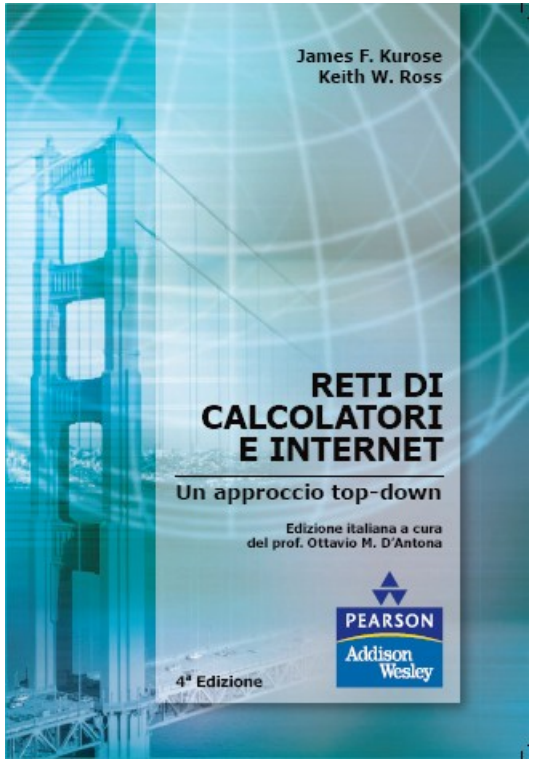
Capitolo 8
La sicurezza nelle reti



Reti di calcolatori e Internet: Un approccio top-down

4ª edizione
Jim Kurose, Keith Ross

Pearson Paravia Bruno Mondadori Spa
©2008

Capitolo 8: La sicurezza nelle reti

Obiettivi:

- Identificare le proprietà per una comunicazione sicura:
  - Tecniche crittografiche e loro molteplici utilizzi al di là della semplice "riservatezza"
  - Autenticazione
  - Integrità del messaggio
- Sicurezza in pratica:
  - Firewall e sistemi per la rilevazione degli intrusi
  - Sicurezza a seconda dello specifico livello (applicazione, trasporto, rete o collegamento)

Capitolo 8 La sicurezza nelle reti

8.1 Sicurezza di rete

8.2 Principi di crittografia

8.3 Integrità dei messaggi

8.4 Autenticazione end-to-end

8.5 rendere sicura la posta elettronica

8.6 Rendere sicure le connessioni TCP: SSL

8.9 Sicurezza operativa: firewall e sistemi di rilevamento delle intrusioni

Sicurezza nella comunicazione

Riservatezza: solo mittente e destinatario devono comprendere il contenuto del messaggio

- Inviare messaggi cifrati
- Ricevere il codice di decifratura

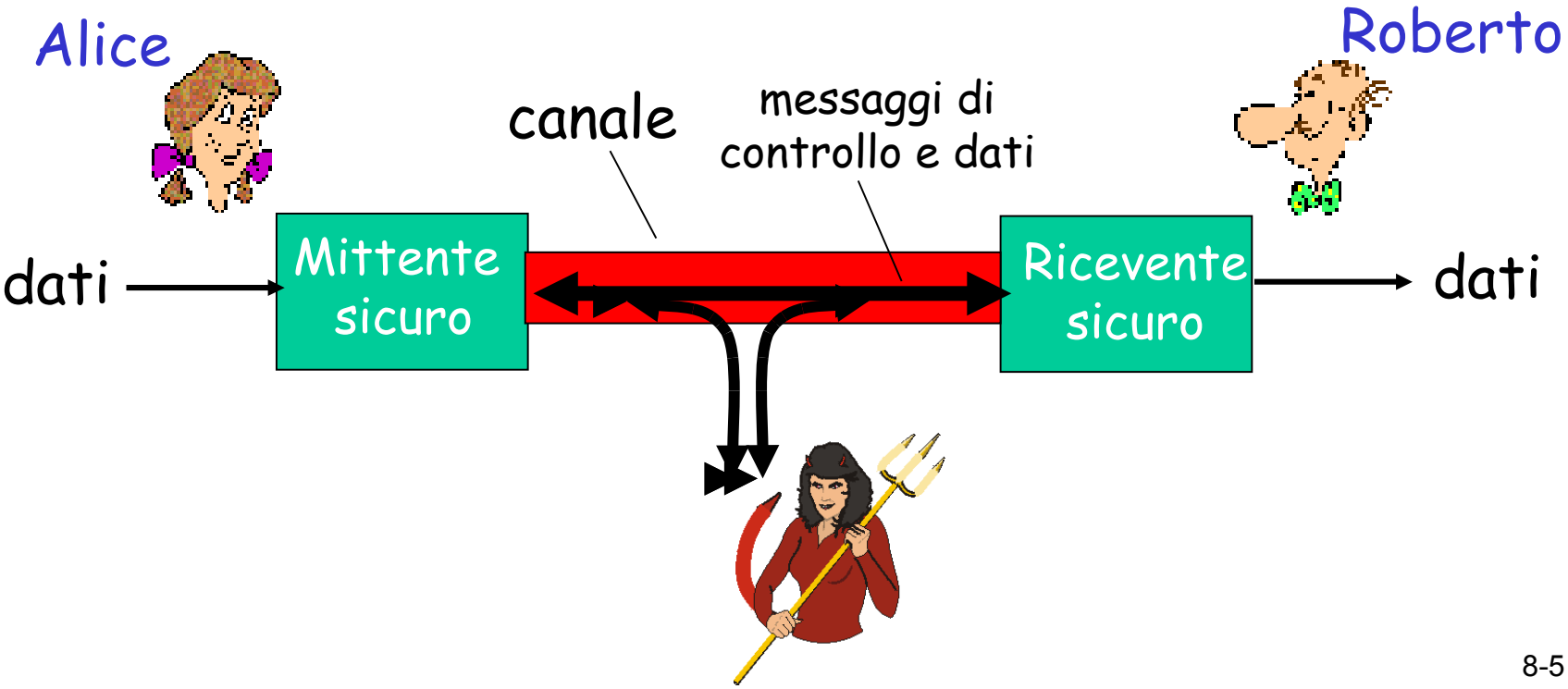
Autenticazione: mittente e destinatario devono essere sicuri della loro identità

Integrità del messaggio: mittente e destinatario devono essere sicuri che il contenuto non subisca alterazioni durante la trasmissione (per cause fortuite o per manipolazioni)

Disponibilità e controllo dell'accesso: un servizio deve essere accessibile a chi è legittimamente autorizzato.

Mittente, ricevente e intruso: Alice, Roberto e l'intruso

- Scenario ben noto nel mondo della sicurezza di rete
- Roberto e Alice vogliono comunicare in modo sicuro
- l'intruso può intercettare, rimuovere, aggiungere messaggi o modificare il loro contenuto



Chi sono Alice e Roberto?

Nella vita reale Alice e Roberto possono essere:

- browser/server Web durante una transazione elettronica (es. un acquisto on-line)
- client/server di banche on-line
- server DNS
- sistemi che si scambiano tabelle d'instradamento
- altro

Là fuori ci sono "cattivi" ragazzi (e ragazze)

D: Cosa può fare un nemico?

R: Molto!

- *spiare:* intercettare i messaggi
- *aggiungere* messaggi e sovraccaricare il sistema
- *impersonare* un altro soggetto
- *dirottare* una sessione in corso e sostituirsi al mittente o al destinatario
- *negare il servizio*

E molto altro ancora! ……

Capitolo 8 La sicurezza nelle reti

8.1 Sicurezza di rete

8.2 Principi di crittografia

8.3 Integrità dei messaggi

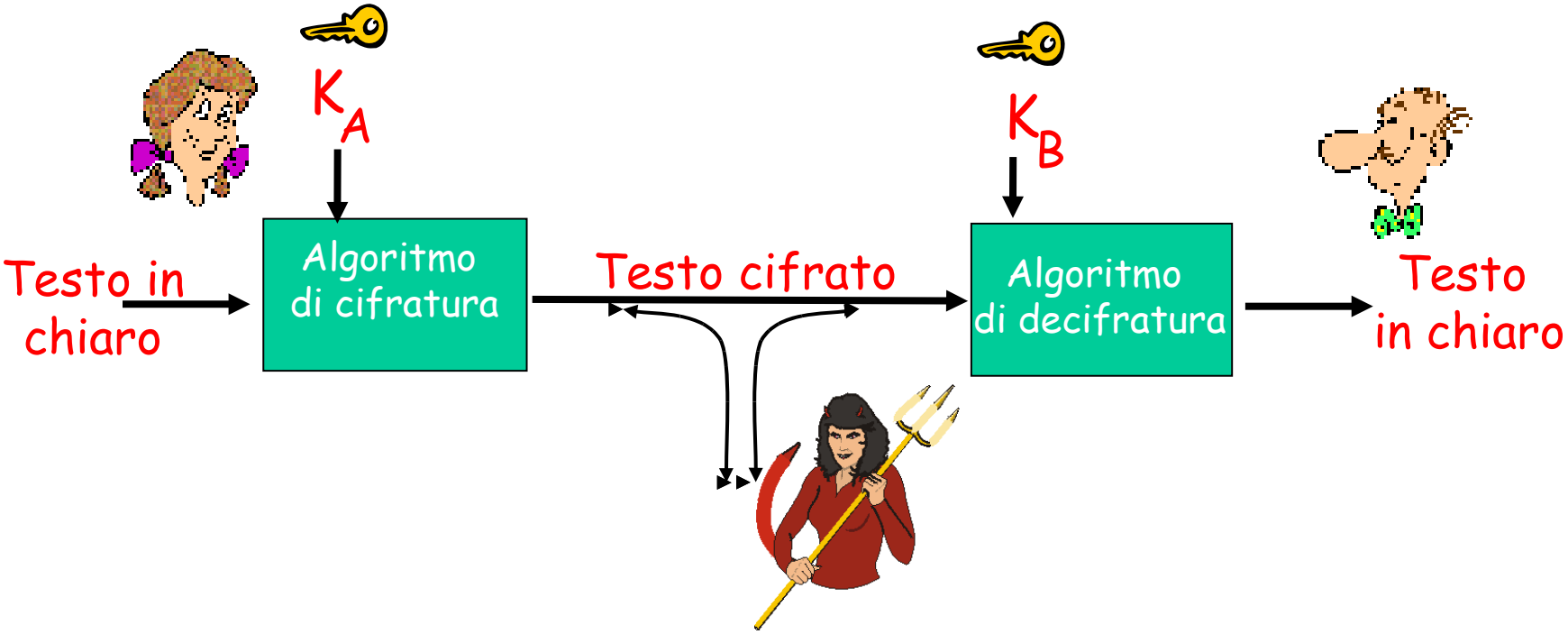
8.4 Autenticazione end-to-end

8.5 rendere sicura la posta elettronica

8.6 Rendere sicure le connessioni TCP: SSL

8.9 Sicurezza operativa: firewall e sistemi di rilevamento delle intrusioni

Principi di crittografia



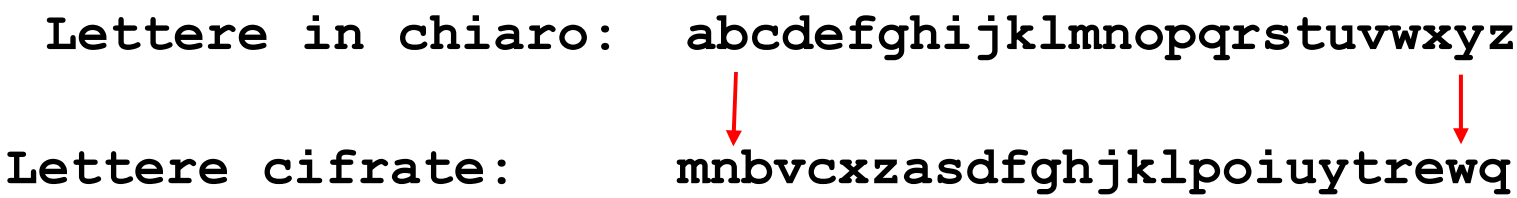
Sistemi a chiave simmetrica: le chiavi del mittente e del destinatario sono identiche

Sistemi a chiave pubblica: la chiave di cifratura è pubblica; la chiave di decifratura è privata

Crittografia a chiave simmetrica

Algoritmo di cifratura: sostituzione di un messaggio in chiaro con uno codificato

- Cifrario monoalfabetico: sostituzione di una lettera con un'altra



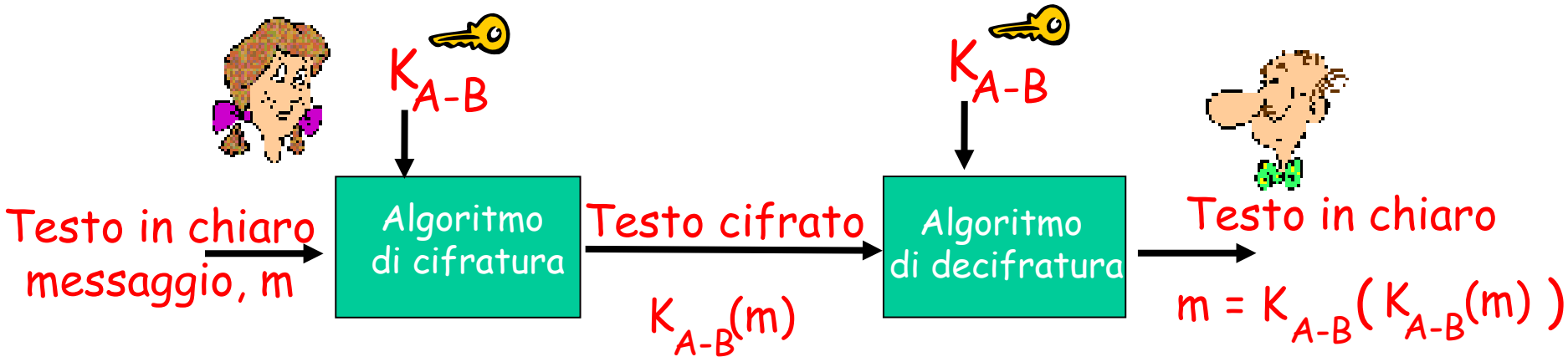
esempio

```
Testo in chiaro: bob. i love you. alice
Testo cifrato:   nkn. s gktc wky. mgsbc
```

D: Come violare questo sistema di cifratura?:

- con un attacco a "forza bruta" (ma quanto bruta?)
- altri sistemi?

Crittografia a chiave simmetrica



- Crittografia a chiave simmetrica: Alice e Roberto utilizzano la stessa chiave K_{A-B}
- es: la chiave è un pattern di sostituzione monoalfabetico
- D: come fanno Roberto e Alice a concordare la chiave?

Crittografia a chiave simmetrica: DES

DES: *Data Encryption Standard*

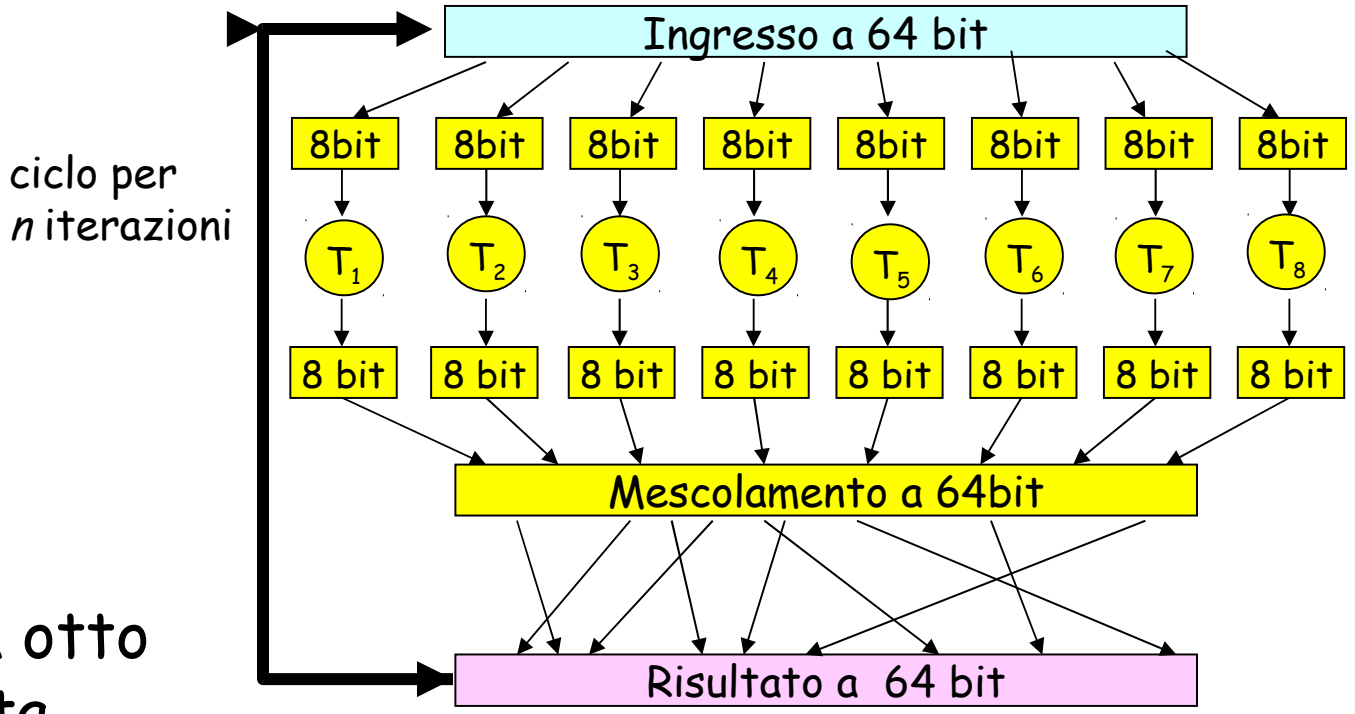
- Standard codificato e aggiornato dall'U.S. National Bureau of Standards [NIST 1993]
- Codifica il testo in chiaro in blocchi di 64 bit; la lunghezza effettiva della chiave è di 56 bit
- Ma quanto è sicuro DES?
  - DES Challenge: nel 1997, durante un concorso, la frase "Strong cryptography makes the world a safer place" fu individuata in meno di 4 mesi
- Come rendere DES più sicuro:
  - usare sequenzialmente tre chiavi (3DES, triplo DES)
  - utilizzare il concatenamento dei blocchi cifrati

AES: Advanced Encryption Standard

(Algoritmo di Rijndael)

- Nel novembre 2001 NIST ha annunciato il sostituto di DES: AES.
- AES processa i blocchi a 128 bit
- Opera con chiavi a 128, 192 e 256 bit
- Se ci fosse un calcolatore che può individuare una chiave DES a 56 bit in 1 secondo, per violare una chiave AES a 128 bit ci impiegherebbe 149 miliardi di anni.

Cifrario a blocchi



- Un bit in ingresso condiziona otto bit in uscita

- Passaggi multipli: ciascun bit in ingresso condiziona tutti i bit in uscita
- comuni cifrari a blocchi: DES, 3DES, AES

Crittografia a chiave pubblica

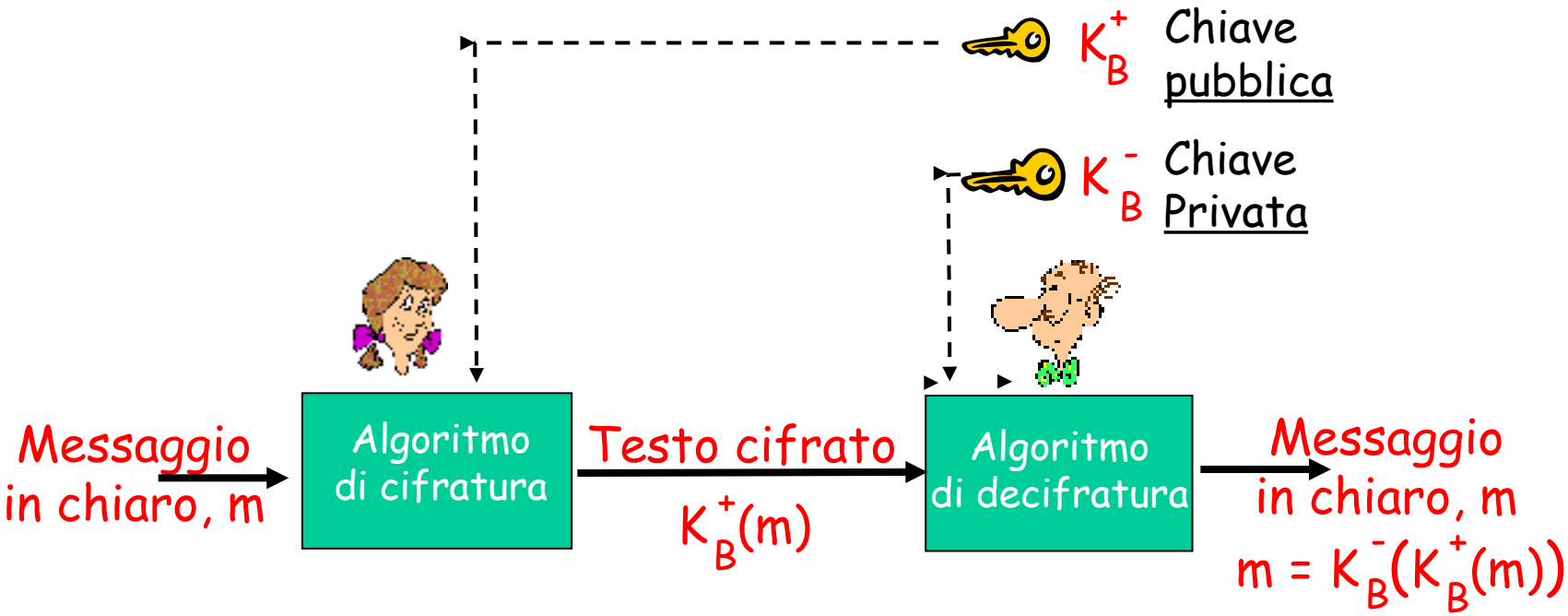
Crittografia a chiave simmetrica

- Richiede che mittente e destinatario condividano una chiave segreta
- D: come si concorda la chiave (specialmente se i due interlocutori non si sono mai "incontrati")?

Crittografia a chiave pubblica

- approccio radicalmente diverso [Diffie-Hellman76, RSA78]
- mittente e destinatario *non* condividono una chiave segreta
- la chiave di cifratura *pubblica* è nota *a tutti*
- la chiave di cifratura *privata* è nota solo al destinatario

Crittografia a chiave pubblica



Algoritmi di cifratura a chiave pubblica

Requisiti:

1. K_B^+ e K_B^- tale che

$$K_B^-(K_B^+(m)) = m$$

2. data la chiave pubblica K_B^+, deve essere impossibile calcolare la chiave privata K_B^-

Algoritmo RSA: acronimo derivato dal nome dei suoi autori: Rivest, Shamir e Adelson

RSA: un'altra importante proprietà

La seguente proprietà sarà *molto* utile più avanti:

$$K_B^-(K_B^+(m)) = m \quad = \quad K_B^+(K_B^-(m))$$

Si usa prima la chiave pubblica, e poi quella privata

Si usa prima la chiave privata, e poi quella pubblica

Il risultato non cambia!

Capitolo 8 La sicurezza nelle reti

8.1 Sicurezza di rete

8.2 Principi di crittografia

8.3 Integrità dei messaggi

8.4 Autenticazione end-to-end

8.5 rendere sicura la posta elettronica

8.6 Rendere sicure le connessioni TCP: SSL

8.9 Sicurezza operativa: firewall e sistemi di rilevamento delle intrusioni

Integrità del messaggio

Roberto riceve un messaggio da Alice, e vuole essere sicuro che:

- il messaggio provenga effettivamente da Alice
- il messaggio non sia stato alterato lungo il cammino

Funzioni hash crittografiche

- prende in input m, produce un valore a lunghezza fissa, H(m)
  - Come nella checksum Internet
- Deve essere computazionalmente impossibile trovare due messaggi x e y tali che H(x) = H(y)
  - o anche: dato m = H(x), (con x sconosciuta), è impossibile determinare x.

La checksum di Internet: un algoritmo di sintesi poco efficace

La checksum di Internet ha alcune delle proprietà di una funzione hash:

- Crea sintesi di messaggi di lunghezza fissa (16 bit)
- È molti-a-uno

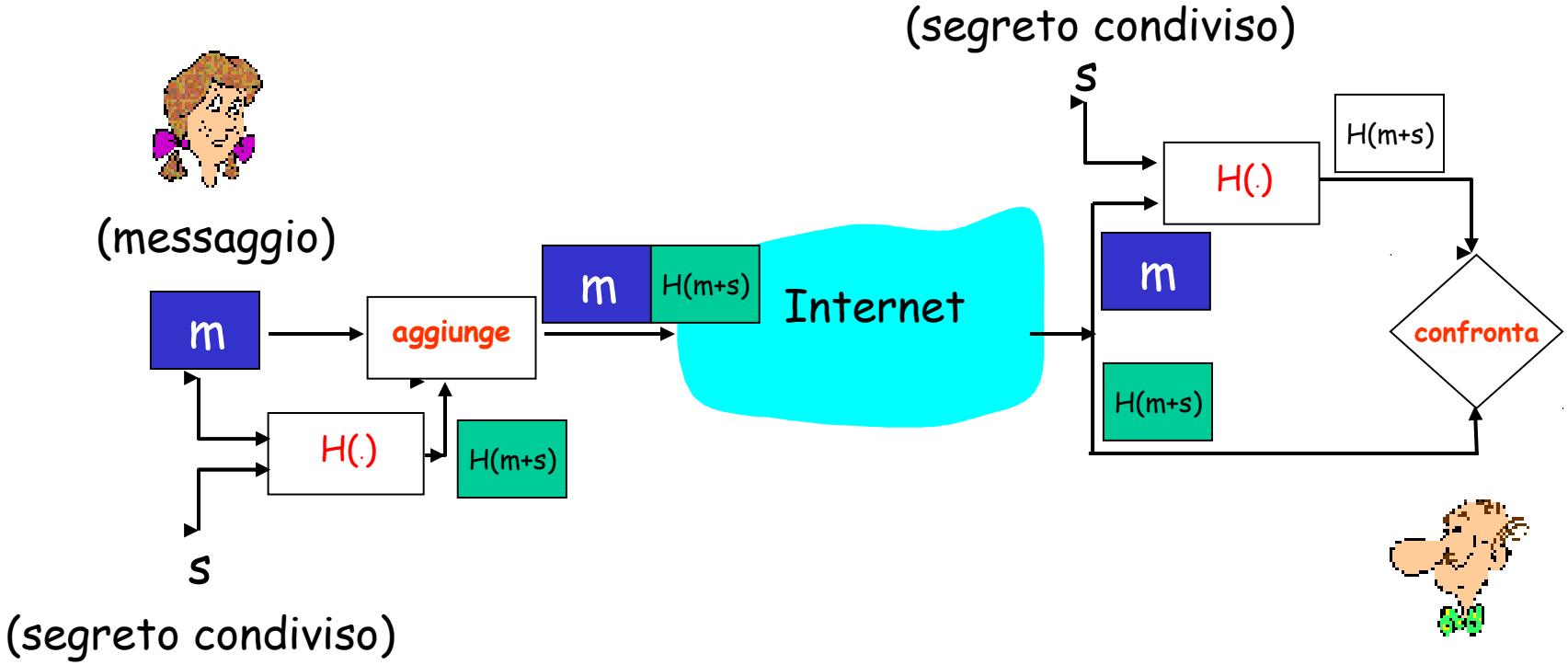
Ma è relativamente semplice trovare altri dati che utilizzano la stessa checksum del messaggio originale:

Messaggio	Rappresentaz. ASCII
I O U 1	73 79 85 49
0 0 . 9	48 48 46 57
9 B O B	57 66 79 66
	178 193 210 172

Messaggio	Rappresentaz. ASCII
I O U 9	73 79 85 57
0 0 . 1	48 48 46 49
9 B O B	57 66 79 66
	178 193 210 172

Messaggi diversi
ma checksum identica!

Codice di autenticazione dei messaggi (MAC)



Codici di autenticazione dei messaggi

- MD5 è molto usato per per l'hash dei messaggi (RFC 1321)
  - Calcola una hash di 128 bit con un processo a 4 fasi
  - Con una stringa x di 128 bit arbitrari, appare difficile costruire un messaggio m il cui hash MD5 sia uguale a x
    - recentemente (2005) sono stati condotti attacchi contro MD5
- È molto usato anche hash sicuro (SHA-1)
  - Standard statunitense [NIST, FIPS PUB 180-1]
  - Produce una sintesi del messaggio di 160 bit

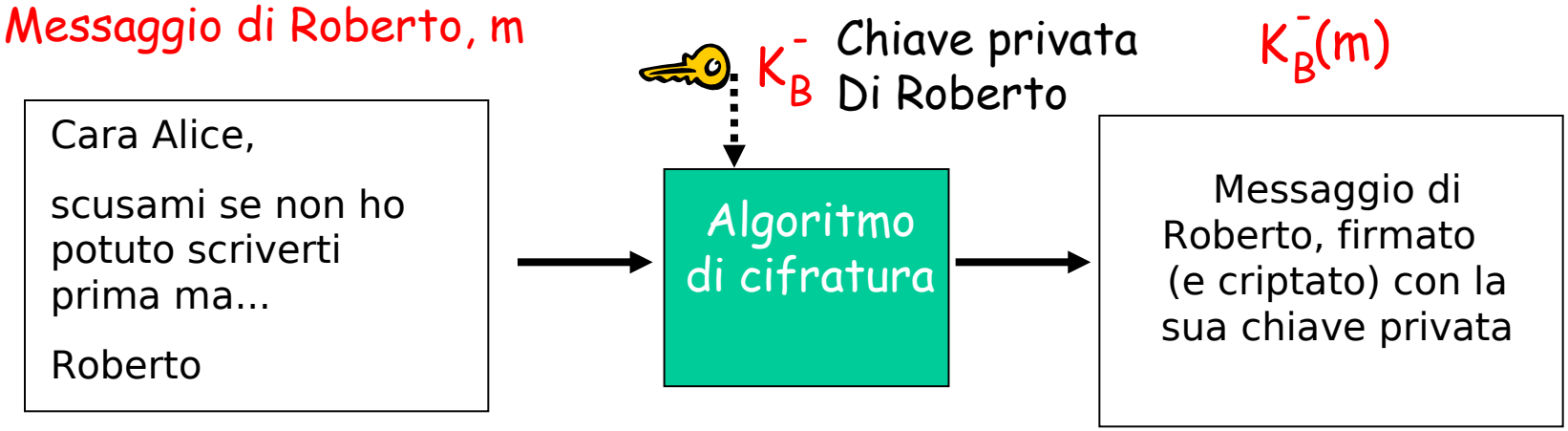
Firma digitale

Tecnica crittografica analoga all'invio di una tradizionale "firma scritta"

- Il mittente (Roberto) firma digitalmente un documento, stabilendo che lui è l'unico proprietario/creatore del messaggio.
- Verificabile e non falsificabile: il destinatario (Alice) può dimostrare che Roberto e nessun altro (Alice inclusa) può aver firmato il documento.

Firma digitale

- Creazione della firma digitale di un messaggio, m:
- Roberto firma un messaggio, m, e lo codifica utilizzando la sua chiave privata K_B^-, creando così un messaggio "firmato", $K_B(m)$



Firma digitale

- Supponiamo che Alice riceva un messaggio m, con la firma digitale $K^-_B(m)$
- Alice verifica che m è firmato da Roberto applicando la chiave pubblica di Roberto K^+_B a $K^-_B(m)$ e controlla che $K^+_B(K^-_B(m)) = m$.
- Se $K^+_B(K^-_B(m)) = m$, chiunque abbia firmato m deve usare la chiave privata di Roberto .

Alice può verificare che:

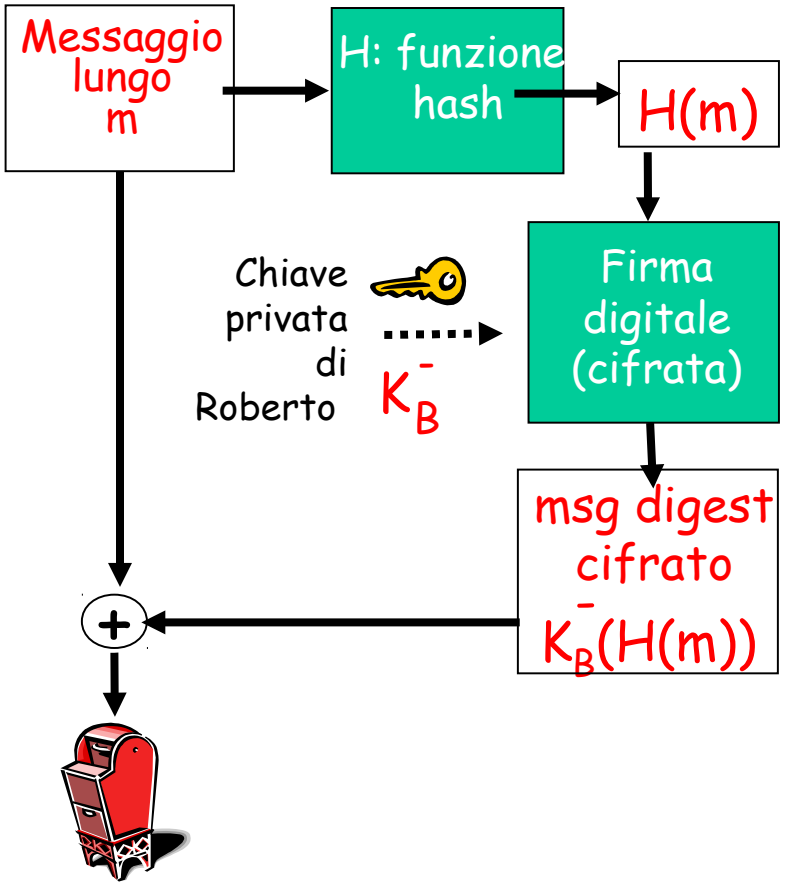
- ✓ Roberto ha firmato m.
- ✓ Nessun altro ha firmato m.
- ✓ Roberto ha firmato m e non m'.

Non-ripudio:

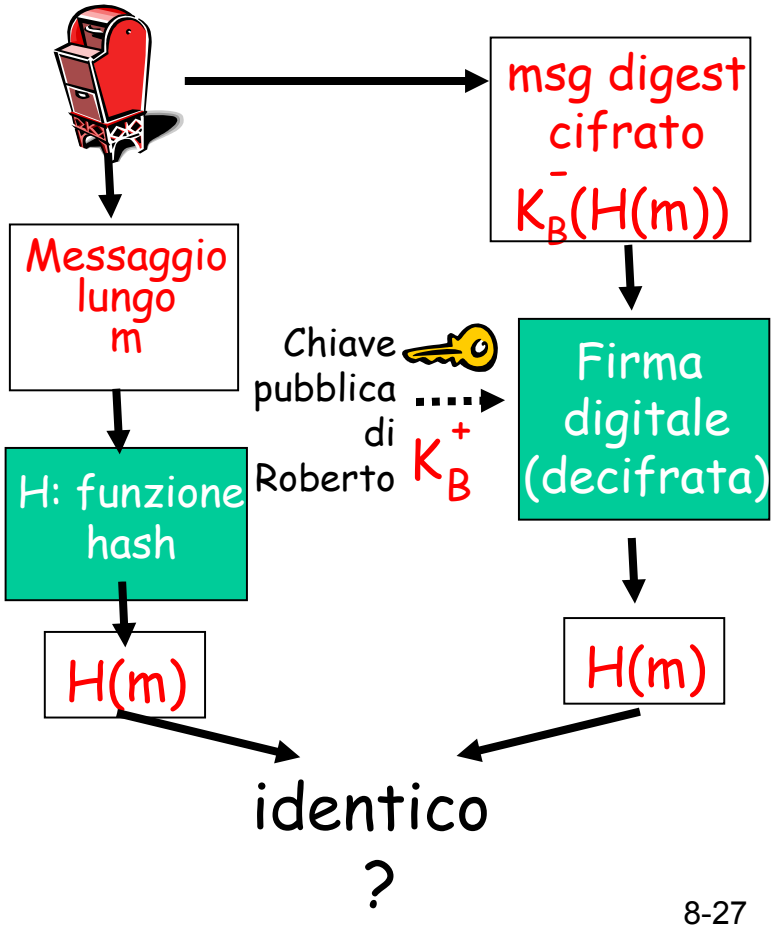
- Alice può prendere m, e la firma $K^-_B(m)$ per dimostrare che Roberto ha firmato m.

Firma digitale = messaggi digest firmati

Roberto invia un messaggio con la firma digitale:



Alice verifica la firma e l'integrità del messaggio con la firma digitale:



Certificazione della chiave pubblica

Problema per la crittografia a chiave pubblica:

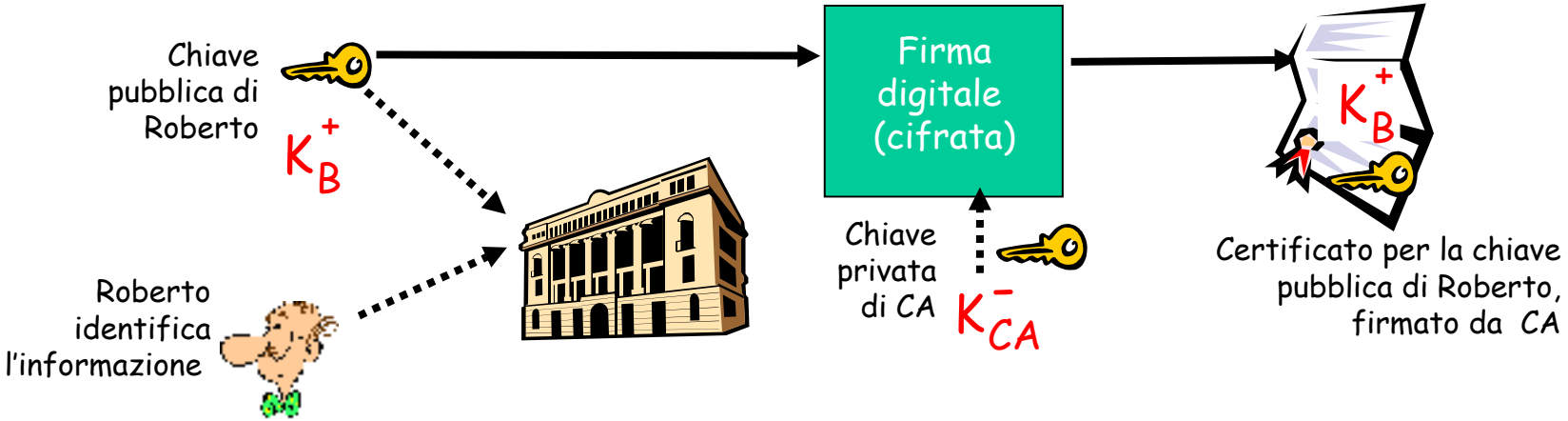
- Quando Alice riceve la chiave pubblica di Roberto (attraverso un dischetto, il sito web o via e-mail), come fa a sapere che è veramente la chiave pubblica di Roberto e non, magari, quella dell'intruso?

Soluzione:

- Autorità di certificazione (*CA*, *certification authority*)

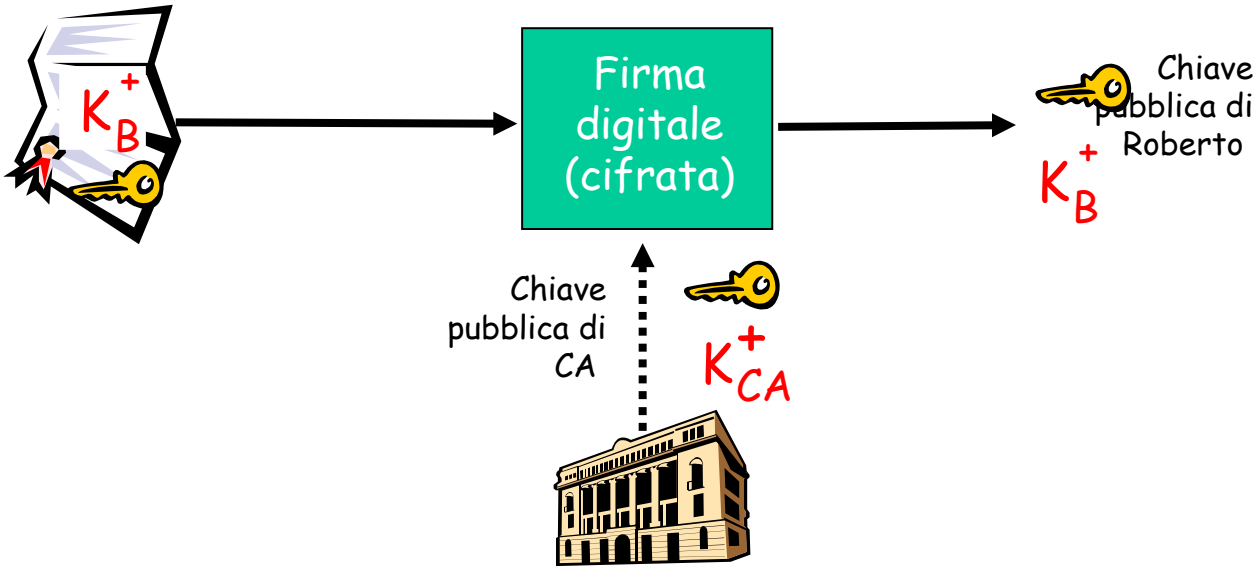
Autorità di certificazione

- Autorità di certificazione (CA): collega una chiave pubblica a una particolare entità, E.
- E (persona fisica, router) registra la sua chiave pubblica con CA.
  - E fornisce una "prova d'identità" a CA.
  - CA crea un certificato che collega E alla sua chiave pubblica.
  - Il certificato contiene la chiave pubblica di E con firma digitale di CA (CA dice "questa è la chiave pubblica di E")



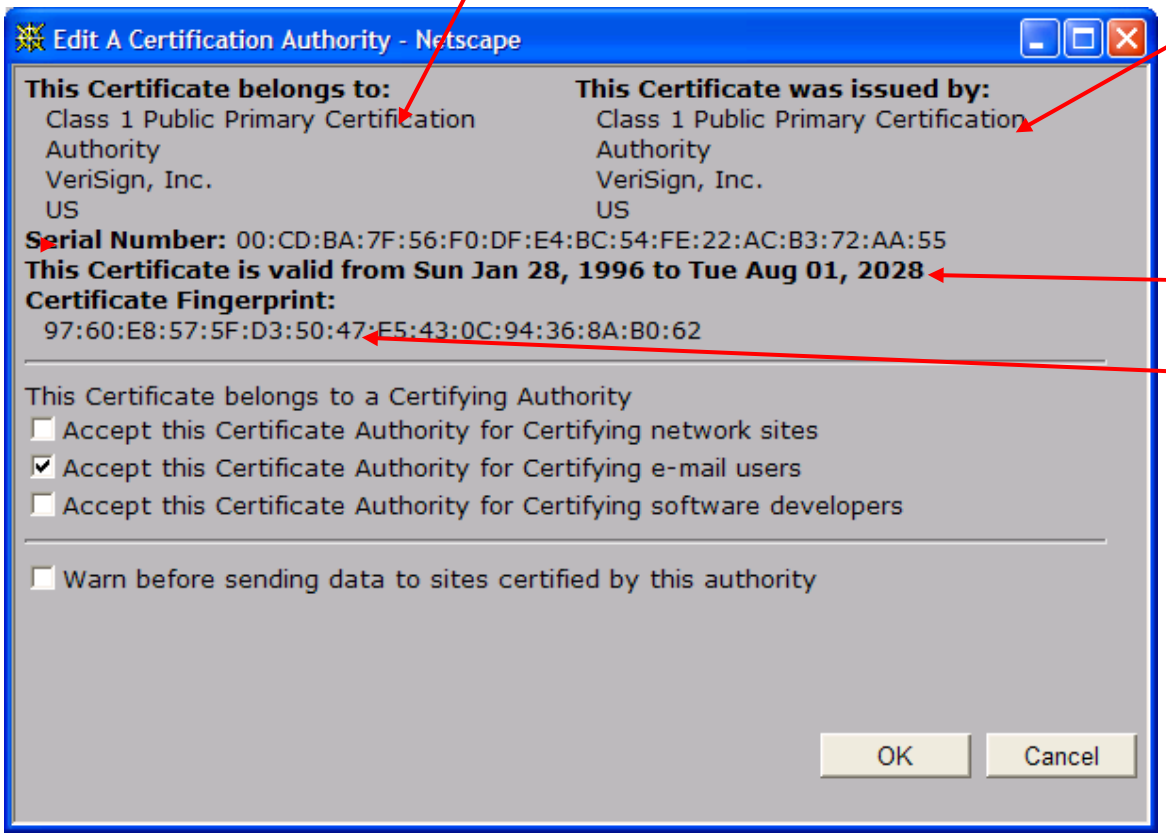
Autorità di certificazione

- Quando Alice vuole la chiave pubblica di Roberto:
  - prende il certificato di Roberto
  - applica la chiave pubblica di CA al certificato pubblico di Roberto e ottiene la chiave pubblica di Roberto



Un certificato contiene:

- Numero di serie
- Informazioni sul titolare, compreso l'algoritmo e il valore della chiave (non illustrato)
- Informazioni su chi ha emesso il certificato
- Date valide
- Firma digitale di chi lo ha emesso



Capitolo 8 La sicurezza nelle reti

8.1 Sicurezza di rete

8.2 Principi di crittografia

8.3 Integrità dei messaggi

8.4 Autenticazione end-to-end

8.5 rendere sicura la posta elettronica

8.6 Rendere sicure le connessioni TCP: SSL

8.9 Sicurezza operativa: firewall e sistemi di rilevamento delle intrusioni

Autenticazione

Obiettivo: Roberto vuole che Alice gli "dimostri" la sua identità

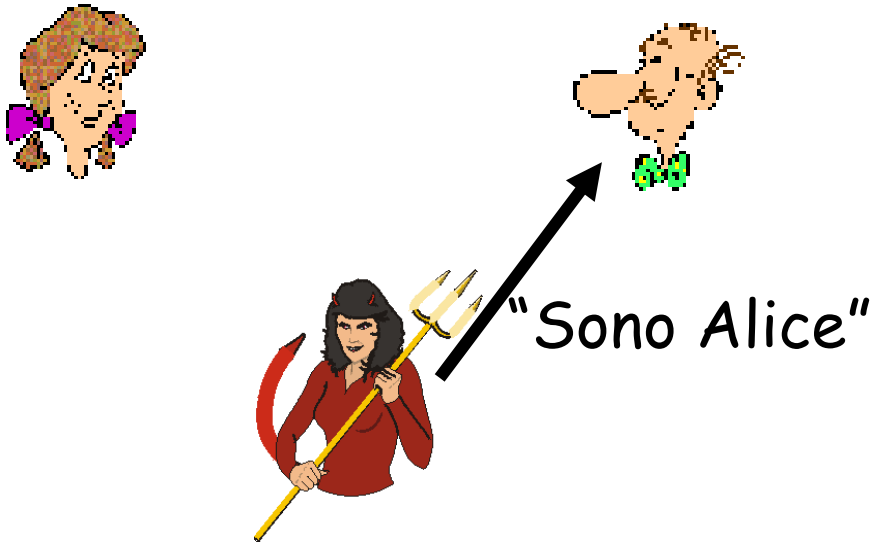
Protocollo ap1.0: Alice dice "Sono Alice"

Scenario con fallimento??

Autenticazione

Obiettivo: Roberto vuole che Alice gli "dimostri" la sua identità

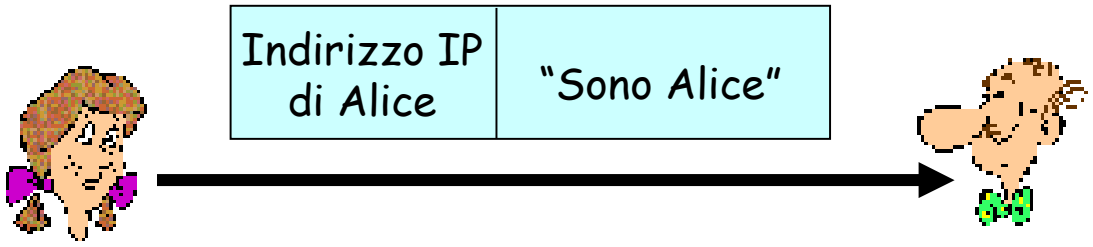
Protocollo ap1.0: Alice dice "Sono Alice"



in una rete, Roberto non può "vedere" Alice, e l'intruso può semplicemente autenticarsi come Alice

Autenticazione: un altro tentativo

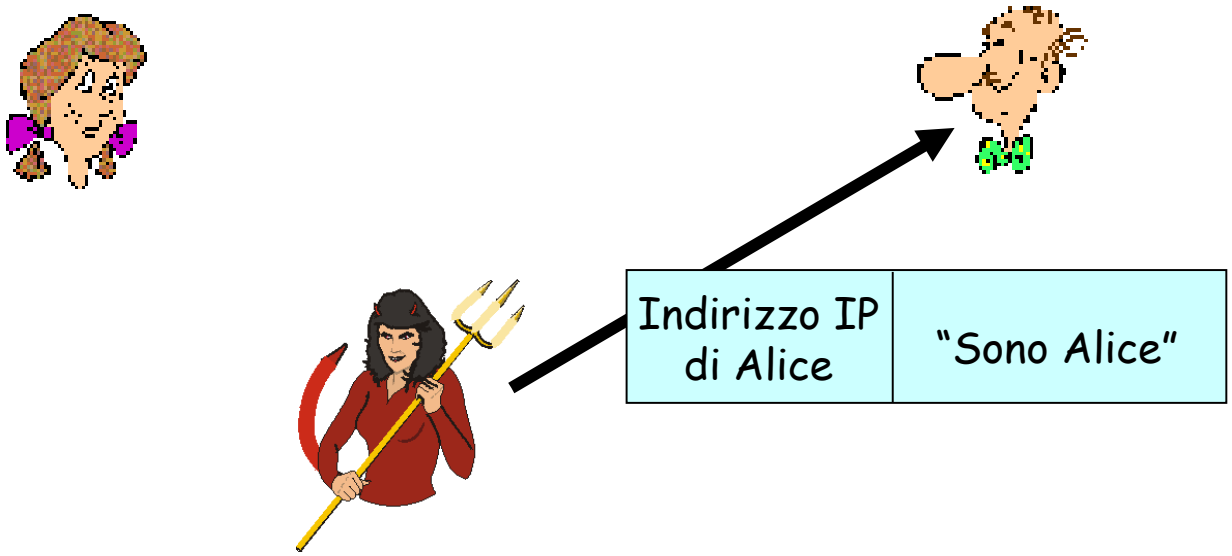
Protocollo ap2.0: Alice dice "Sono Alice" in un pacchetto IP che contiene il suo indirizzo IP sorgente



Scenario con fallimento??

Autenticazione: un altro tentativo

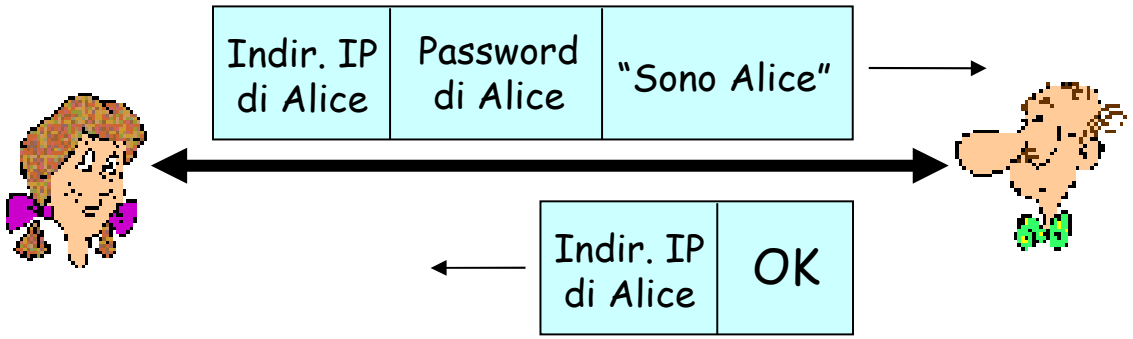
Protocollo ap2.0: Alice dice "Sono Alice" in un pacchetto IP che contiene il suo indirizzo IP sorgente



L'intruso può creare un pacchetto che imita l'indirizzo di Alice (spoofing)

Autenticazione: un altro tentativo

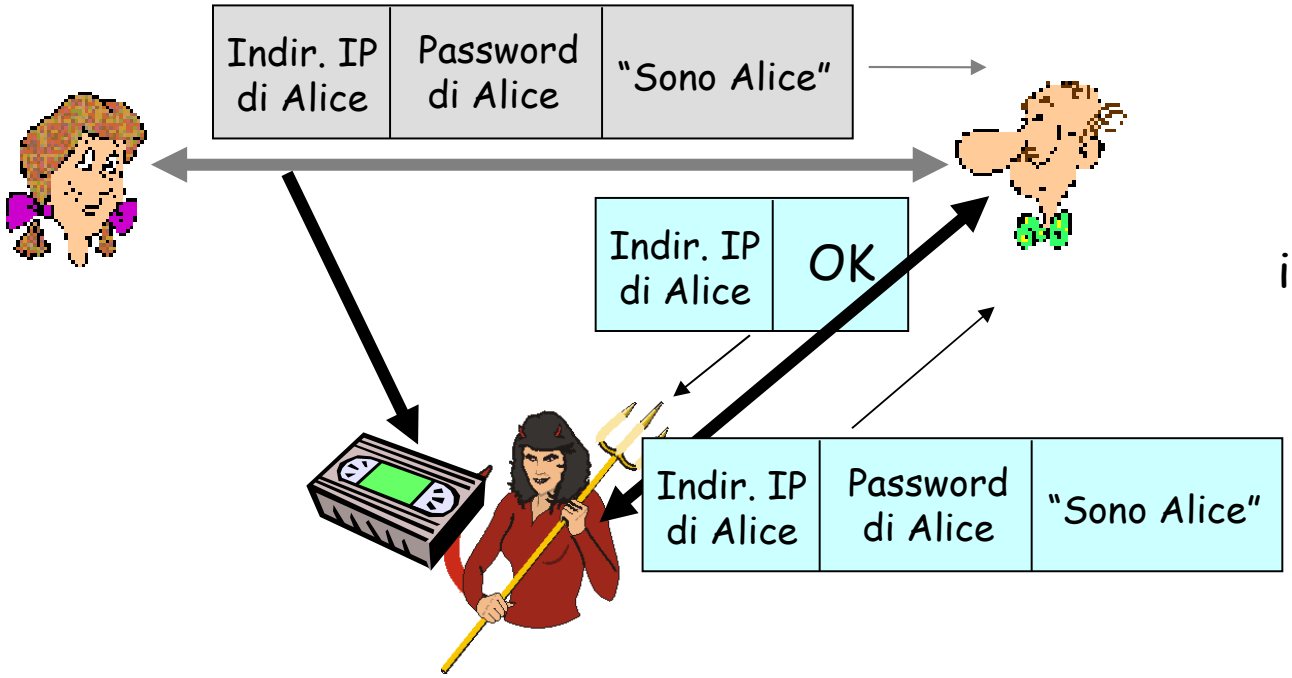
Protocollo ap3.0: Alice dice "Sono Alice" e invia la sua password segreta per "dimostrarlo"



Scenario con fallimento??

Autenticazione: un altro tentativo

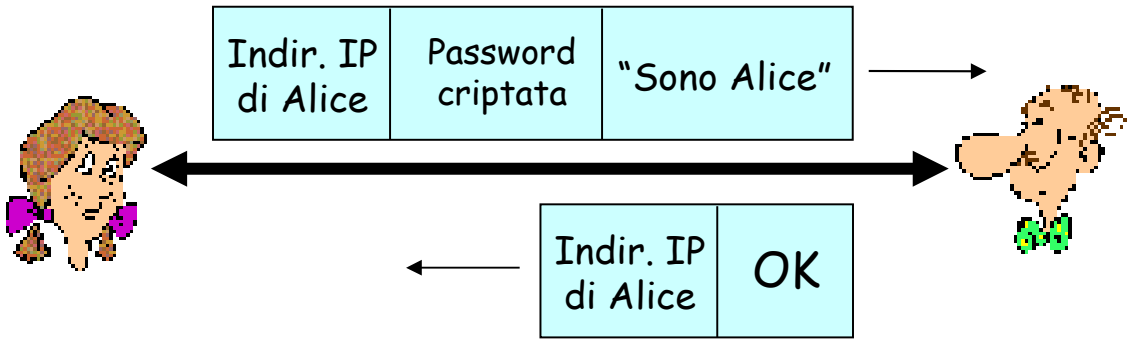
Protocollo ap3.0: Alice dice "Sono Alice" e invia la sua password segreta per "dimostrarlo"



attacco di replica: L'intruso registra il pacchetto di Alice e lo riproduce successivamente trasmettendolo a Roberto

Autenticazione: ancora un altro tentativo

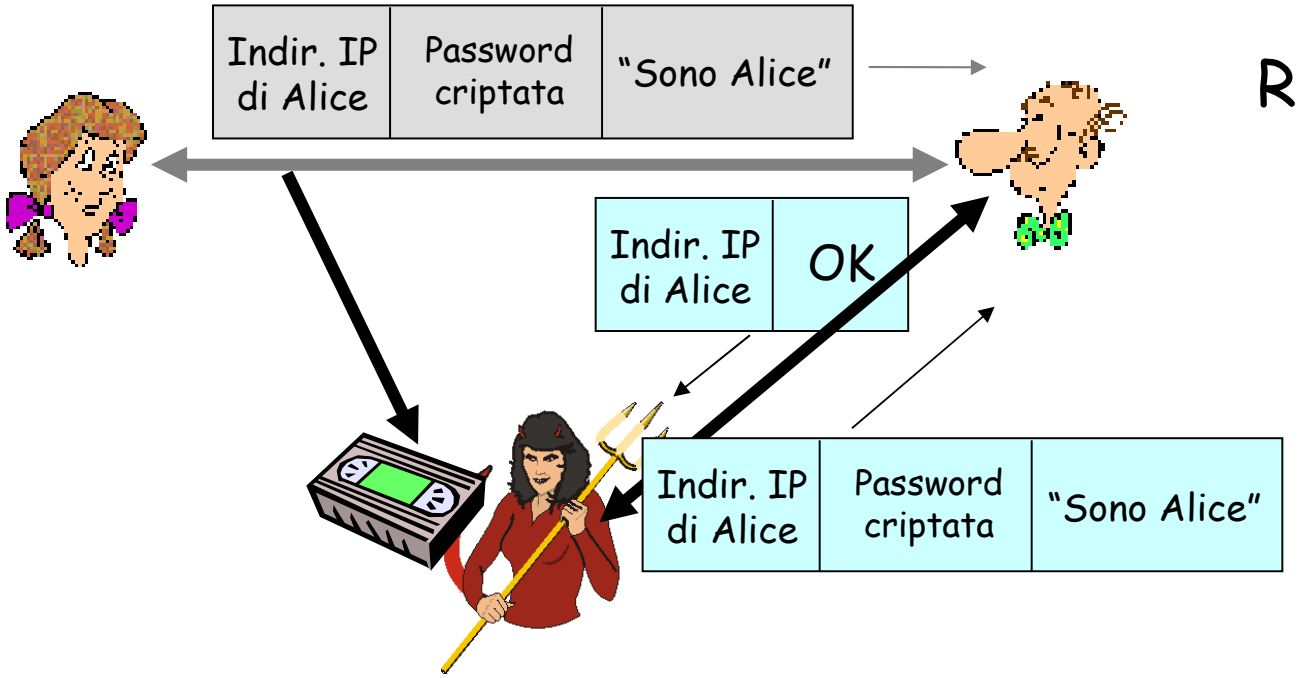
Protocollo ap3.1: Alice dice "Sono Alice" e invia la sua password segreta criptata per "dimostrarlo".



Scenario con fallimento??

Autenticazione: ancora un altro tentativo

Protocollo ap3.1: Alice dice "Sono Alice" e invia la sua password segreta criptata per "dimostrarlo".



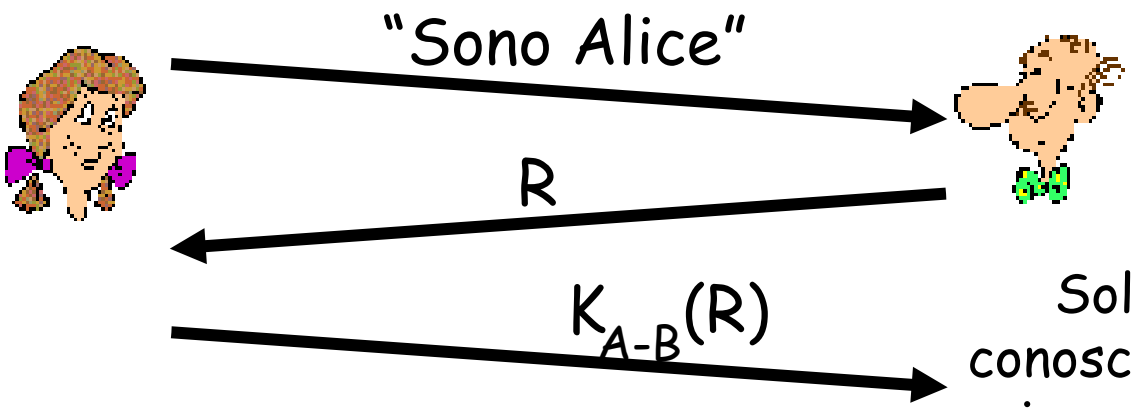
Registrazione e riproduzione funzionano ancora!

Autenticazione: ancora un altro tentativo

Obiettivo: evitare un attacco di replica (*playback attack*)

Nonce: è un numero (R) che verrà usato *soltanto una volta*.

Protocollo ap4.0: Alice manda il messaggio "Sono Alice", Roberto sceglie e manda ad Alice un nonce, R.
Alice reinvia il nonce R, criptato utilizzando la chiave simmetrica segreta.



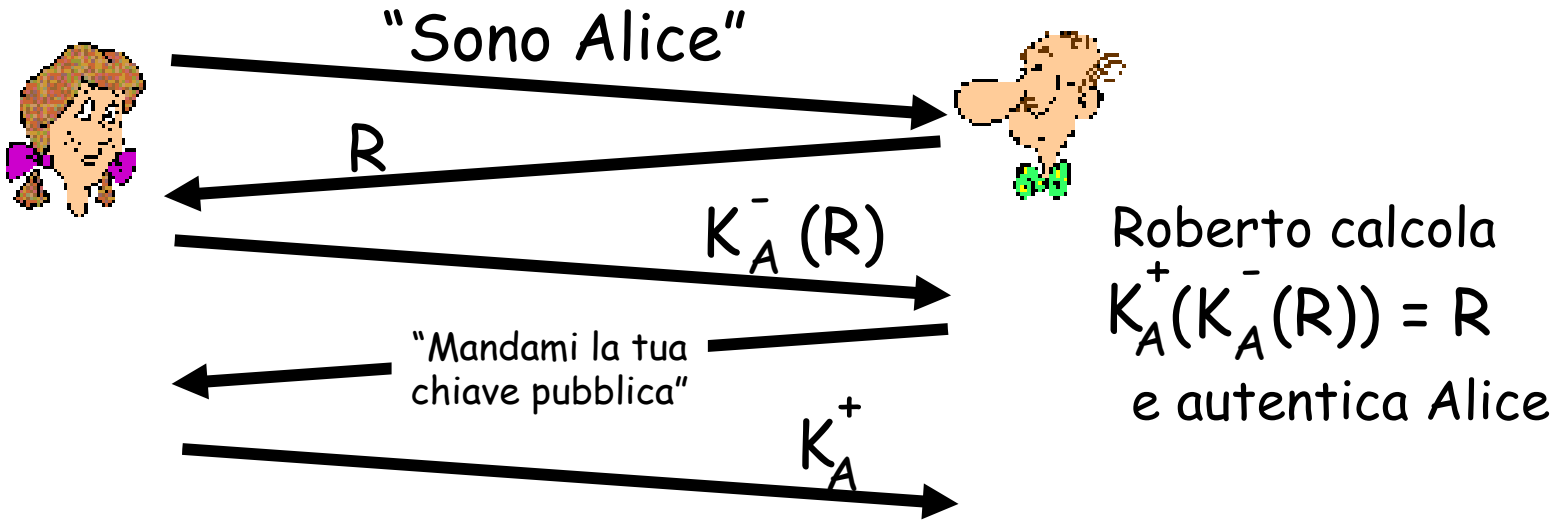
Attacco fallito?

Autenticazione: protocollo *ap.5.0*

Nel protocollo ap4.0 è stato usato un nonce e la crittografia a chiave simmetrica

- Si può utilizzare la crittografia a chiave pubblica?

Protocollo ap5.0: usa un nonce e la crittografia a chiave pubblica



Protocollo *ap.5.0* : un buco nella sicurezza

Attacco man-in-the-middle: l'intruso si finge Alice (nei confronti di Roberto) e si finge Roberto (nei confronti di Alice)

Sono Alice

Sono Alice

R

$K_T^-(R)$

R

$K_A^-(R)$

Mandami la tua chiave pubblica

K_T^+

Mandami la tua chiave pubblica

K_A^+

$K_T^+(m)$

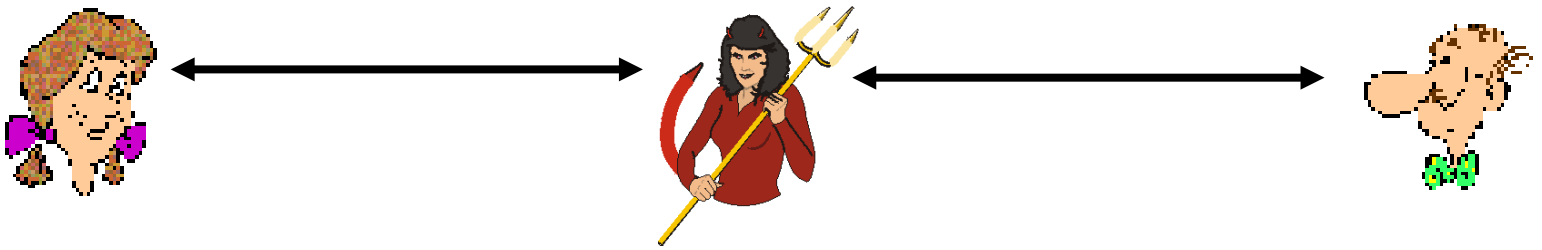
L'intruso decifra
$m = K_T^-(K_T^+(m))$
e invia m ad
Alice criptato
con la chiave
pubblica di Alice

$K_A^+(m)$

$m = K_A^-(K_A^+(m))$

Protocollo *ap.5.0* : un buco nella sicurezza

Attacco man-in-the-middle: l'intruso si finge Alice (nei confronti di Roberto) e si finge Roberto (nei confronti di Alice)



Difficile da individuare:

- Roberto riceve sempre tutti messaggi di Alice, e viceversa (e quindi nulla li fa sospettare di un'intromissione)
- Il problema è che anche l'intruso riceve benissimo tutti i messaggi!

Capitolo 8 La sicurezza nelle reti

8.1 Sicurezza di rete

8.2 Principi di crittografia

8.3 Integrità dei messaggi

8.4 Autenticazione end-to-end

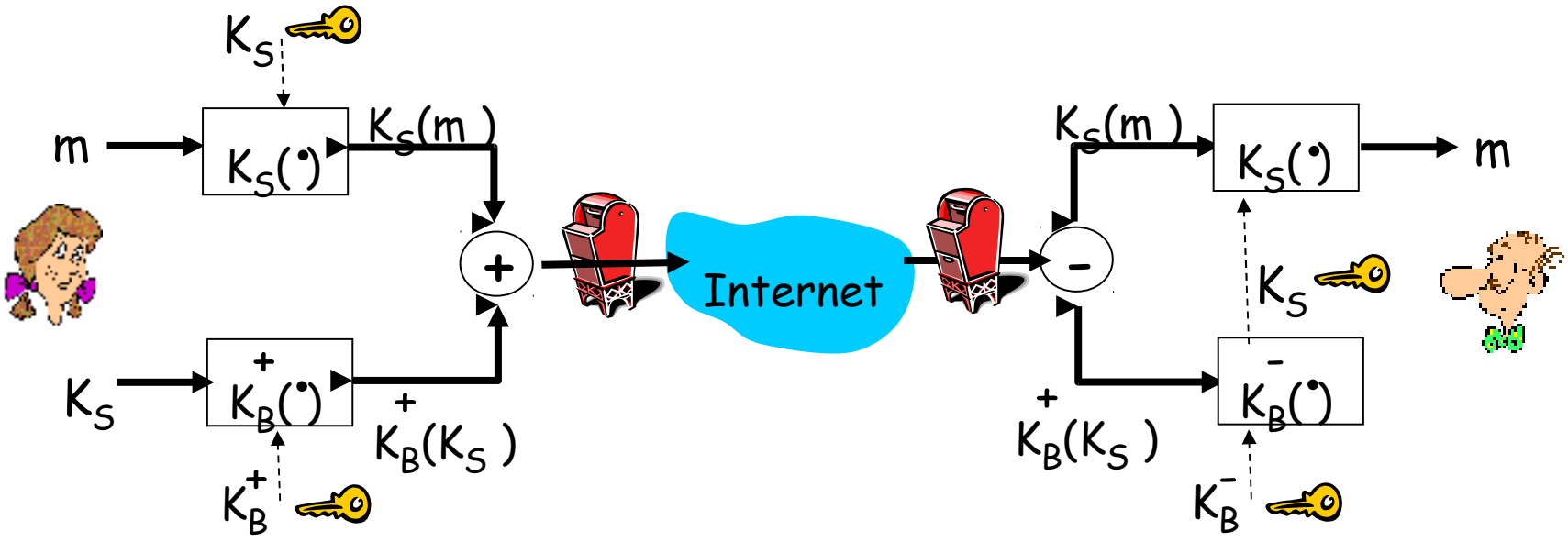
8.5 Rendere sicura la posta elettronica

8.6 Rendere sicure le connessioni TCP: SSL

8.9 Sicurezza operativa: firewall e sistemi di rilevamento delle intrusioni

E-mail sicure

- Alice vuole inviare un messaggio e-mail riservato, m, a Roberto.

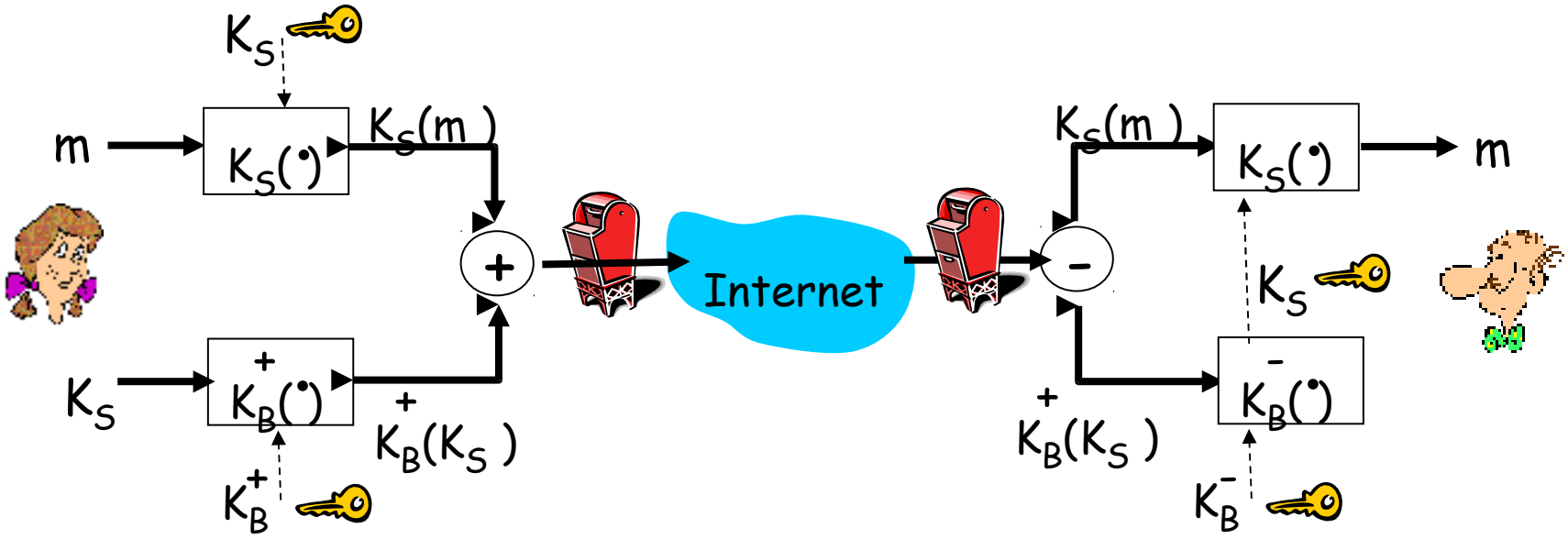


Alice:

- crea una chiave simmetrica privata, K_S.
- codifica il messaggio con K_S.
- codifica K_S con la chiave pubblica di Roberto.
- invia $K_S(m)$ e $K^+_B(K_S)$ a Roberto.

E-mail sicure

- Alice vuole inviare un messaggio e-mail riservato, m, a Roberto.

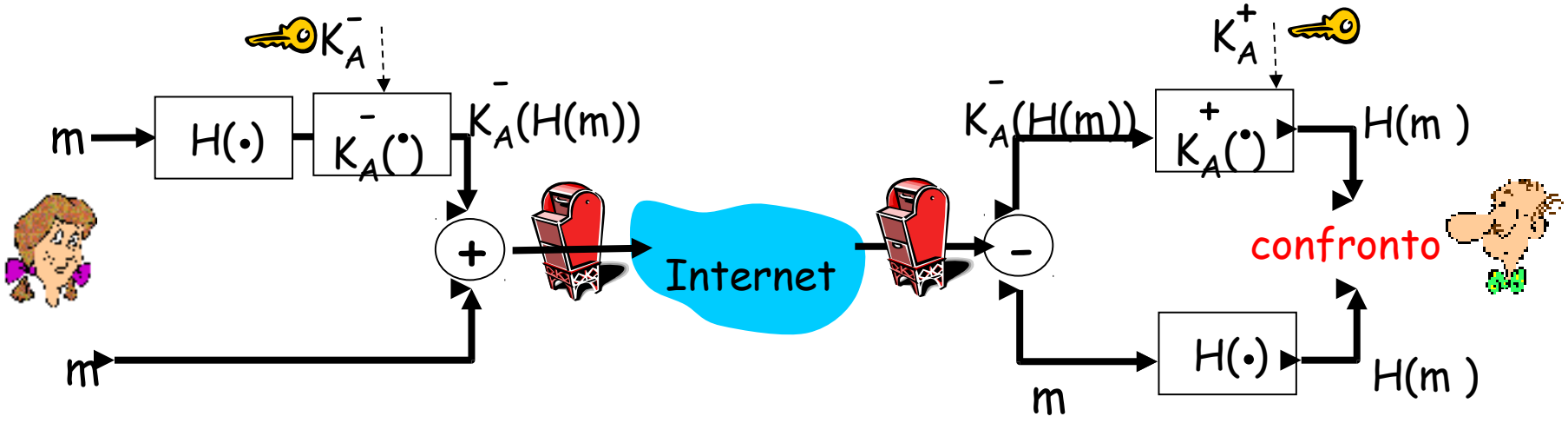


Roberto:

- utilizza la sua chiave privata per ottenere la chiave simmetrica K_S
- utilizza K_S per decodificare $K_S(m)$ e ottiene m.

E-mail sicure (continua)

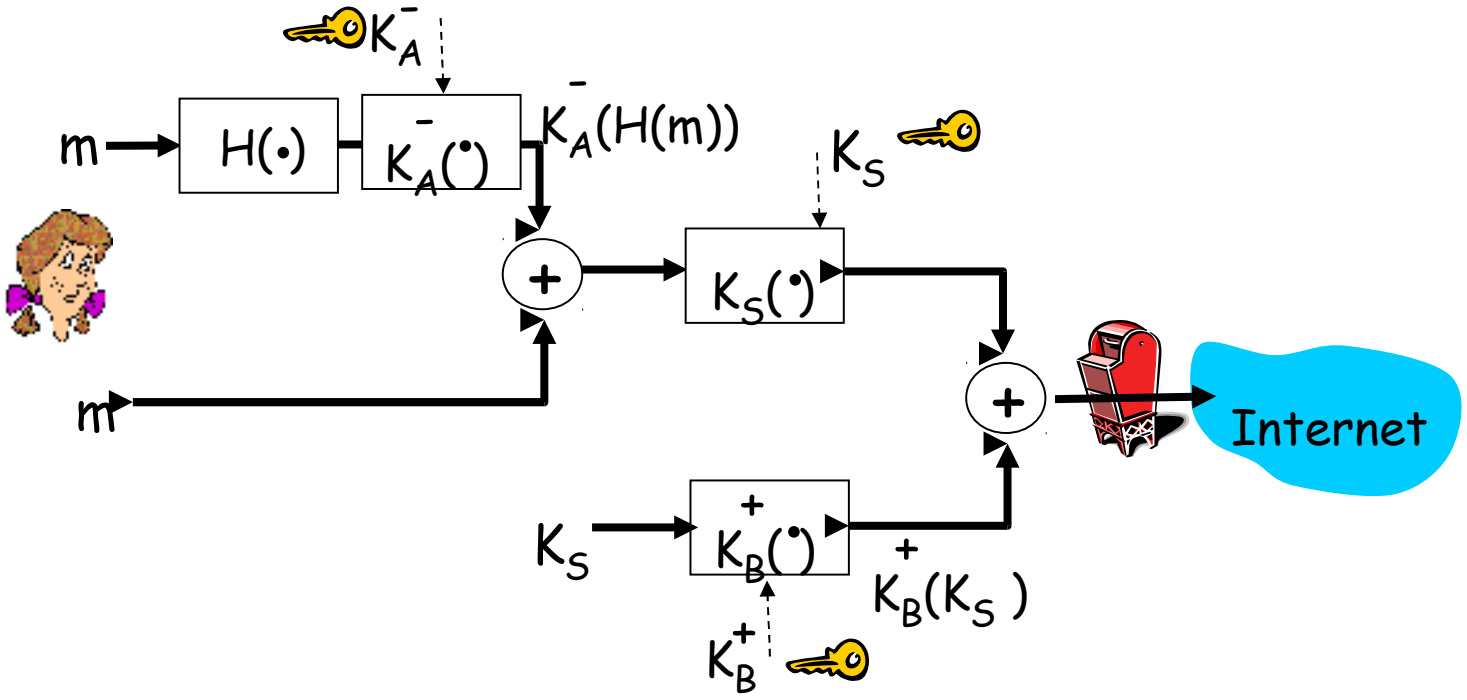
• Alice vuole essere sicura dell'integrità del messaggio e dell'autenticazione del mittente.



• Alice firma digitalmente il messaggio.
• Invia il messaggio (in chiaro) e la firma digitale.

E-mail sicure (continua)

- Alice vuole ottenere segretezza, autenticazione del mittente e integrità del messaggio.



Alice usa tre chiavi: la sua chiave privata, la chiave pubblica di Roberto e la chiave simmetrica appena generata.

PGP (*Pretty good privacy*)

- Schema di cifratura per la posta elettronica che è diventato uno standard.
- Usa chiavi simmetriche di crittografia, chiavi pubbliche, funzioni hash e firme digitali.
- Assicura sicurezza, integrità del messaggio e autenticazione del mittente.
- L'inventore, Phil Zimmerman, fu indagato per tre anni dai servizi federali.

Messaggio PGP firmato:

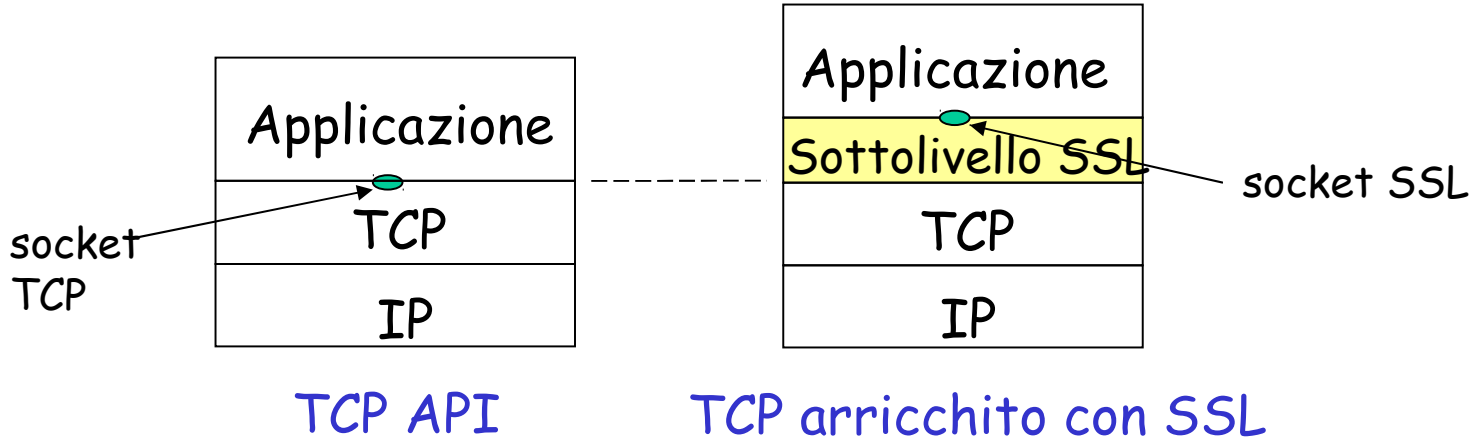
```
---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1

Bob:My husband is out of town
   tonight.Passionately yours,
   Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3mqJh
   FEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

Capitolo 8 La sicurezza nelle reti

8.1 Sicurezza di rete
8.2 Principi di crittografia
8.3 Integrità dei messaggi
8.4 Autenticazione end-to-end
8.5 Rendere sicura la posta elettronica
8.6 Rendere sicure le connessioni TCP: SSL
8.9 Sicurezza operativa: firewall e sistemi di rilevamento delle intrusioni

Livello di socket sicura (SSL)

- Costituisce la base del protocollo di sicurezza a livello di trasporto.
  - Ampiamente utilizzato nelle transazioni commerciali e finanziarie su Internet (shttp)
- Servizi di sicurezza:
  - Autenticazione del server, cifratura dei dati, autenticazione del client (opzionale)

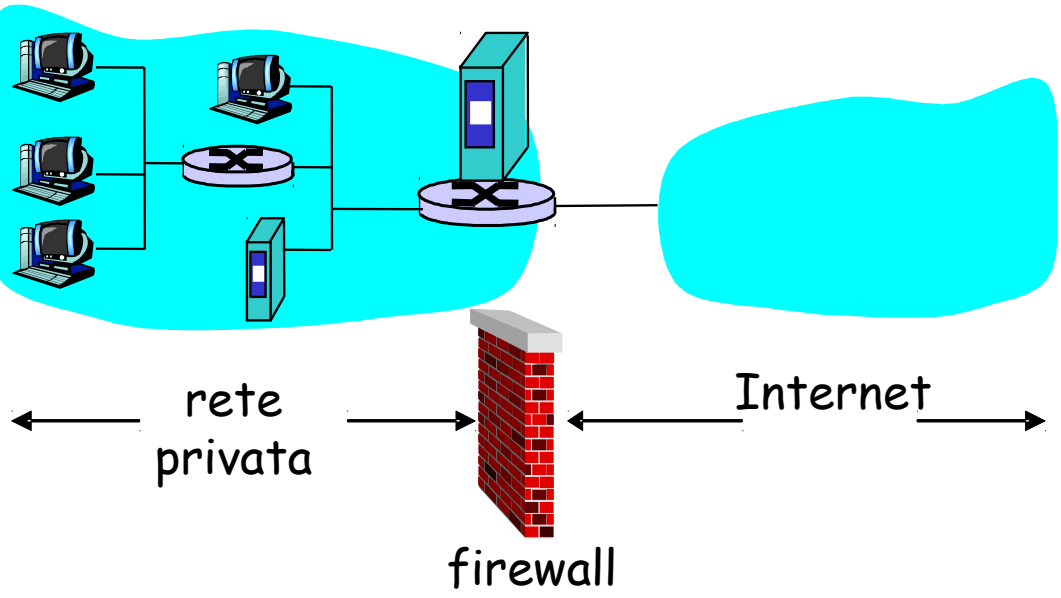


Capitolo 8 La sicurezza nelle reti

8.1 Sicurezza di rete
8.2 Principi di crittografia
8.3 Integrità dei messaggi
8.4 Autenticazione end-to-end
8.5 Rendere sicura la posta elettronica
8.6 Rendere sicure le connessioni TCP: SSL
8.9 Sicurezza operativa: firewall e sistemi di rilevamento delle intrusioni

Firewall

Struttura hardware e software che separa una rete privata dal resto di Internet e consente all'amministratore di controllare e gestire il flusso di traffico tra il mondo esterno e le risorse interne.



Firewall: perché

Prevenire attacchi di negazione del servizio:

- SYN flooding: l'intruso stabilisce molte connessioni TCP fasulle per non lasciare risorse alle connessioni "vere".

Prevenire modifiche/accessi illegali ai dati interni.

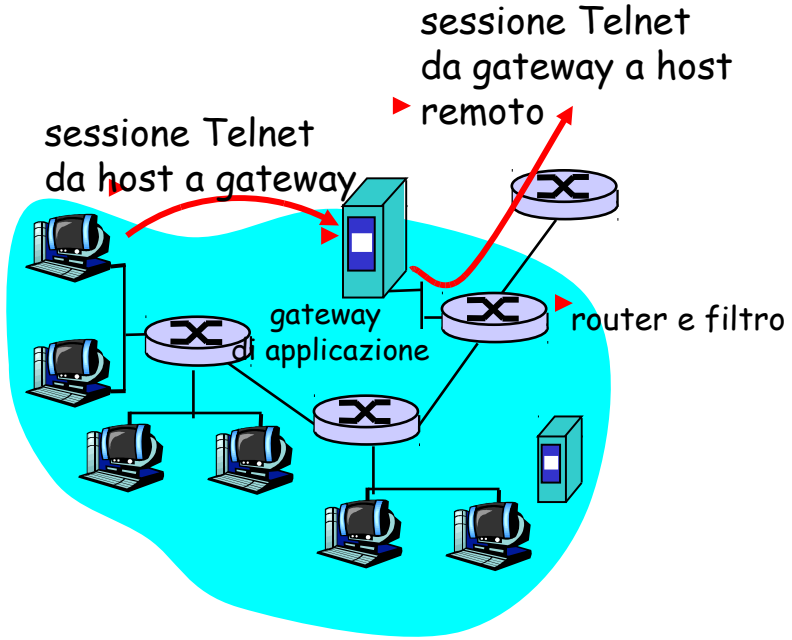
- es., l'intruso può sostituire l'homepage del MIUR con qualcos'altro.

Consentire solo accessi autorizzati all'interno della rete (una serie di utenti/host autenticati)

Tre tipi di firewall:

- A filtraggio dei pacchetti
- A filtraggio dei pacchetti con memoria dello stato
- A livello di applicazione (gateway)

Gateway



- Il filtraggio dei pacchetti consente di effettuare un controllo sulle intestazioni IP e TCP/UDP.
- Esempio: permette ai client interni (autorizzati) le connessioni Telnet ma impedisce il contrario.

1. Tutte le connessioni Telnet verso l'esterno devono passare attraverso il gateway.
2. Il gateway non solo concede l'autorizzazione all'utente ma smista anche le informazioni fra l'utente e l'host.
3. La configurazione del filtro del router blocca tutti i collegamenti eccetto quelli che riportano l'indirizzo IP del gateway.

Limiti di firewall e gateway

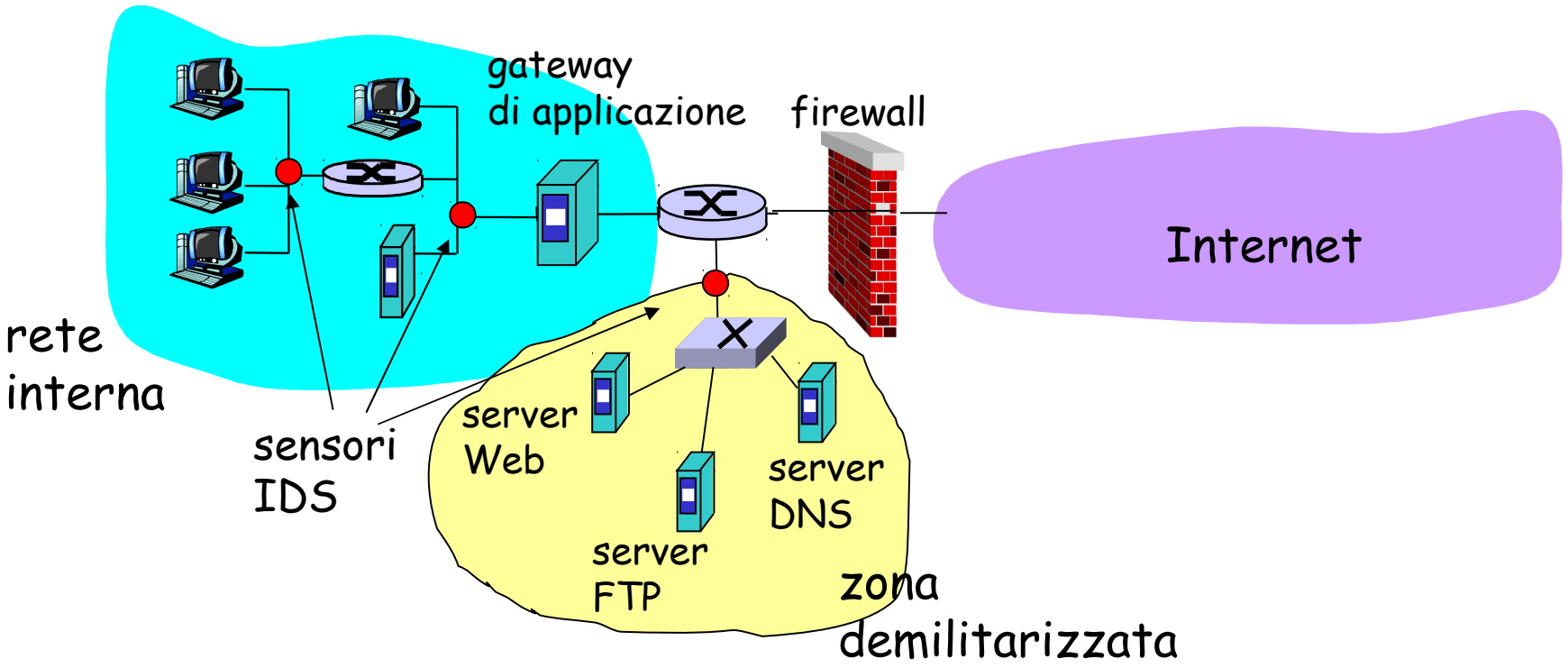
- IP spoofing: azione utilizzata per nascondere la vera identità dell'aggressore.
- Se più applicazioni necessitano di un trattamento speciale, ciascuna avrà il suo gateway di applicazione.
- Il software del client deve sapere come contattare il gateway.
  - Es. deve impostare l'indirizzo IP del proxy nel browser Web.
- Spesso sono configurati secondo una politica "intransigente" senza vie di mezzo, per esempio inibendo tutto il traffico UDP.
- Compromesso: grado di comunicazione con il mondo esterno/livello di sicurezza
- Numerosi siti con protezioni elevate sono ancora soggetti ad attacchi.

Sistemi di rilevamento delle intrusioni

- filtraggio dei pacchetti:
  - funziona solo sulle intestazioni TCP/IP
  - nessun controllo di correlazione fra le sessioni
- IDS: *intrusion detection system*
  - *Rileva un'ampia gamma di attacchi:* guarda il contenuto dei pacchetti
  - Esamina le correlazioni among multiple packets
    - Scansione delle porte
    - Scansione della pila TCP
    - Attacchi DoS

Sistemi di rilevamento delle intrusioni

- Molteplici sistemi di rilevamento delle intrusioni: differenti tipi di controllo in punti diversi



La sicurezza nelle reti (riassunto)

Tecniche di base...

- Crittografia (simmetrica e pubblica)
- Autenticazione
- Integrità del messaggio
- Distribuzione di chiavi

... usate nei diversi scenari di sicurezza

- E-mail sicure
- Livello di socket sicura (SSL)

Sicurezza operativa: firewall e IDS