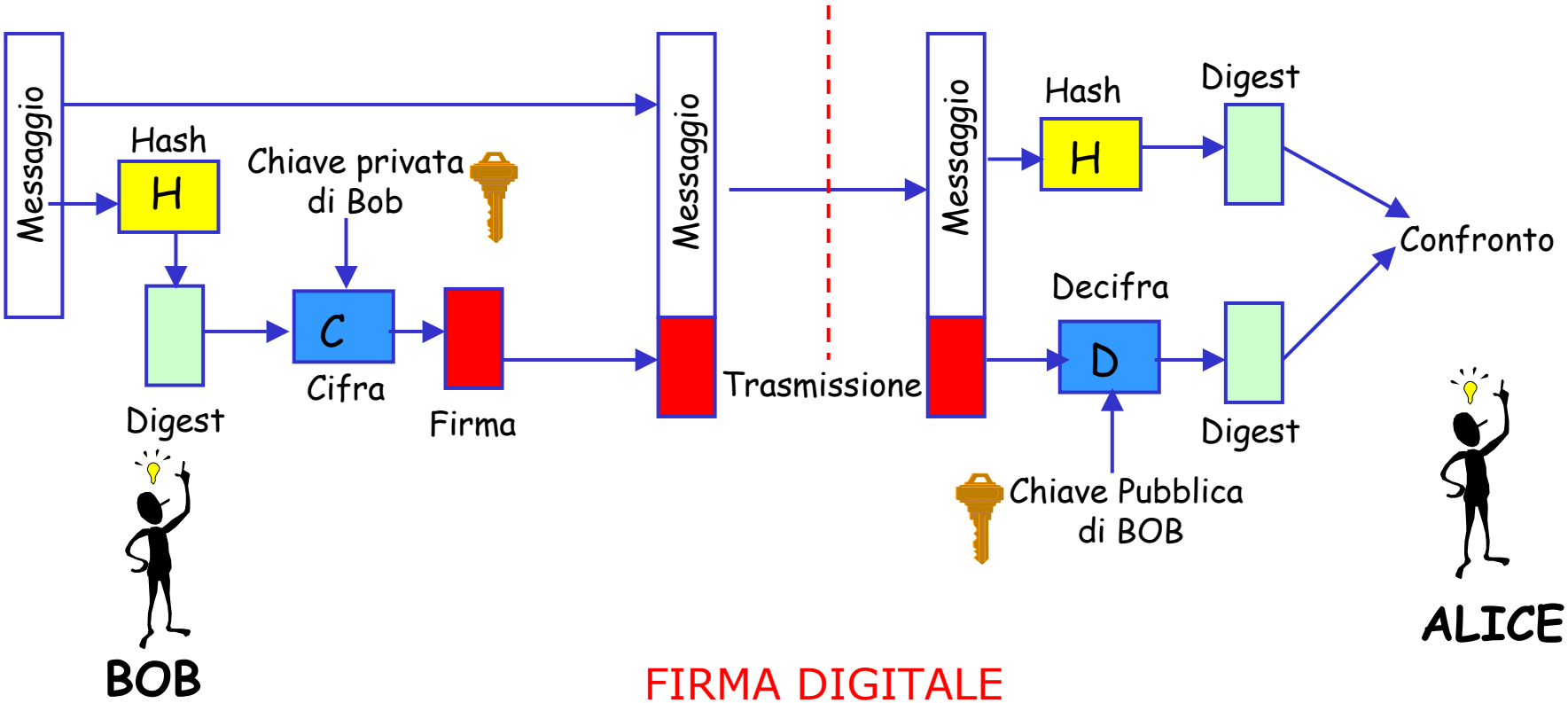
L'obiettivo di una funzione hash, H, è produrre una "impronta" del messaggio, del file, di un blocco di dati.
Le funzioni Hash non usano chiavi segrete !



# 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

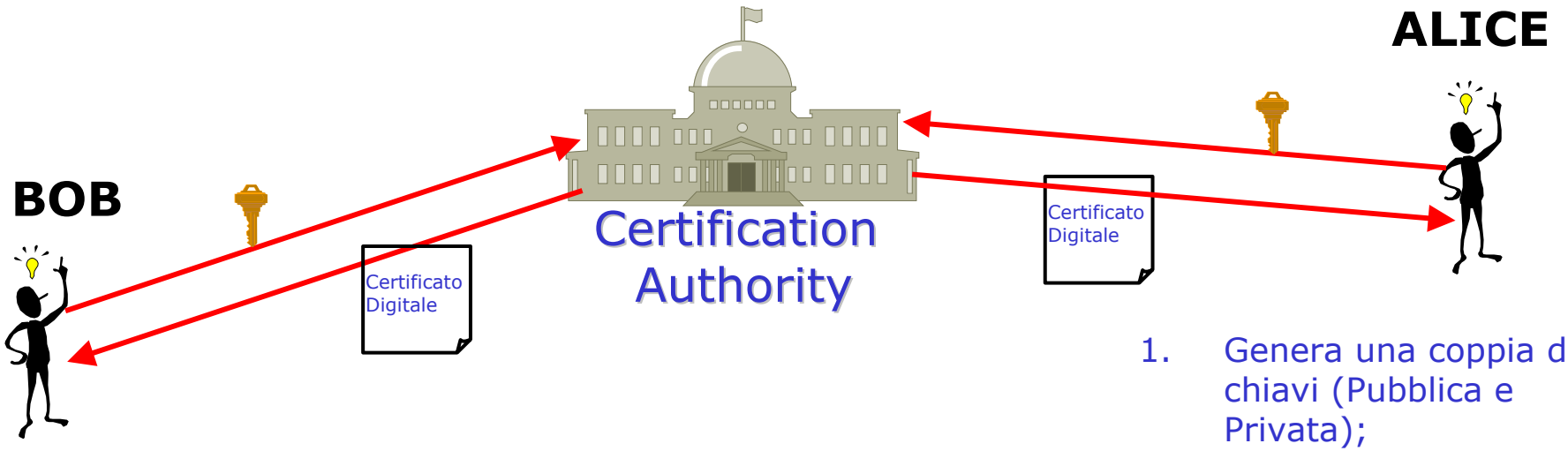
Con gli algoritmi di cifratura Asimmetrici, per la distribuzione delle chiavi, viene spesso utilizzata una terza parte fidata, denominata **Autorità di Certificazione** (*Certification Authority*). Il compito fondamentale della CA è di garantire l'appartenenza di una data chiave pubblica ad un determinato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

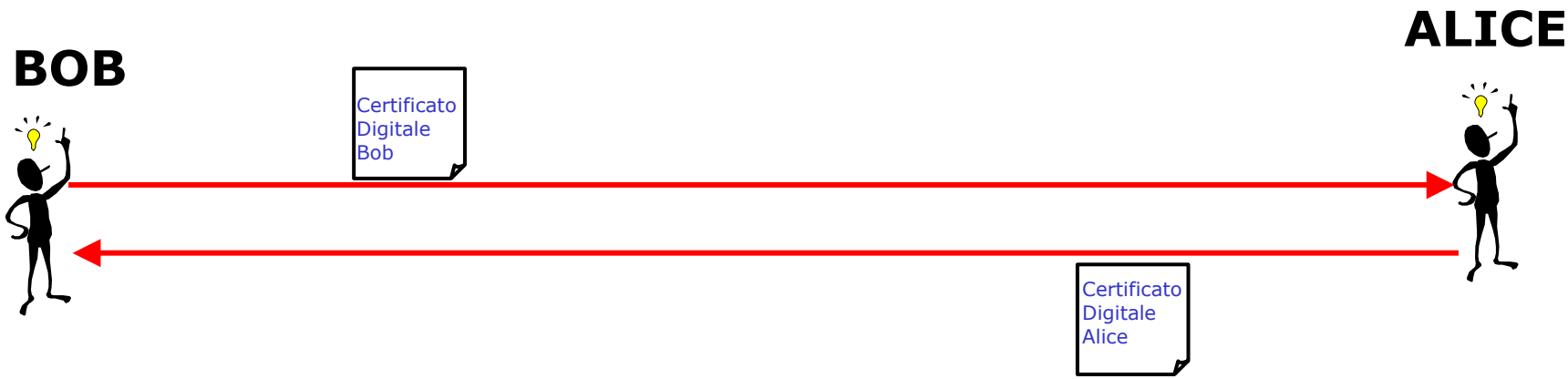



1. Genera una coppia di chiavi (Pubblica e Privata);
2. Invia la chiave pubblica alla CA;
3. Riceve il certificato digitale.

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

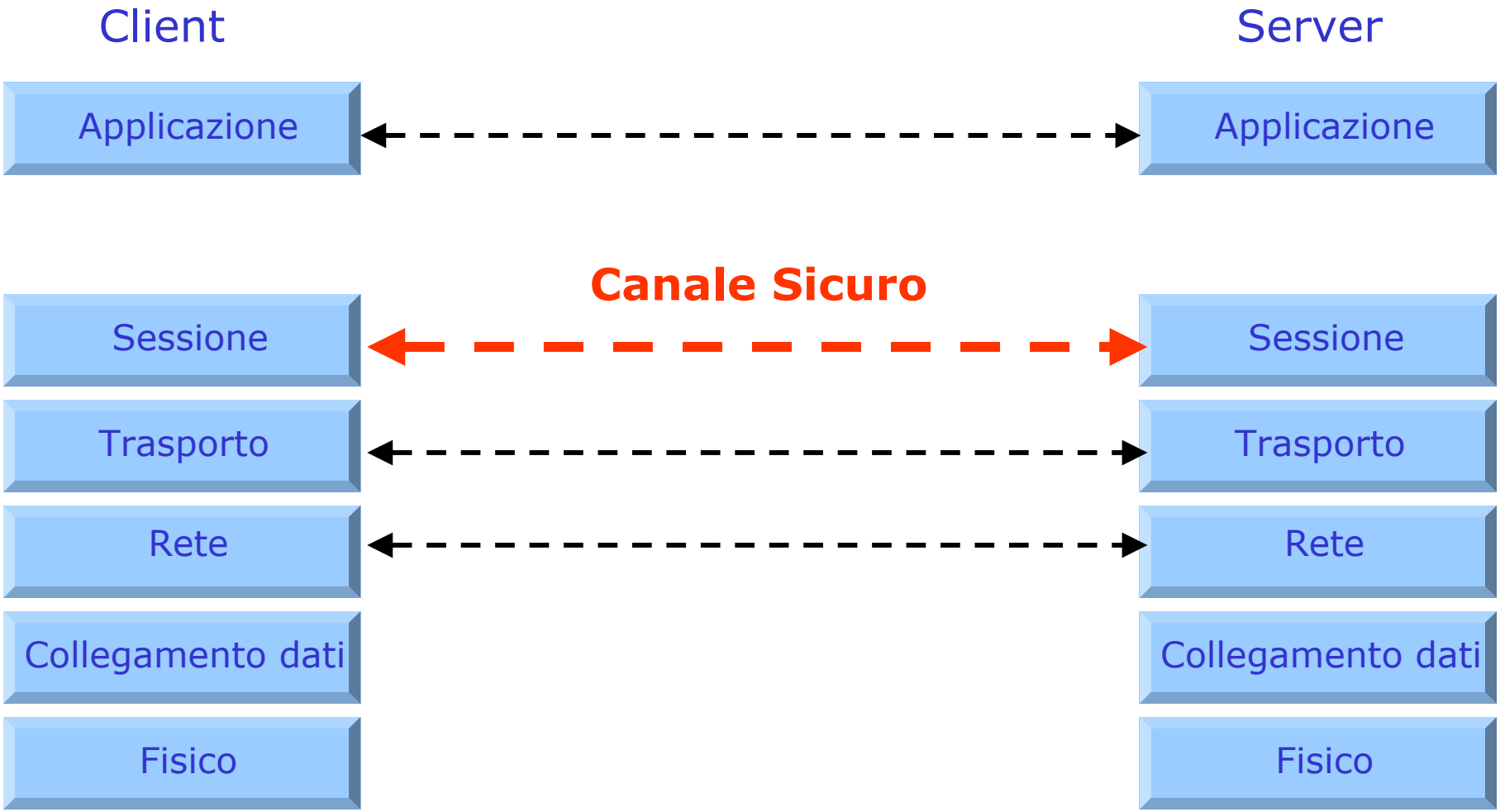
Lo standard più diffuso per la protezione dei Servizi offerti tramite internet è Secure Socket Layer (**SSL**).

SSL offre i seguenti servizi di sicurezza:

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

# Secure Socket Layer (SSL)

SSL offre un “Canale Sicuro” a livello di Sessione.



# Secure Socket Layer (SSL)



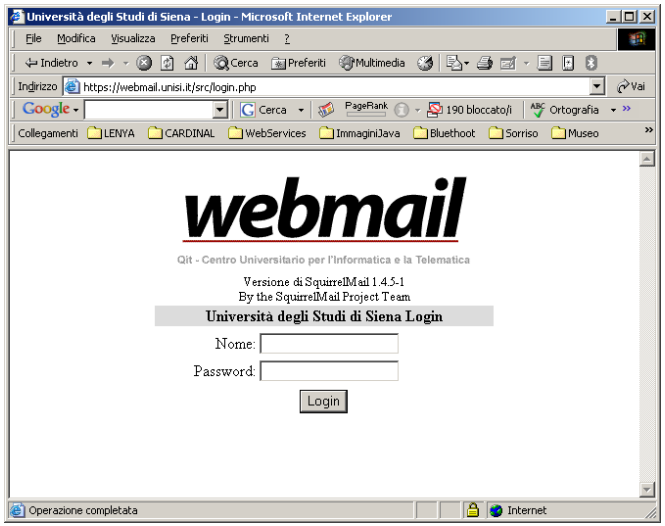

Tutti i dati trasmessi dal Client al Server, e viceversa vengono “cifrati” usando un algoritmo Simmetrico.

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

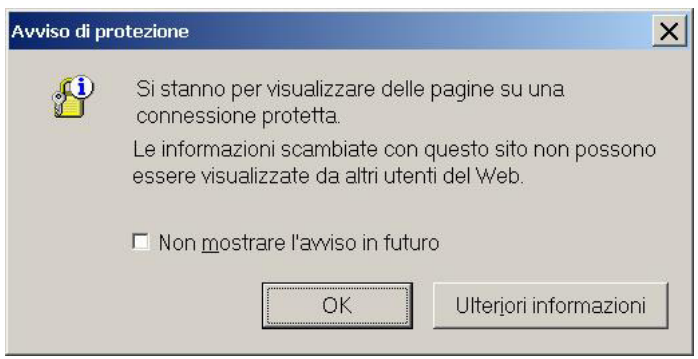
L’integrità dei dati è garantita con l’utilizzo di Codici di Autenticazione di messaggio (MAC).

# Secure Socket Layer
## Utilizzo di SSL

Gli indirizzi dei siti protetti con **ssl** iniziano per **https://**

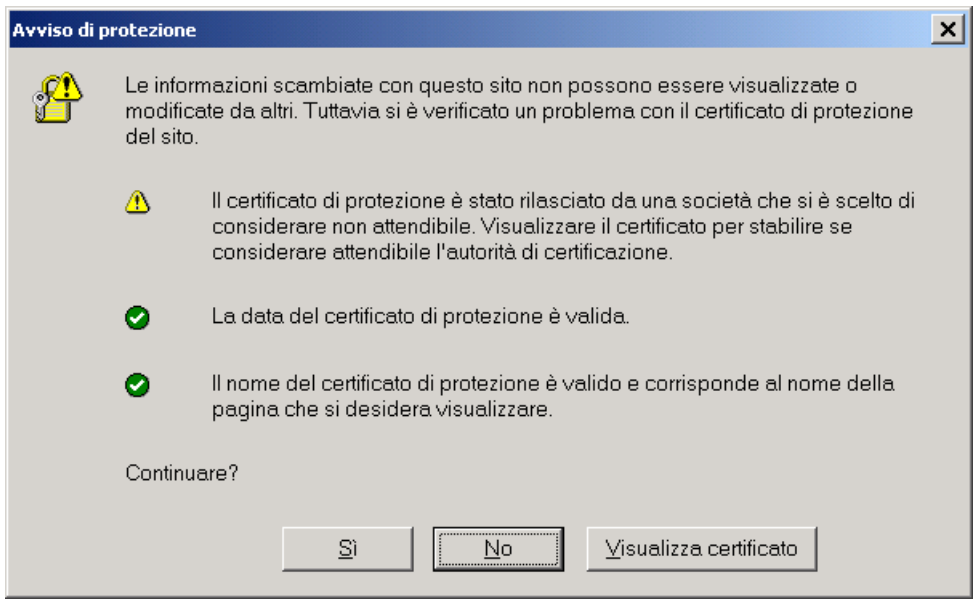



Quando un client, Browser Web, tenta di accedere ad una risorsa protetta con SSL viene visualizzato il seguente messaggio.



# Secure Socket Layer

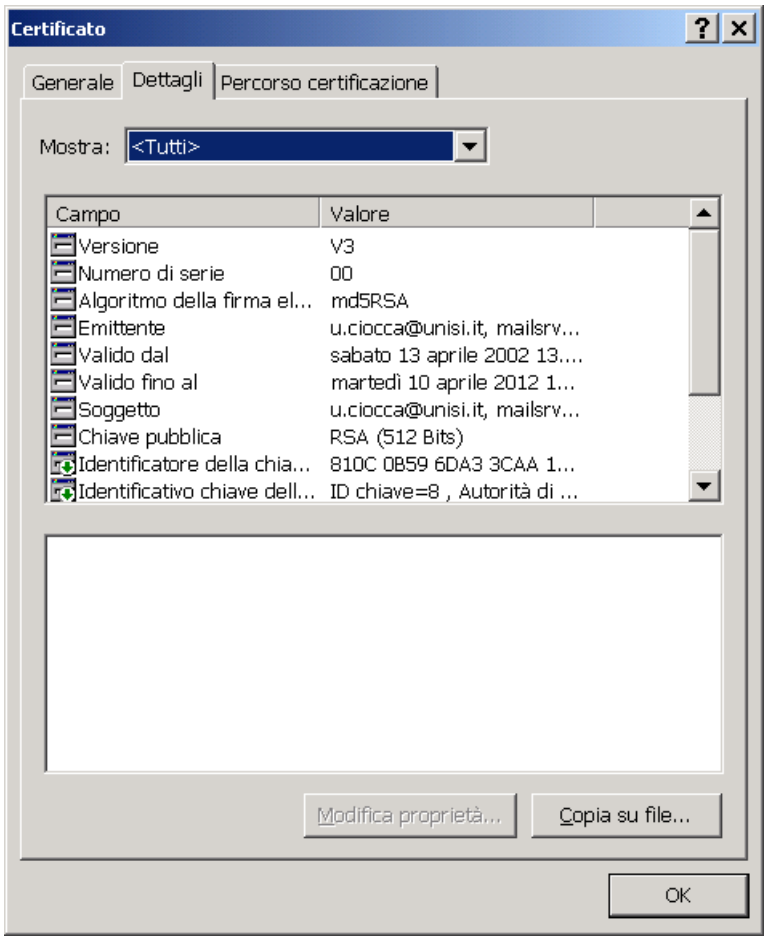
## Utilizzo di SSL




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

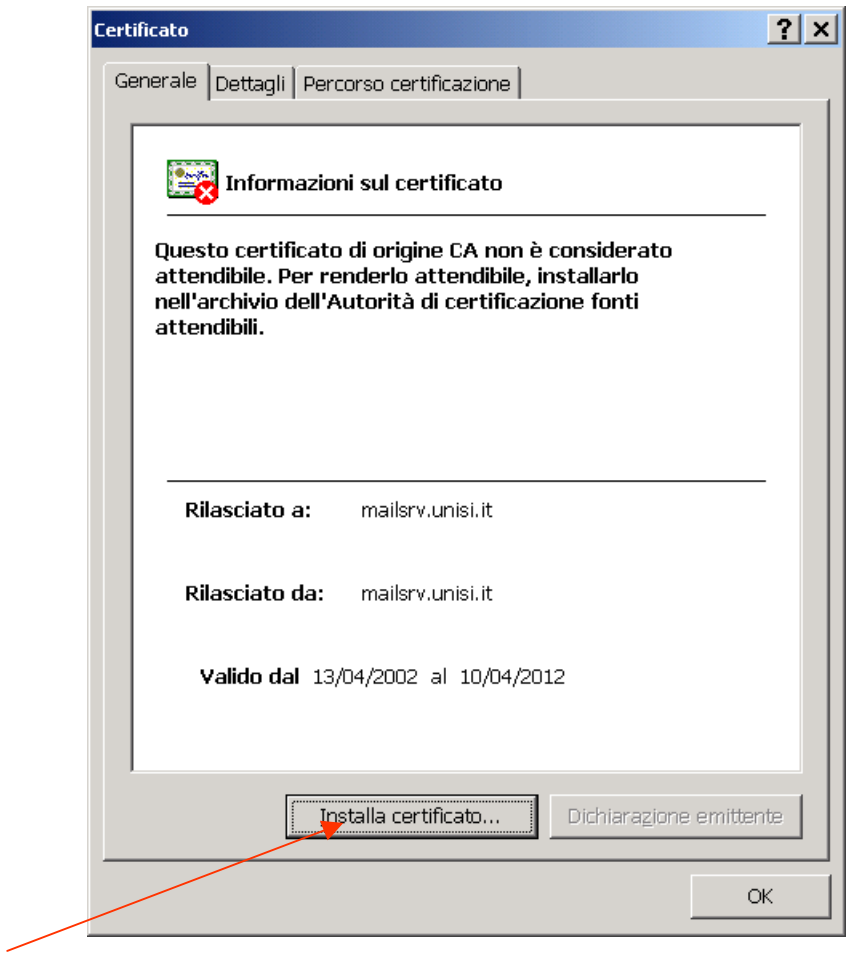
# Utilizzo di SSL

## Certificato digitale del Server



# Secure Socket Layer

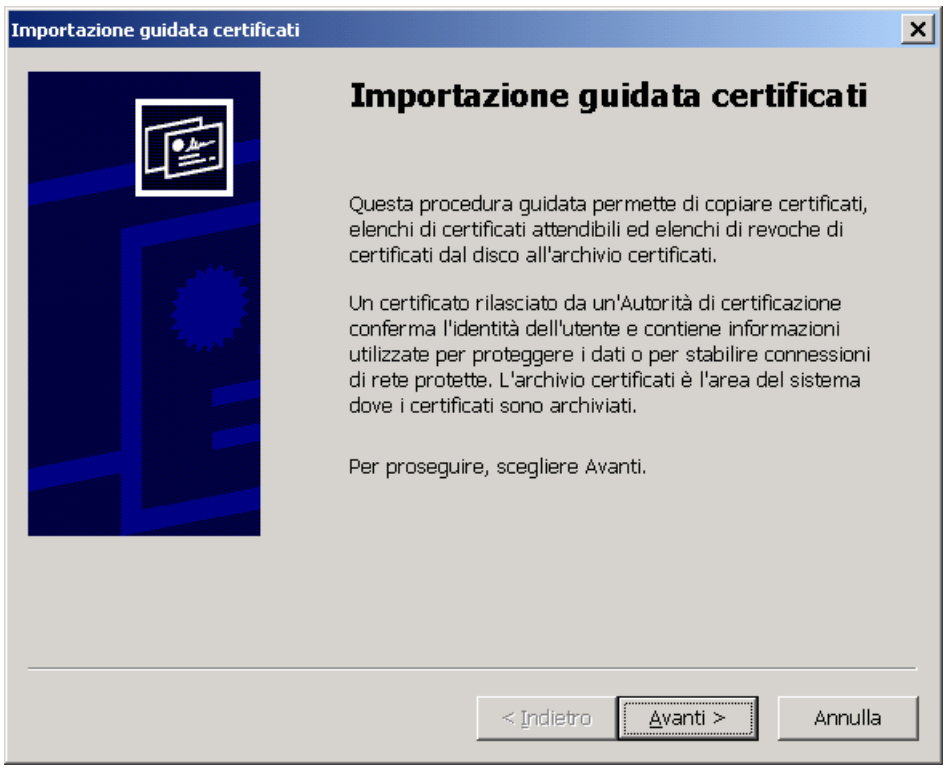
## Installazione Certificati



# Secure Socket Layer

## Installazione Certificati

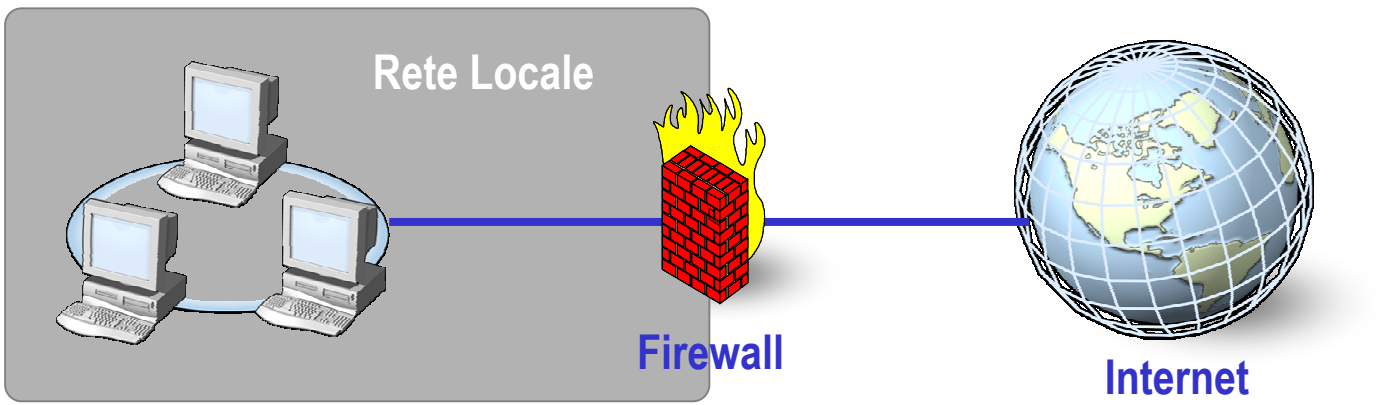
Viene attivata la procedura guidata per l'installazione dei certificati.



# I Firewall

Un firewall è un insieme di componenti logiche e fisiche il cui scopo principale è separare una rete privata da Internet e stabilire a quali servizi interni si possa accedere dall'esterno e a quali servizi esterni si possa accedere dall'interno

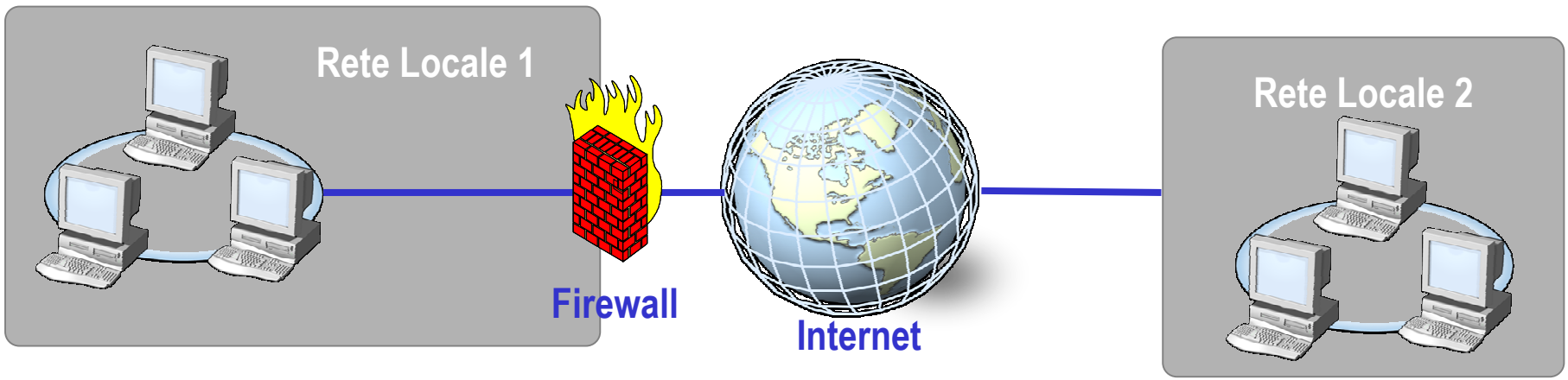
La separazione si ottiene facendo in modo che la comunicazione con il mondo esterno avvenga solo attraverso la mediazione di una o poche macchine della rete privata che costituiscono il firewall.



# I Firewall

## Principio di funzionamento del firewall

Il firewall impedisce il transito di determinati pacchetti in base alle politiche di sicurezza specificate da una tabella di configurazione.

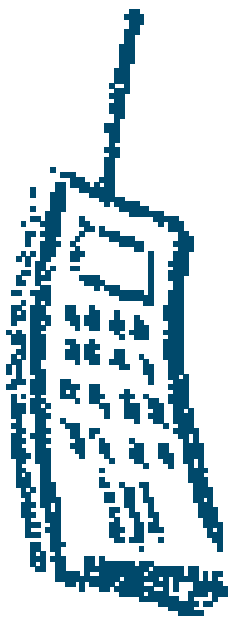



| ID | Azione | Protocollo | Sorgente (Indirizzo - Maschera) | Destinazione (Indirizzo - Maschera) | Porta | Bit ACK |
|---|---|---|---|---|---|---|
| Access-List 101 | OK | TCP | 192.201.127.0 0.0.0.255 | 0.0.0.0 255.255.255.255 | 23 | |
| Access-List 101 | STOP | IP | 0.0.0.0 255.255.255.255 | 0.0.0.0 255.255.255.255 | | |
| Access-List 102 | OK | TCP | 0.0.0.0 255.255.255.255 | 192.201.127.0 0.0.0.255 | > 1024 | OK |
| Access-List 102 | STOP | IP | 0.0.0.0 255.255.255.255 | 0.0.0.0 255.255.255.255 | | |

Tabella di configurazione del Firewall

# La sicurezza nelle reti mobili

Le trasmissioni d'informazioni via etere sono più soggette a problematiche di sicurezza rispetto a quelle che usano il cavo come mezzo fisico. Ascoltare le comunicazioni su una tratta radio può essere, in alcuni casi, abbastanza semplice e non richiede l'accesso a particolari posizioni fisiche.



# La sicurezza nelle reti mobili

Il modello di sicurezza nel **GSM** (Global System for Mobile Communications)

Le funzioni di sicurezza presenti nel sistema GSM hanno 2 obiettivi:

Proteggere la rete da accessi non autorizzati

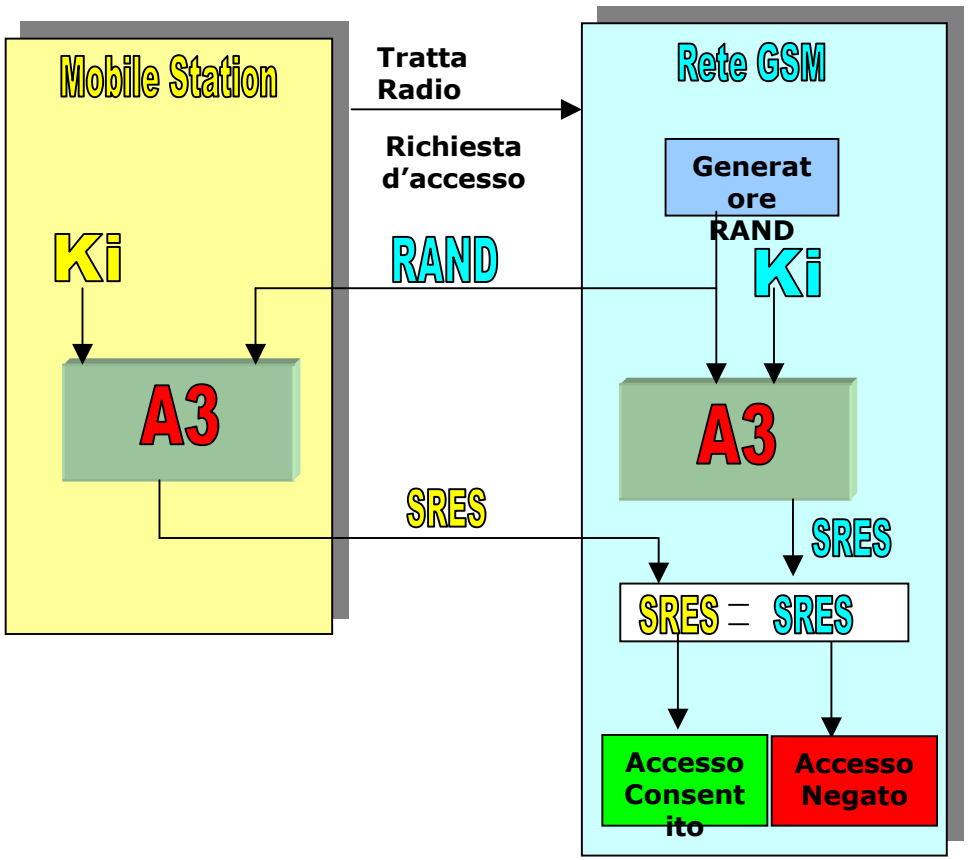
Viene realizzato un controllo sull'identità dell'utente attraverso l'utilizzo di un informazione segreta (**Ki**) condivisa solo dall'utente e dalla rete.

Proteggere la Privacy dell'utente

La privacy è ottenuta tramite la cifratura delle informazioni trasmesse (voce) e dei dati di segnalazione.

# Autenticazione nel GSM

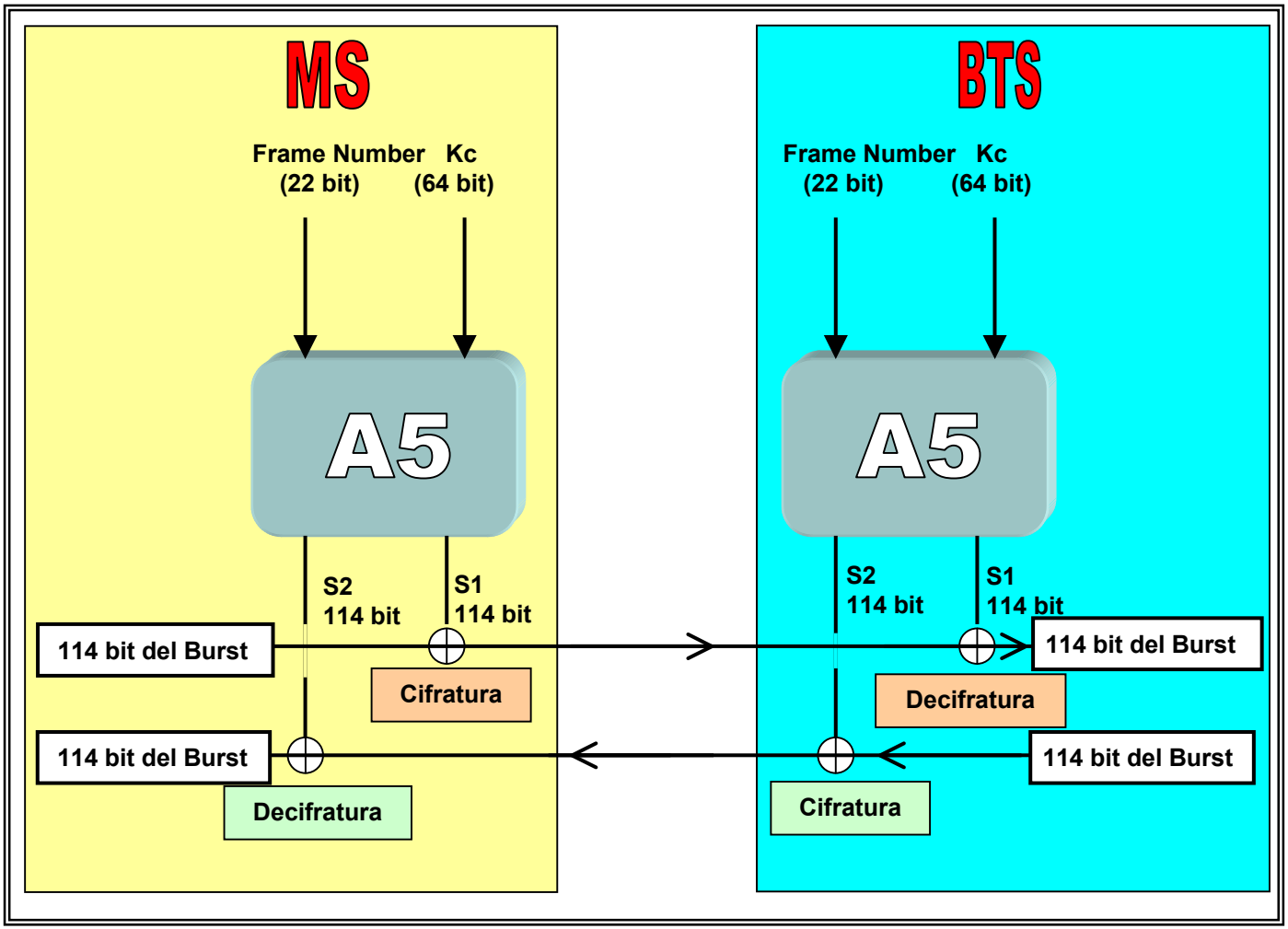
Lo schema di autenticazione presso l'operatore si fonda sulla condivisione di una chiave segreta rappresentata da un numero: il **Ki** di 128 bit




- Lato utente la chiave KI è memorizzata in un area protetta della SIM.
- L'Algoritmo A3 è implementato nella SIM, è dipendente dall'operatore di rete e non è pubblico.

# Protezione dei dati nel GSM

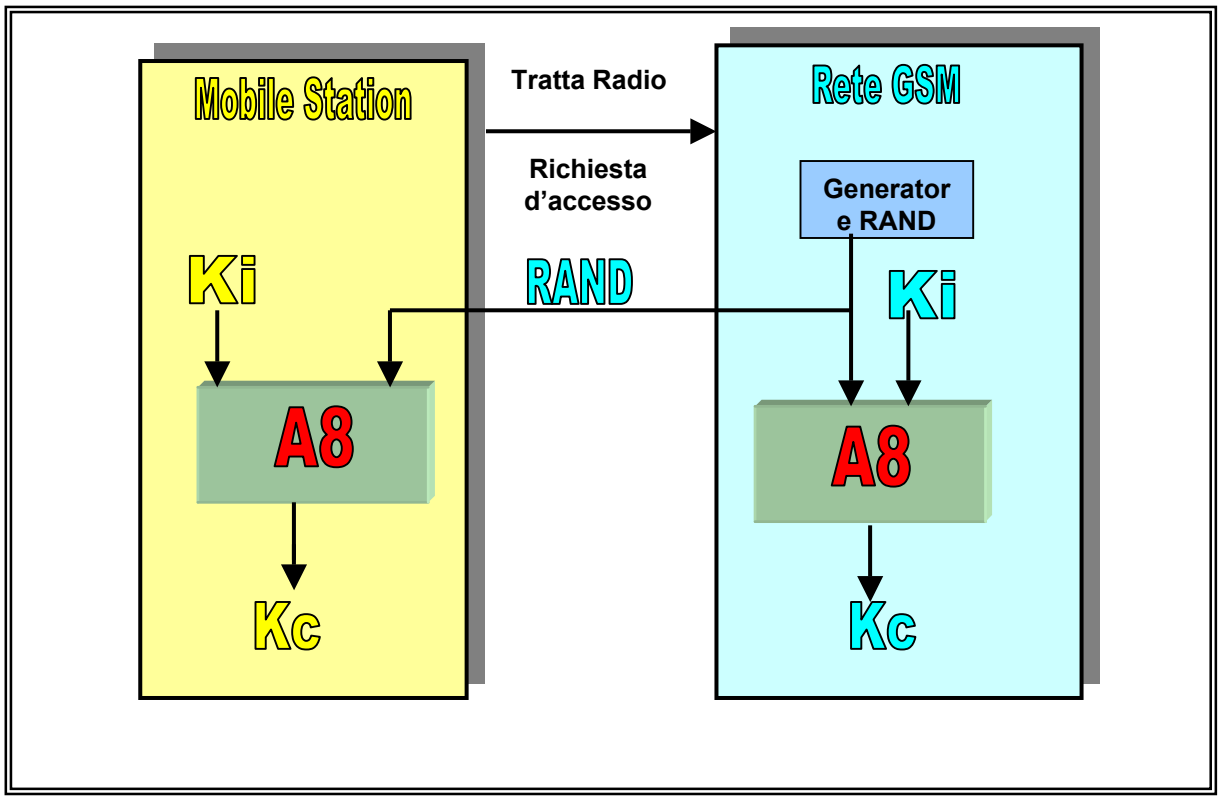
I dati utente vengono protettiti con la cifratura solamente sull'interfaccia radio: tra la MS e la BTS.




L'algoritmo A5 è standardizzato a livello internazionale ed è implementato nella Stazione Mobile. L'algoritmo utilizza una chiave Kc che viene stabilita attraverso una opportuna procedura.

# Calcolo della chiave di sessione Kc

La chiave di sessione Kc viene accordata tra l'MS e la rete durante l'autenticazione.




Per il calcolo della chiave Kc si utilizza un algoritmo A8 che dipende dall'operatore di rete, quindi è implementato nella SIM. Lato utente il Kc viene memorizzato nelle SIM.

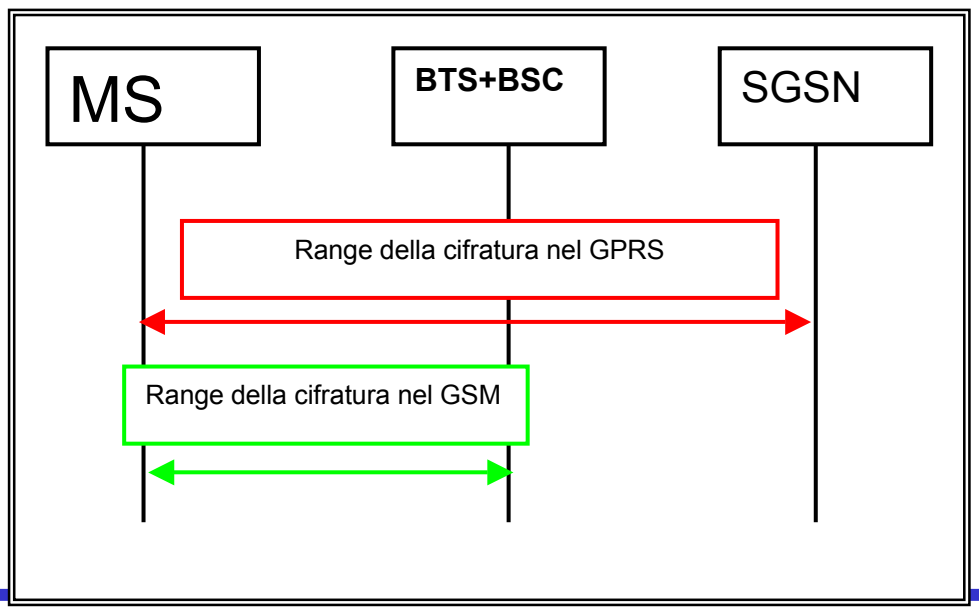
# Il modello di sicurezza nel GPRS, General Radio Packet Service

Le funzioni di sicurezza delle rete GPRS sono del tutto identiche a quelle del GSM. Per l'autenticazione degli utenti ed il calcolo della chiave di sessione si usano rispettivamente gli algoritmi A3 e A8, implementati nella SIM.

La sola differenza tra GSM e GPRS sta negli elementi della rete che realizzano le funzioni di sicurezza.

La procedura di autenticazione è gestita dal SGSN (Service GPRS Support Node), si tratta fondamentalmente di un router (commuta a pacchetto).

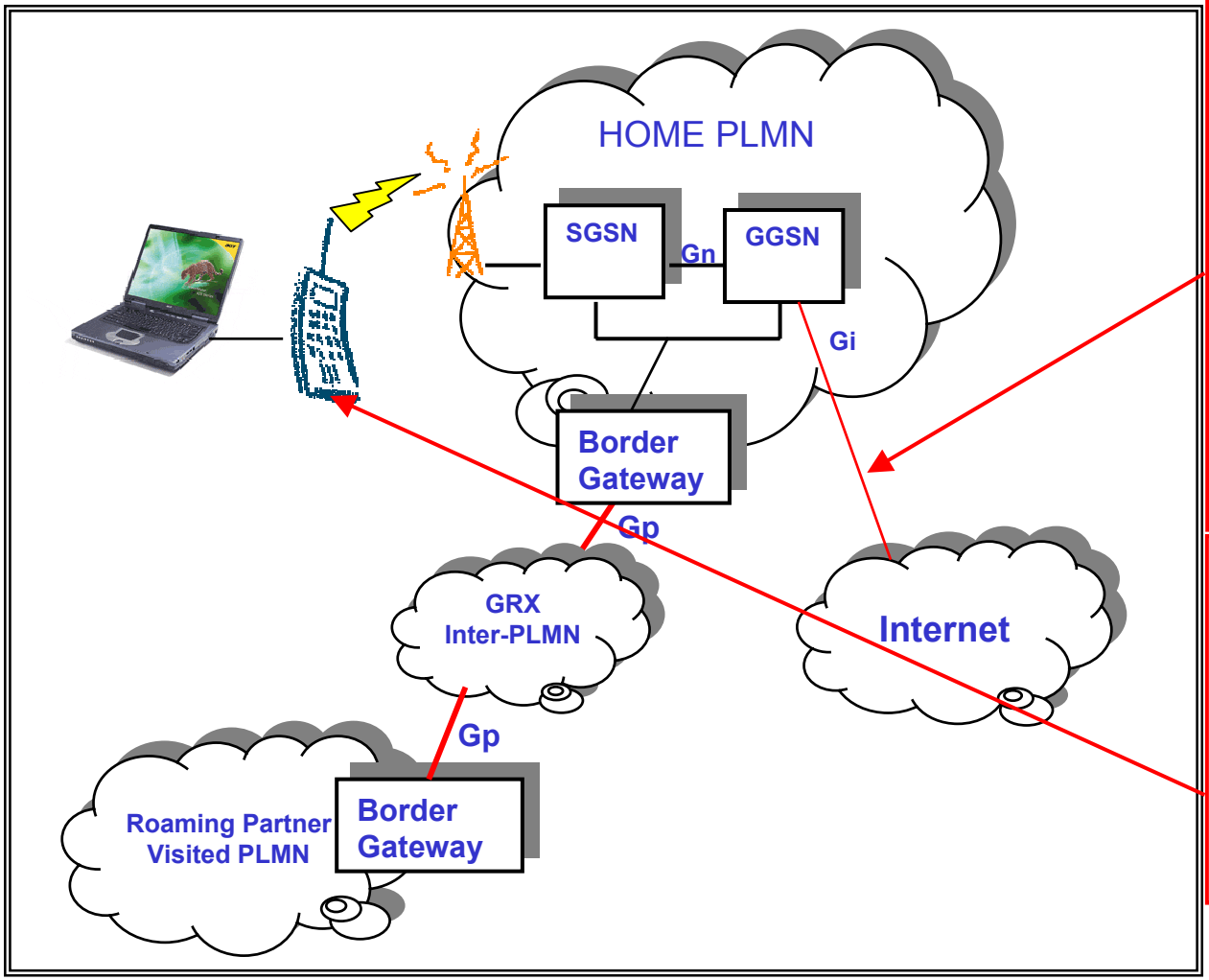
Per quanto riguarda la cifratura la differenza principale sta nel "range" (estensione) della cifratura. Il range della cifratura nel GSM va dalla stazione mobile alla BTS, mentre nel GPRS arriva fino al nodo SGSN.




L'algoritmo utilizzato è un versione ottimizzata dell'A5 per il traffico a pacchetti.

# Minacce alla sicurezza della rete GPRS

Con l'aggiunta dei nuovi servizi per i dati, gli operatori hanno esposto le loro reti a ulteriori rischi per la sicurezza delle comunicazioni.

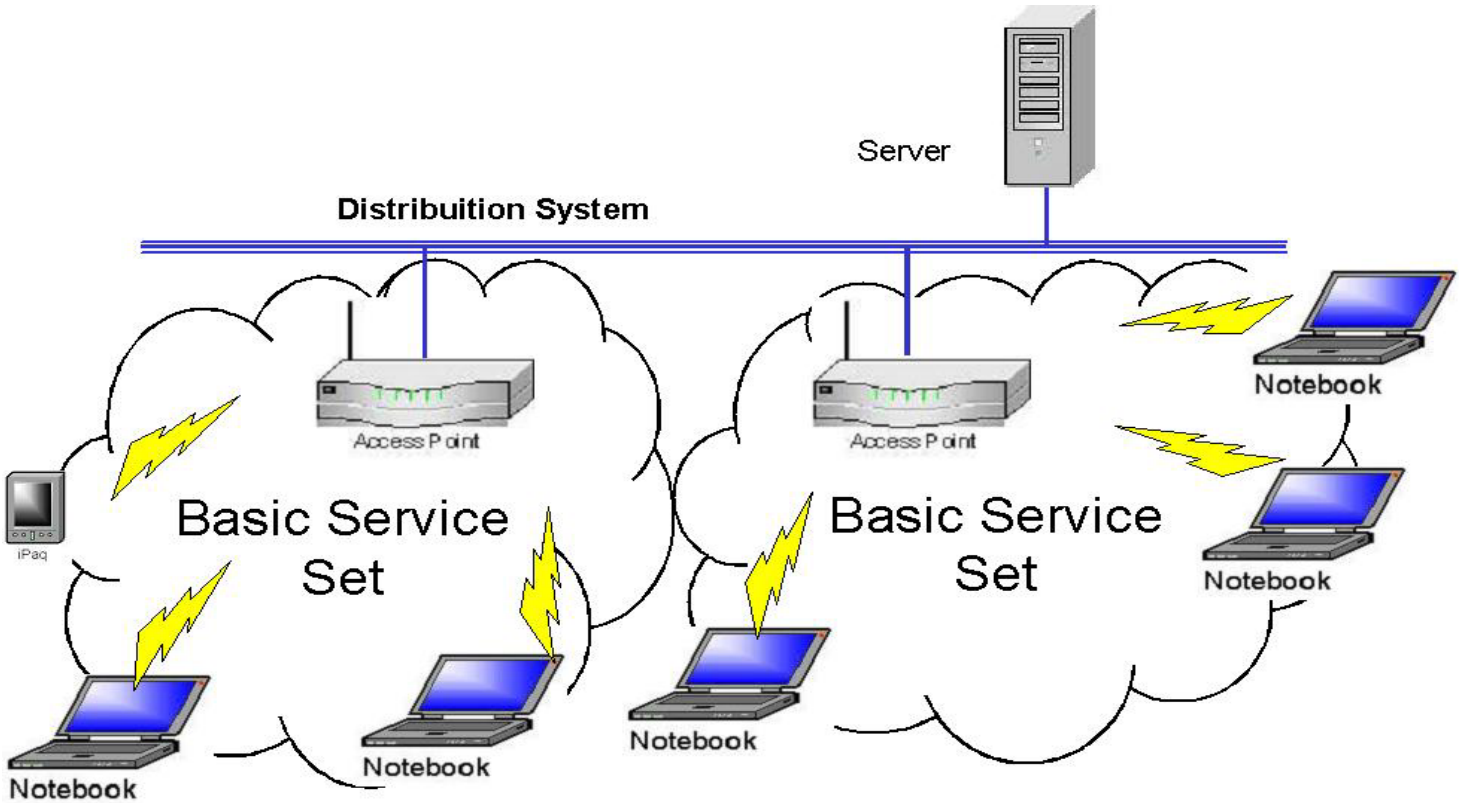



L'attacco Denial of Service rappresenta la minaccia più pericolosa sull'interfaccia Gi. Viene ottenuto inondando di traffico il link di connessione tra la rete dell'operatore ed e la rete Internet.

Se un'elevata quantità di traffico viene indirizzata direttamente verso l'indirizzo IP di una MS, si impedisce a questa di utilizzare la rete GPRS.

# La sicurezza nelle reti mobili

## Sicurezza nelle Wireless LAN - 802.11

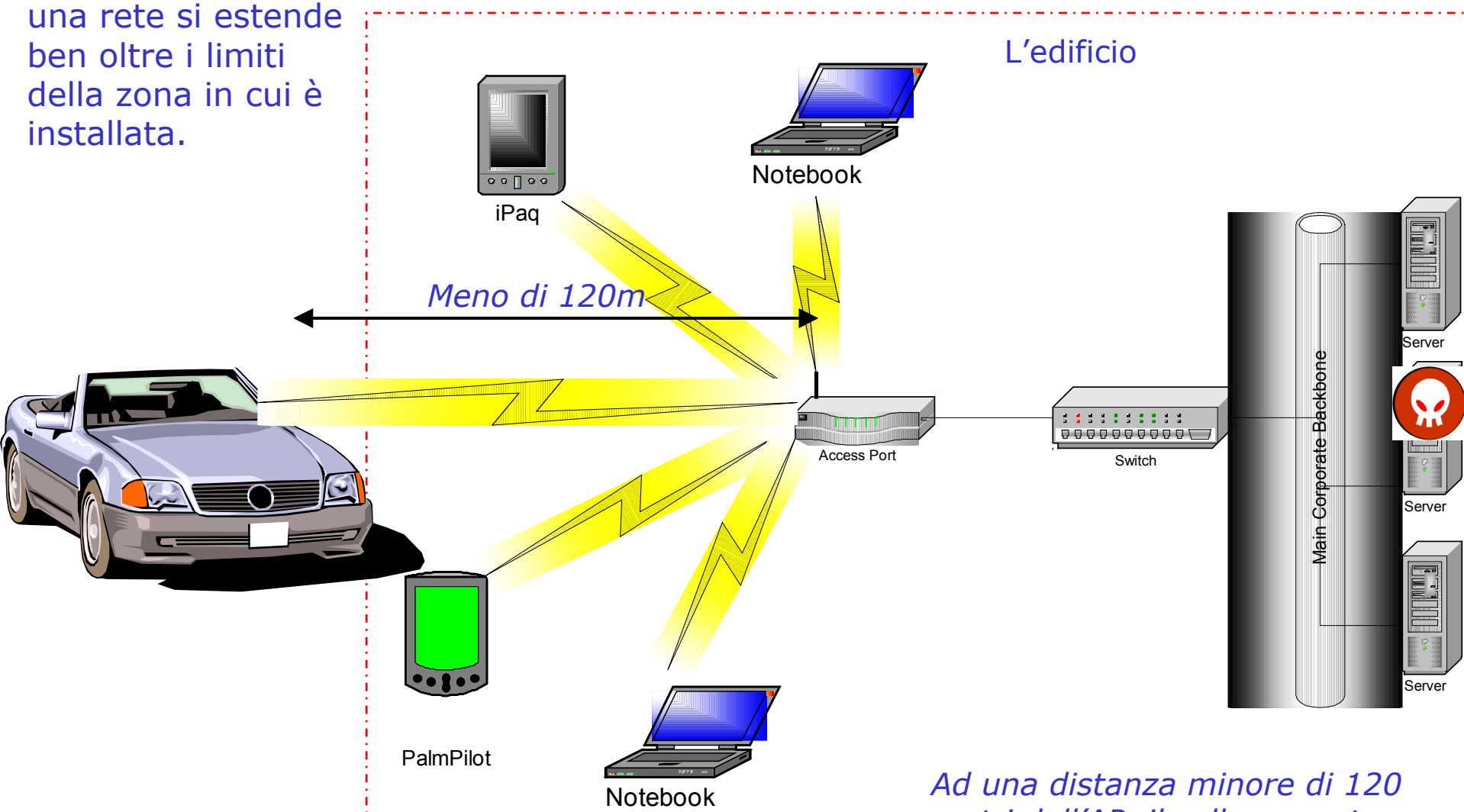



Wireless Lan Infrastructure

L'Access Point è l'elemento delle rete Wireless che permette alle stazioni appartenenti ad una stessa BSS di comunicare tra loro. Inoltre consente l'accesso al Sistema di Distribuzione ed eventualmente ad Internet.

# Sicurezza nelle Wireless LAN

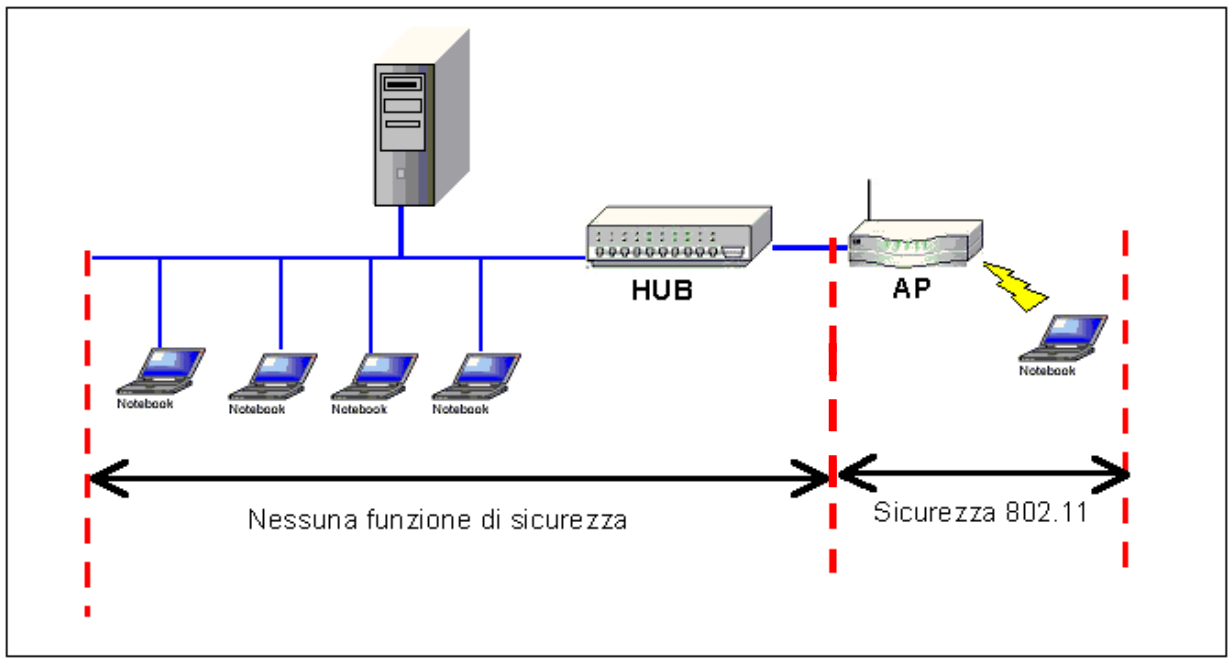
Il difetto principale delle reti wireless è dovuto al fatto che il raggio di copertura di una rete si estende ben oltre i limiti della zona in cui è installata.




*Ad una distanza minore di 120 metri dall'AP, il collegamento puo` essere ottenuto anche dall'esterno dell'azienda.*

# Sicurezza nelle Wireless LAN

Lo standard 802.11 utilizza il protocollo **Wired Equivalent Privacy** (**WEP**) come strumento per la protezione dei dati durante la loro trasmissione in "aria" tra le stazioni client e l'Access Point, quindi il WEP non fornisce un livello di sicurezza end-to-end, ma solamente per la porzione della tratta wireless.



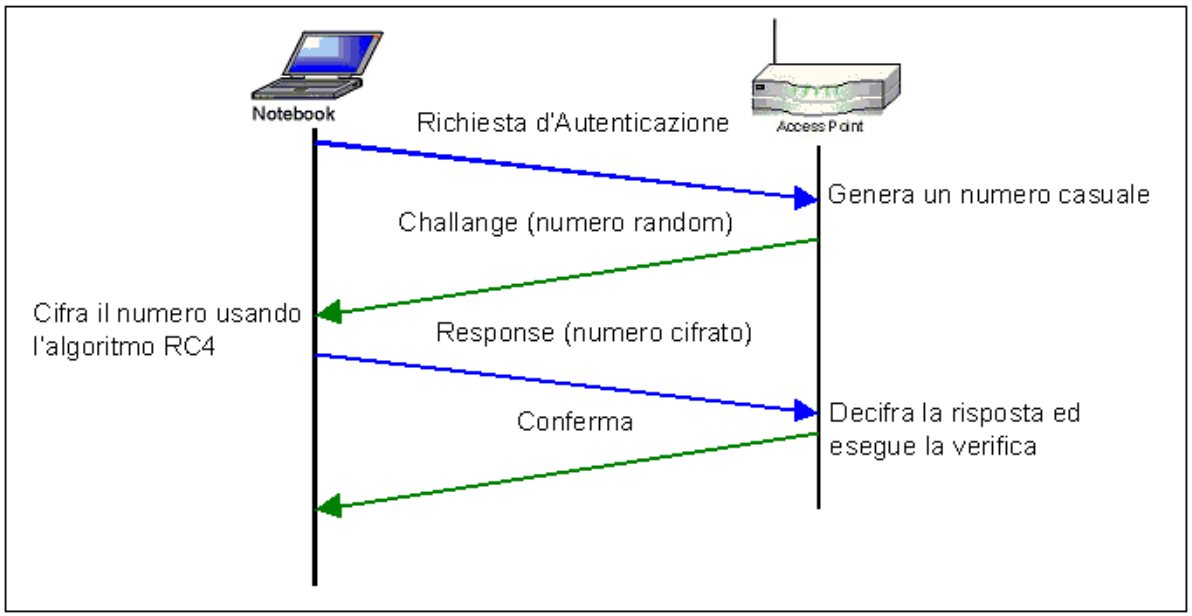

Il WEP si pone 3 obiettivi:

1. Verificare l'identità delle stazioni comunicanti attraverso un processo di Autenticazione.
2. Proteggere i dati utente (Privacy) durante la loro trasmissione in aria.
3. Assicurare l'integrità dei dati.

# Sicurezza nelle Wireless LAN

## Procedura di Autenticazione: ***Shared Key Authentication***

Si tratta di una procedura che utilizza tecniche crittografiche.

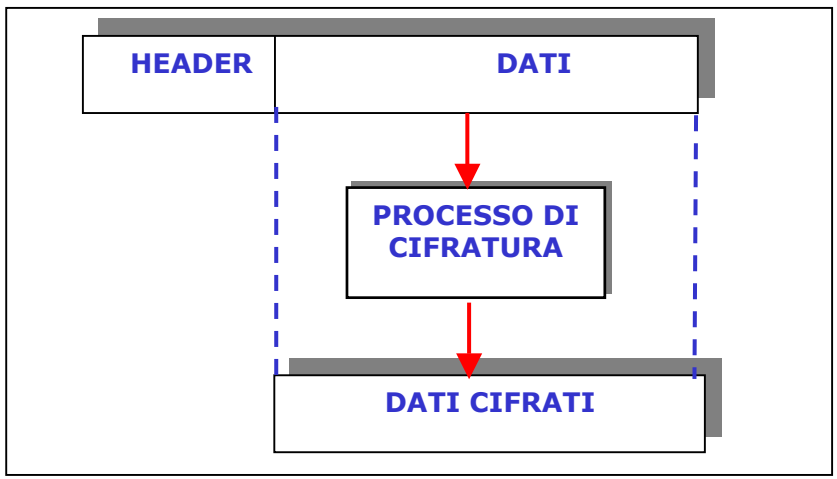



1. Il client invia all'Access Point una richiesta di autenticazione;
2. L'Access Point invia al client un numero casuale;
3. Il client cifra il numero casuale usando una chiave segreta K, condivisa con l'access point, e l'algoritmo RC4;
4. Il client invia il numero cifrato all'Access Point;
5. L'Access Point decifra la risposta ed esegue la verifica;
6. L'Access Point invia una conferma al Client.

Difetti: la chiave condivisa viene impostata manualmente dall'amministratore di rete sia sull'Access Point che sui client. Il client non autentica l'Access-Point.

# Sicurezza nelle Wireless LAN

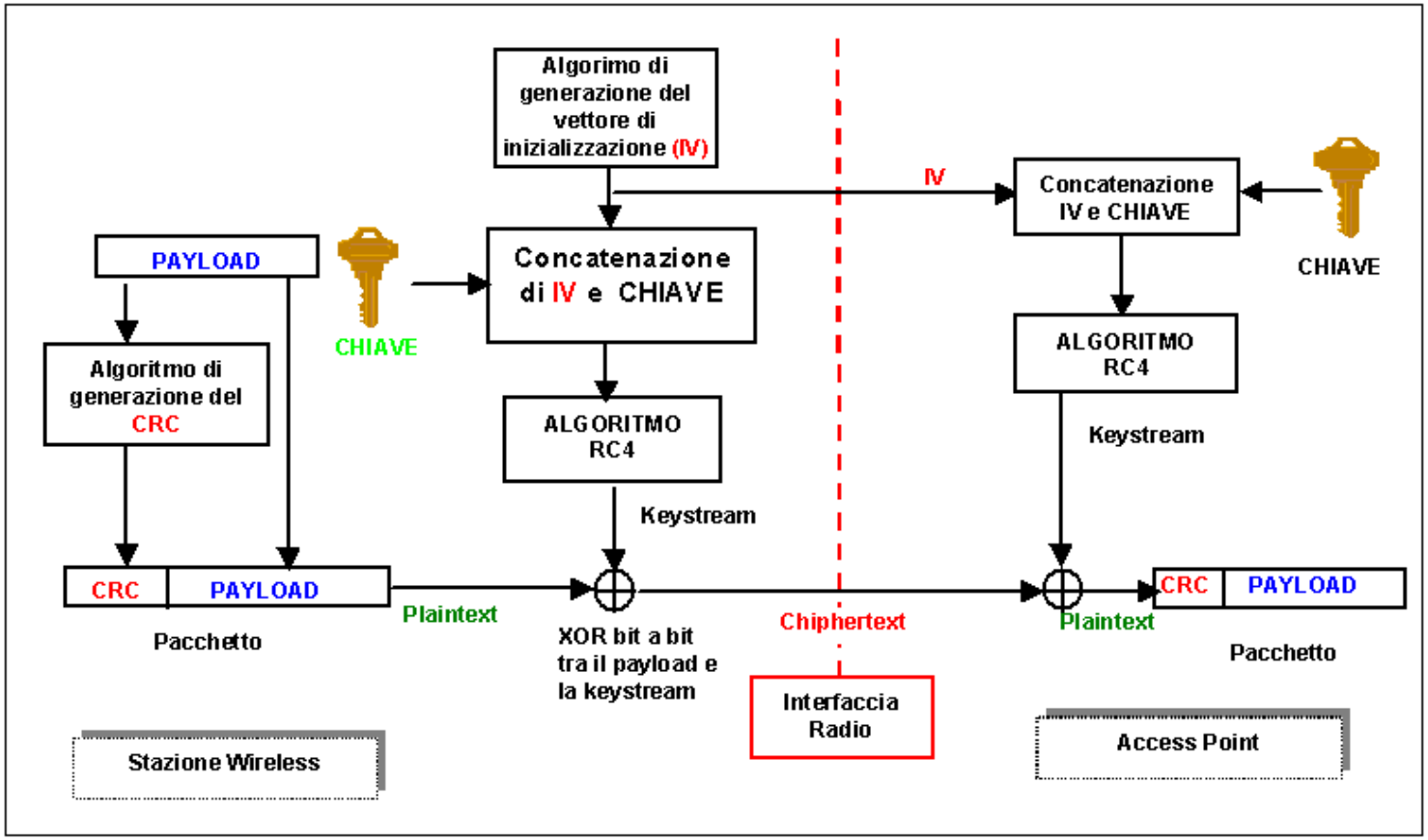
Protezione dei dati utente: viene ottenuta cifrando il campo dati della Frame. Quindi la protezione viene applicata a tutto il traffico appartenente ai livelli superiori al secondo.

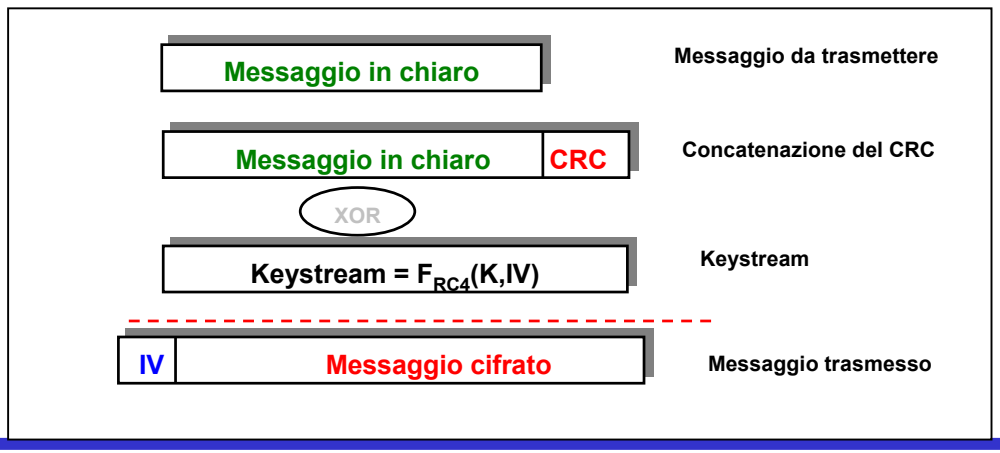



In sostanza i pacchetti TCP/IP attraversano il collegamento wireless in modalità cifrata.

Per cifrare i dati viene usato un cifrario a Flusso (RC4) e la stessa chiave K usata per il processo di autenticazione.

# Processo di cifratura nel WEP.



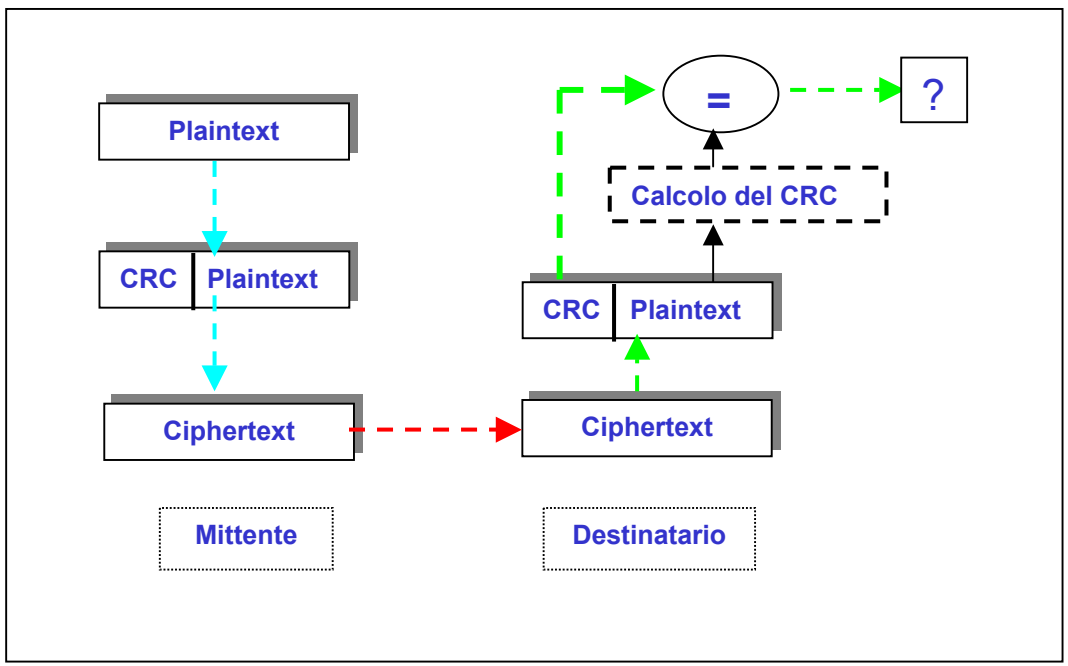

CRC: è una checksum di 32 bit

# Integrità dei dati.

Il protocollo **WEP** garantisce l'integrità dei dati attraverso il calcolo di una semplice checksum (CRC), quindi non utilizza Codici di Autenticazione di Messaggio (MAC) o funzioni hash unidirezionali.

Questo fatto rende l'integrità dei dati uno degli aspetti più deboli del protocollo WEP.

In sostanza il CRC, appeso al payload, ha lo scopo di rilevare errori casuali che si verificano durante la trasmissione.




Verifica del CRC

# Debolezze delle Wireless Lan

Tra gli attacchi più frequenti quello passivo risulta il più semplice da realizzare.

Con questo tipo d'attacco non è necessario associarsi all'Access Point, in quanto la stazione attaccante si limita ad ascoltare e registrare tutto il traffico (sniffing) che attraversa la rete wireless.

Con opportuni software d'analisi dei pacchetti memorizzati è addirittura possibile risalire alle chiavi WEP.

Il software più utilizzato per apportare questo tipo d'attacco, **AirSnort,** richiede semplicemente un computer con sistema operativo Linux ed una scheda di rete Wireless. AirSnort monitora passivamente le trasmissioni e riesce a calcolare la chiave WEP dopo aver collezionato almeno 100MB di dati.




Fabio Burroni

Università degli Studi di Siena

**burronif@unisi.it**