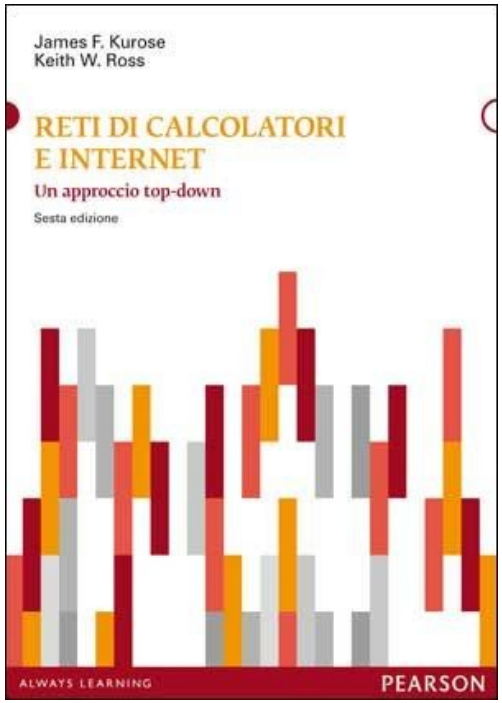
Capitolo 8
La sicurezza nelle reti



Reti di calcolatori e Internet: Un approccio top-down

6ª edizione
Jim Kurose, Keith Ross

Pearson Paravia Bruno Mondadori Spa
©2012_

Nota per l'utilizzo:

Abbiamo preparato queste slide con l'intenzione di renderle disponibili a tutti (professori, studenti, lettori). Sono in formato PowerPoint in modo che voi possiate aggiungere e cancellare slide (compresa questa) o modificarne il contenuto in base alle vostre esigenze.
Come potete facilmente immaginare, da parte nostra abbiamo fatto *un sacco* di lavoro. In cambio, vi chiediamo solo di rispettare le seguenti condizioni:

- se utilizzate queste slide (ad esempio, in aula) in una forma sostanzialmente inalterata, fate riferimento alla fonte (dopo tutto, ci piacerebbe che la gente usasse il nostro libro!)
- se rendete disponibili queste slide in una forma sostanzialmente inalterata su un sito web, indicate che si tratta di un adattamento (o che sono identiche) delle nostre slide, e inserite la nota relativa al copyright.

Thanks and enjoy! JFK/KWR

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:
  - Sicurezza a seconda dello specifico livello (applicazione, trasporto, rete o collegamento)
  - Firewall e sistemi per la rilevazione degli intrusi

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
8.7 Sicurezza a livello di rete: IPSec
8.8 Sicurezza nelle LAN wireless
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
- Decifrare il messaggio ricevuto

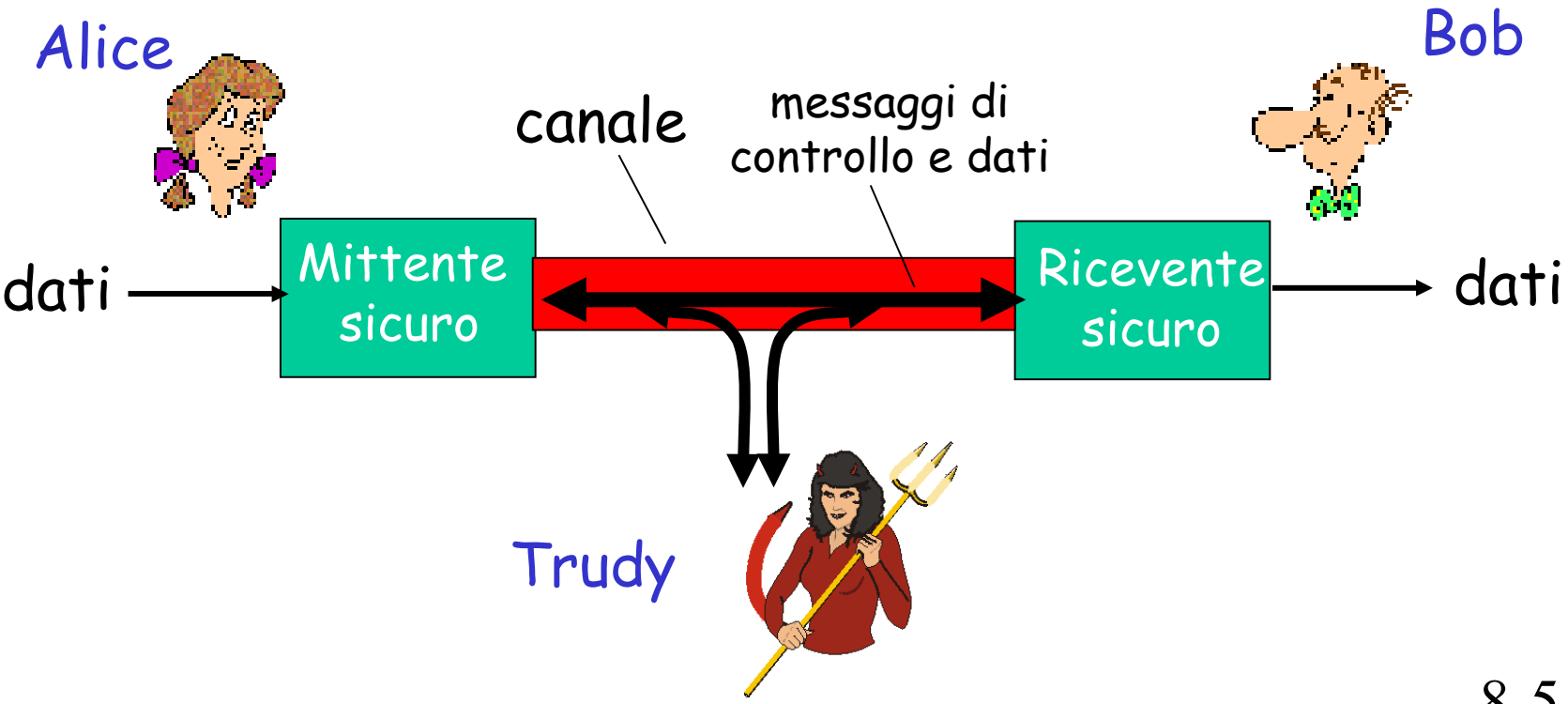
Autenticazione: mittente e destinatario devono essere sicuri della loro identità

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 Tommaso

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



Chi sono Alice e Roberto?

Nella vita reale Alice e Bob 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!

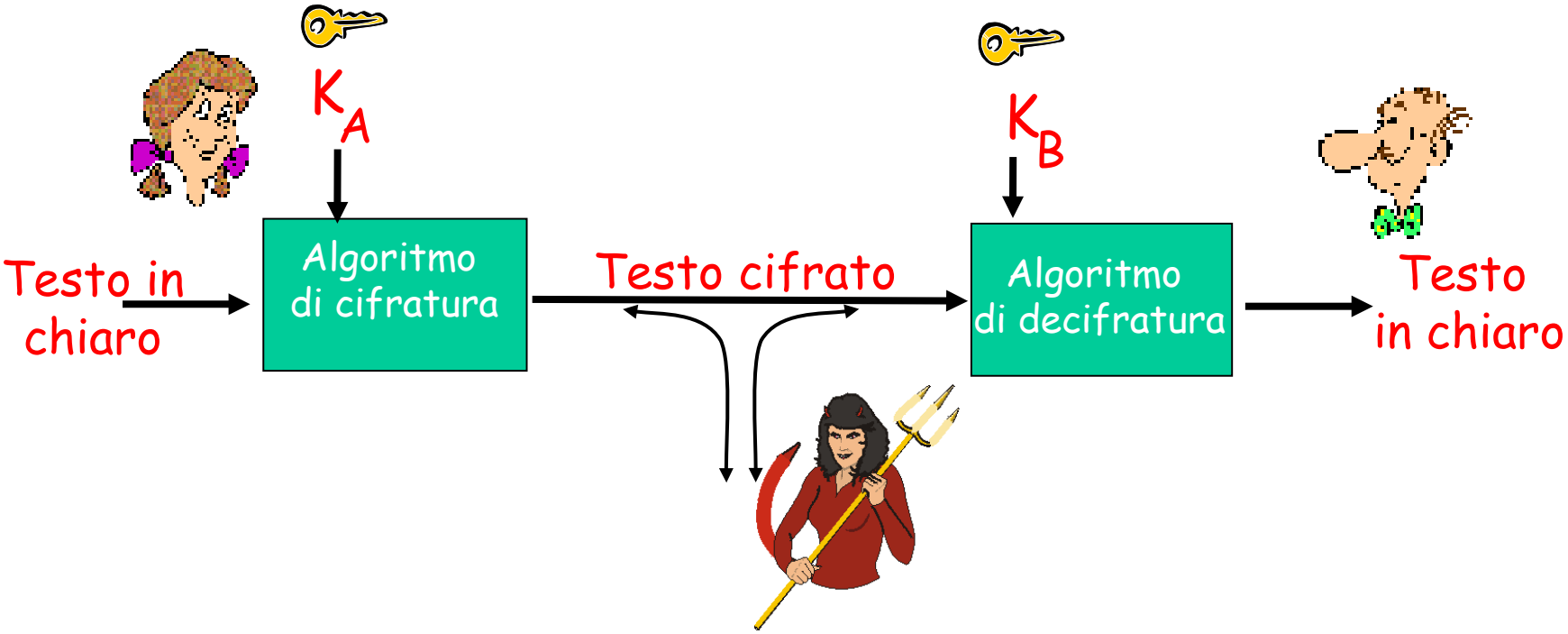
- *spiare:* intercettare i messaggi
- *aggiungere* messaggi e sovraccaricare il sistema
- *impersonare* un altro soggetto
- *dirottare* una sessione in corso e sostituirsi al mittente o al destinatario
- *negare il servizio*

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
8.7 Sicurezza a livello di rete: IPSec
8.8 Sicurezza nelle LAN wireless
8.9 Sicurezza operativa: firewall e sistemi di rilevamento delle intrusioni

Principi di crittografia

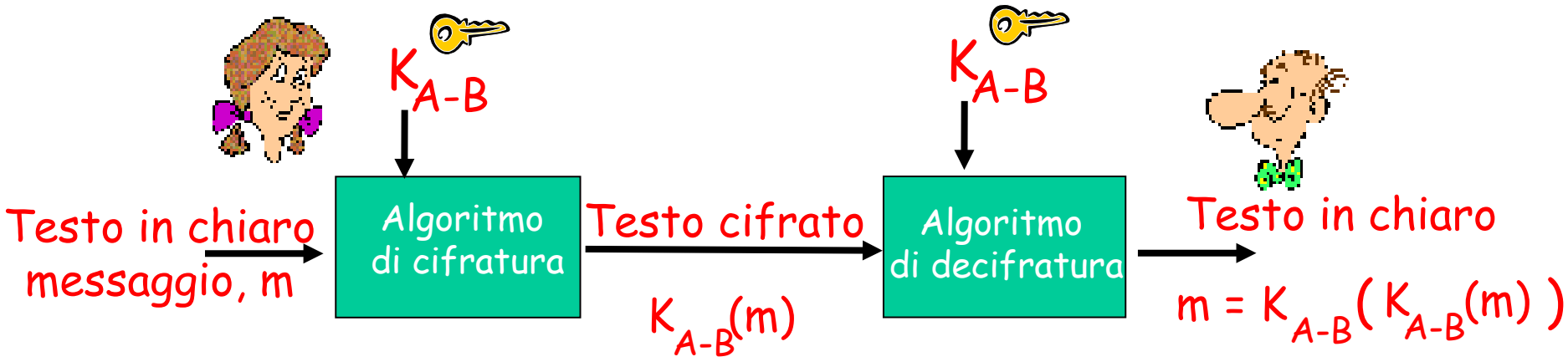


m messggio in chiaro

$K_A(m)$ messaggio cifrato con la chiave *A*

$m=K_B(K_A(m))$

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?

Semplice schema di cifratura

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

```
Lettere in chiaro:   abcdefghijklmnopqrstuvwxyz
                      ↓                       ↓
Lettere cifrate:     mnbvcxzasdfghjklpoiuytrewq
```

esempio

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

Chiave di cifratura: sequenza di lettere cifrate

Schema di cifratura più complesso

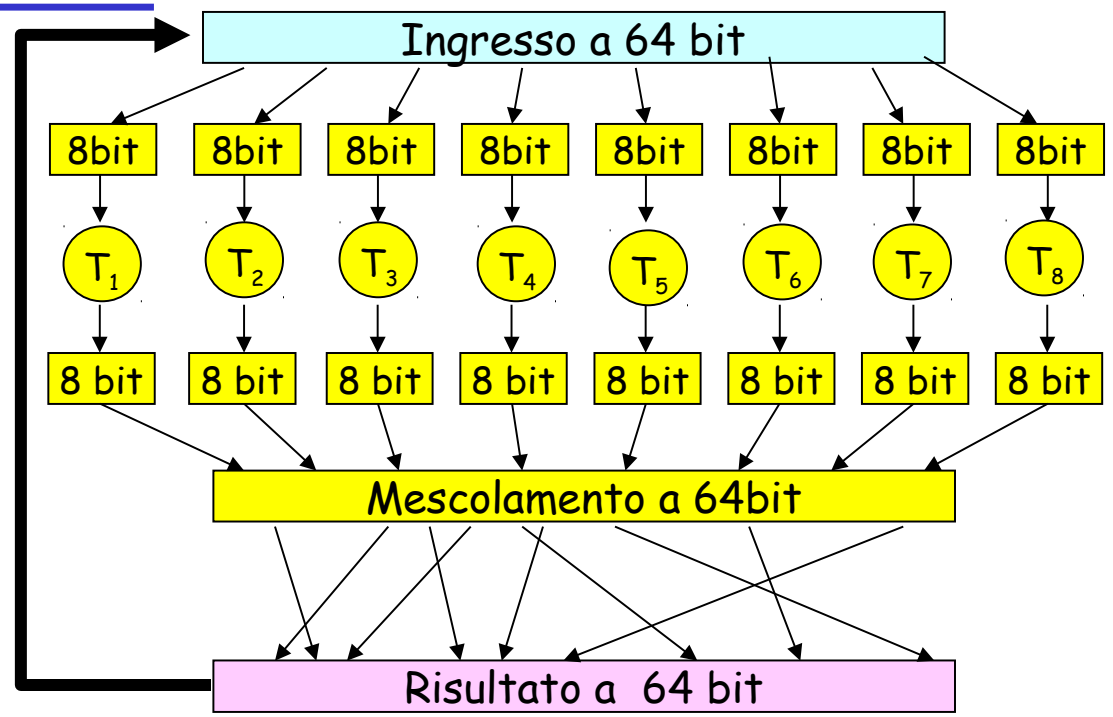
- n cifrari a sostituzione, $M_1, M_2, \ldots, M_n$
- Utilizzo cicliclo:
  - Esempio., n=4: M_1, M_3, M_4, M_3, M_2; M_1, M_3, M_4, M_3, M_2; ..
- Per ogni nuovo simbolo, usare il successivo schema di sostituzione nel ciclo
- dog: d da M_1, o da M_3, g da M_4

Chiave di cifratura: n cifrari a sostituzione e lo schema del ciclo

Violare un sistema di cifratura

- Attacchi con solo testo cifrato:
  Tommaso ha del testo cifrato che vuole analizzare.
- Due approcci:
  - Forza bruta: cercare tutte le chiavi
  - Analisi statistica
- Testo in chiaro noto:
  Tommaso possiede del testo in chiaro corrispondente a quello cifrato
- Testo in chiaro scelto:
  Tommaso può ottenere del testo cifrato corrispondente al testo in chiaro da lui scelto.

Cifrario a blocchi

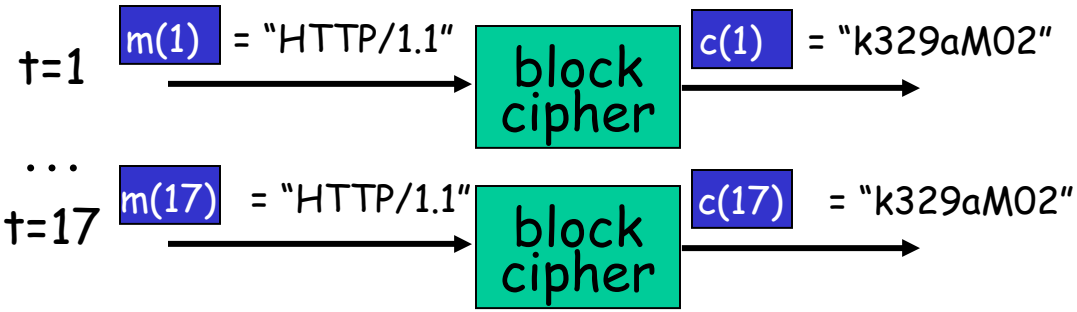


- Un bit in ingresso condiziona otto bit in uscita

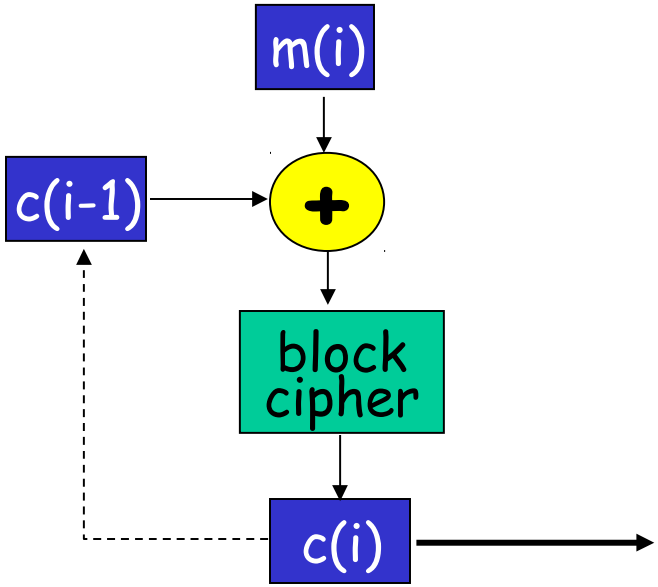
- Passaggi multipli: ciascun bit in ingresso condiziona tutti i bit in uscita
- comuni cifrari a blocchi: DES, 3DES, AES

Cipher Block Chaining

- Cifrario a blocchi: se un blocco in ingresso viene ripetuto, produrrà lo stesso testo cifrato.



- *Cipher block chaining:* Effettua un'operazione di XOR sull'*i*-esimo blocco in ingresso, m(i), con il precedente blocco di testo cifrato, c(i-1)
  - c(0) trasmesso in chiaro al ricevente
    - IV initialization vector
  - Cosa accade nello scenario "HTTP/1.1" qui a lato?



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

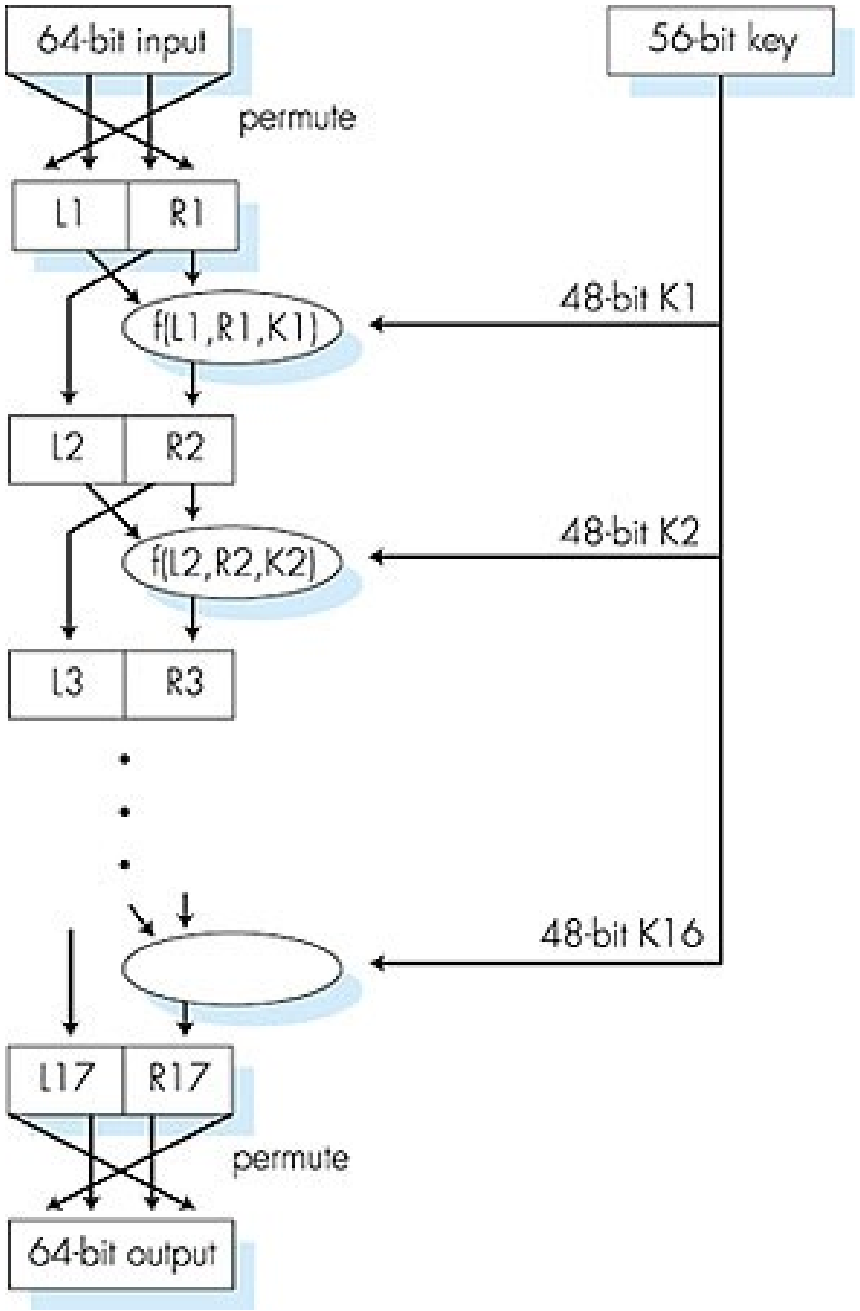
Crittografia a chiave simmetrica: DES

Operazioni base di DES

Permutazione iniziale

16 iterazioni intermedie identiche, ciascuna con 48 bit differenti come chiave

Permutazione finale



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
- Si stima che un calcolatore in grado di ricostruire una chiave DES a 56 bit in 1 sec impiegherebbe 149 miliardi di anni per violare una chiave AES a 128 bit.

Crittografia a chiave pubblica

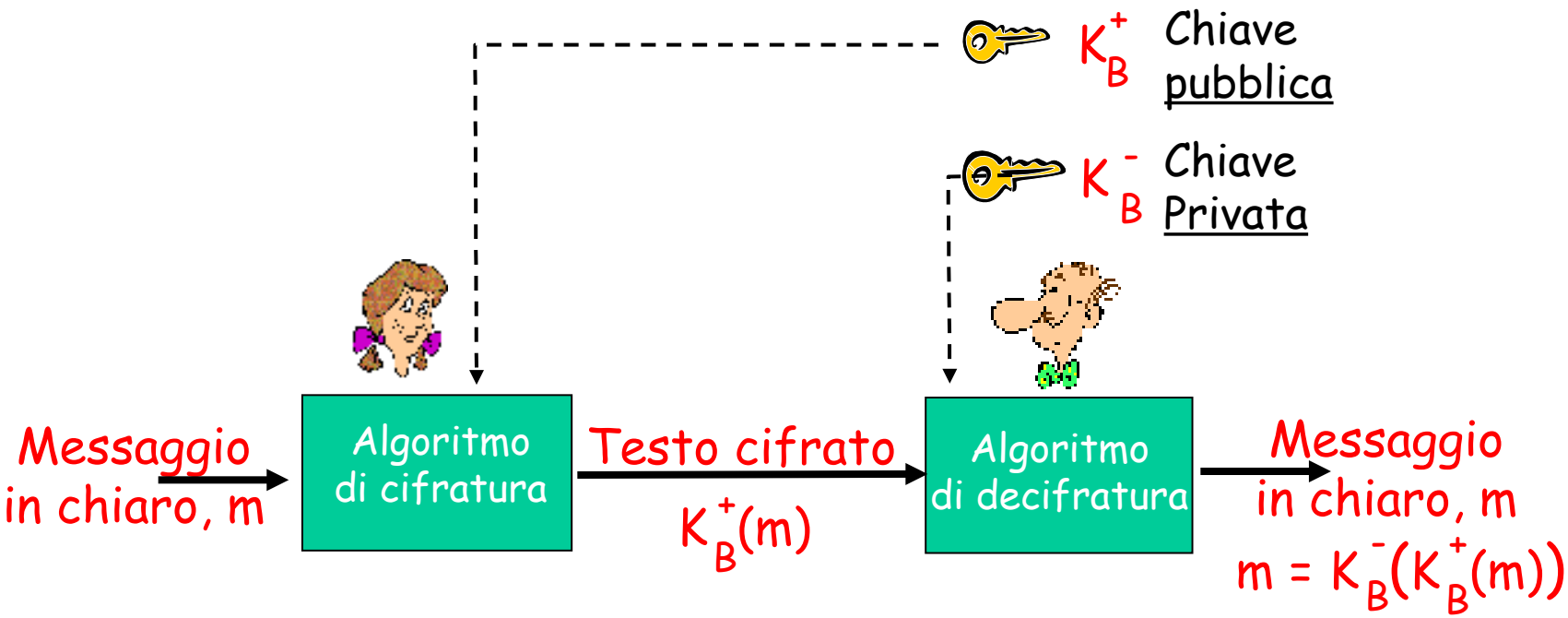
Crittografia a chiave simmetrica

- 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. $K_B^+(\cdot)$ e $K_B^-(\cdot)$ 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.

Prerequisiti: aritmetica modulare

- x mod n = resto della divisione di x per n
- fatti:

  [(a mod n) + (b mod n)] mod n = (a+b) mod n

  [(a mod n) - (b mod n)] mod n = (a-b) mod n

  [(a mod n) * (b mod n)] mod n = (a*b) mod n
- così

  $(a \bmod n)^d \bmod n = a^d \bmod n$
- Esempio: x=14, n=10, d=2: $(x \bmod n)^d \bmod n = 4^2 \bmod 10 = 6$ $x^d = 14^2 = 196$ $x^d \bmod 10 = 6$

RSA: preparazione

- messaggio: una qualunque sequenza di bit
- una sequenza di bit corrisponde ad un numero
- Pertanto, criptare un messaggio è equivalente a criptare un numero
- *Esempio*
  - m= 10010001 . Questo messaggio rappresenta il numero 145.
  - Per criptare m, criptiamo il numero 145 e otteniamo un nuovo numero, corrispondente al messaggio cifrato

RSA: scelta delle chiavi

1. Scegliere due numeri primi di valore elevato: *p*, *q*. (es.: 1024 bit ciascuno)

2. Calcolare $n = pq$, $z = (p-1)(q-1)$

3. Scegliere *e* (con $e < n$) tale che non abbia fattori in comune con z. (*e*, *z* sono "relativamente primi").

4. Scegliere *d* tale che *ed-1* sia esattamente divisibile per *z*. (in altre parole: *ed* mod *z* = *1*).

5. La chiave *pubblica* è $\underbrace{(n,e)}_{K_B^+}$, quella *privata* è $\underbrace{(n,d)}_{K_B^-}$.

RSA: cifratura, decifratura

0. Dati (n,e) e (n,d) calcolati come abbiamo appena visto,

1. Per la codifica, $m < n$, si calcola

$$c = m^e \bmod n$$

2. Per decifrare il messaggio ricevuto, c, si calcola

$$m = c^d \bmod n$$

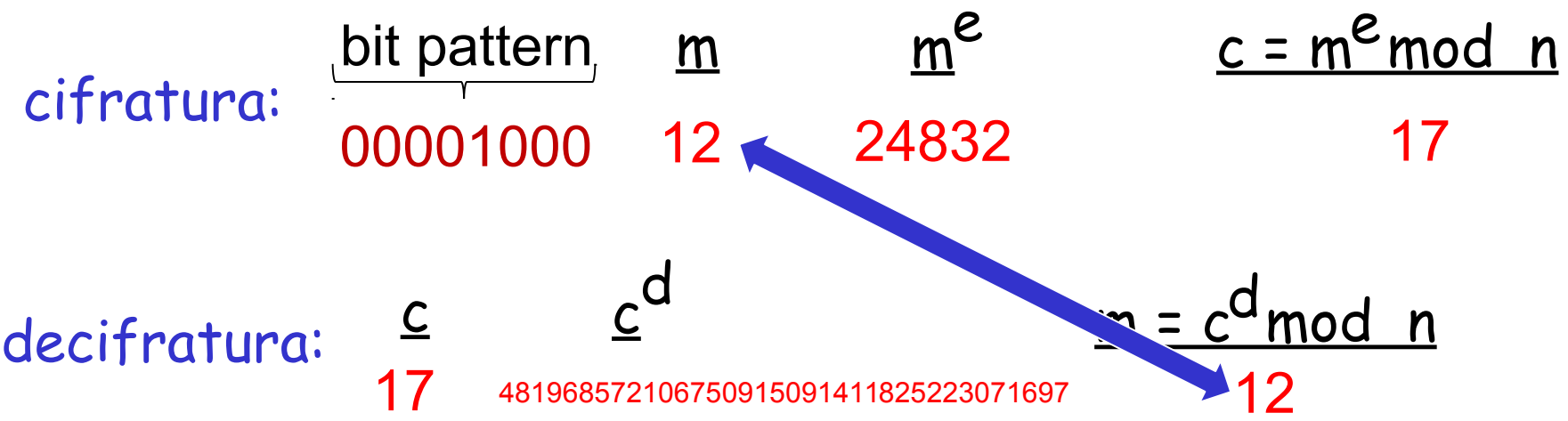
Incredibile! $m = (\underbrace{m^e \bmod n}_{c})^d \bmod n$

Un esempio di RSA:

Roberto sceglie *p=5, q=7*. Poi *n=35, z=24*.

e=5 (così *e, z* sono relativamente primi).

d=29 (così *ed-1* è esattam. divisibile per z).



RSA: Perché $m = (m^e \bmod n)^d \bmod n$

Utilizzamo la teoria dei numeri: se p e q sono primi e $n = pq$, allora:

$$x^y \bmod n = x^{y \bmod (p-1)(q-1)} \bmod n$$

$$(m^e \bmod n)^d \bmod n = m^{ed} \bmod n$$

$$= m^{ed \bmod (p-1)(q-1)} \bmod n$$

(usando la teoria dei numeri vista sopra)

$$= m^1 \bmod n$$

(perché abbiamo scelto che e e d siano divisibili per $(p-1)(q-1)$ con resto 1)

$$= m$$

RSA: un'altra importante proprietà

La seguente proprietà sarà *molto* utile più avanti:

$$\underbrace{K_B^-(K_B^+(m))}_{\text{Si usa prima la chiave pubblica, e poi quella privata}} = m = \underbrace{K_B^+(K_B^-(m))}_{\text{Si usa prima la chiave privata, e poi quella pubblica}}$$

Il risultato non cambia!

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

- Segue direttamente dall'aritmetica modulare:

- $(m^e \bmod n)^d \bmod n = m^{ed} \bmod n$

$= m^{de} \bmod n$

$= (m^d \bmod n)^e \bmod n$

Perché RSA è sicura?

- Supponete di conoscere la chiave pubblica di Bob (n,e). Quanto è difficile determinare b.
- Essenzialmente è necessario trovare p e q senza conoscerli.
- Fatto: Scomporre in fattori primi un numero grande è difficile.

RSA in pratica: chiave di sessione

- L'elevamento a potenza in RSA è computazionalmente intensivo.
- DES è almeno 100 volte più veloce di RSA
- Soluzione: usare la cittogragia a chiave pubblica per stabilire un canale sicuro di comunicazione, e scambiarsi in questo canale un nuova chiave K_S (chiave di sessione) per un algoritmo a chiave simmetrica
- Una vola stabilito e comunicato K_S, usare la crittografia a chiave simmetrica per il resto della comunicazione.

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
8.7 Sicurezza a livello di rete: IPSec
8.8 Sicurezza nelle LAN wireless
8.9 Sicurezza operativa: firewall e sistemi di rilevamento delle intrusioni

Firma digitale

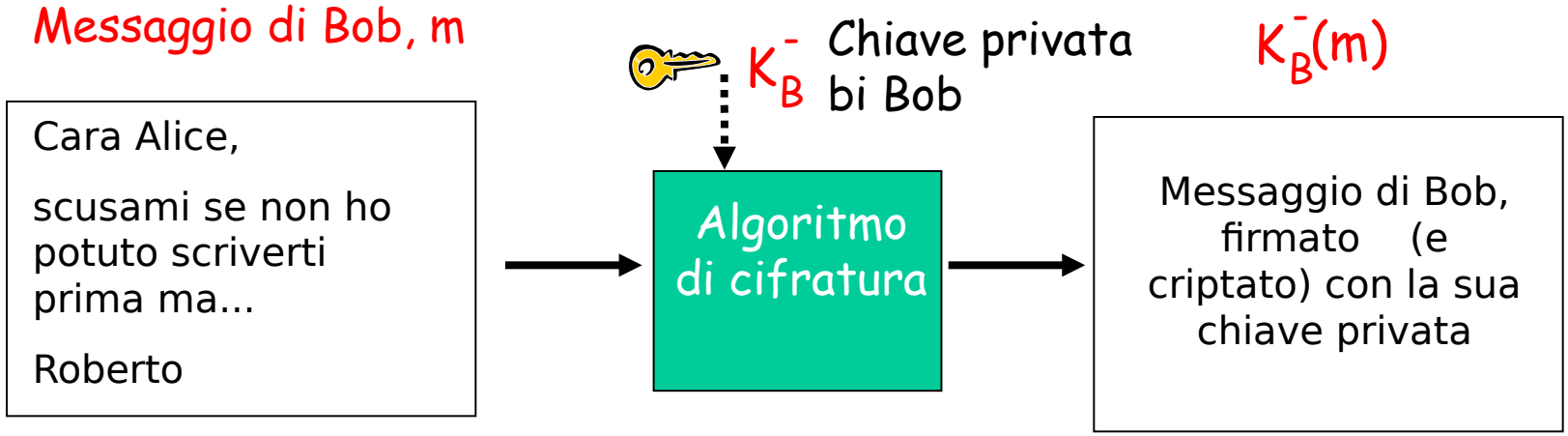
Tecnica crittografica analoga all'invio di una tradizionale "firma scritta"

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

Firma digitale

Semplice firma digitale di un messaggio, m:

- Bob 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 Bob 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 Bob .

Alice può verificare che:

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

Non-ripudio:

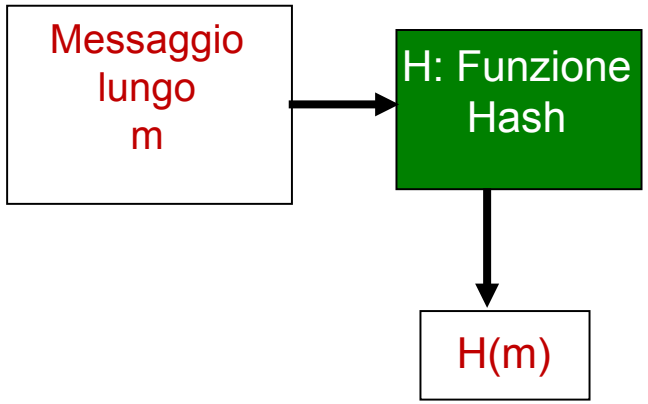
- ✓ Alice può prendere m, e la firma $K_B^-(m)$ per dimostrare che Roberto ha firmato m.

Message digest

criptare messaggi lunga usando la crittografia a chiave pubblica è computazionalmente costoso.

obiettivo: "impronte digitali" di un messaggio, di lunghezza fissa e facili da calcolare

soluzione: applicare una funzione hash H al messaggio m, per ottenere una "impronta" H(m) di lunghezza fissa (chiamata anche digest)



- Proprietà delle funzioni hash crittografiche
  - Molti ad uno
  - Produce digest di lunghezza fissa
  - Dato un digest x, è computazionalmente impossibile trovare un messaggio m tale che H(m)=x.

La checksum di Internet: una funzione hash 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:

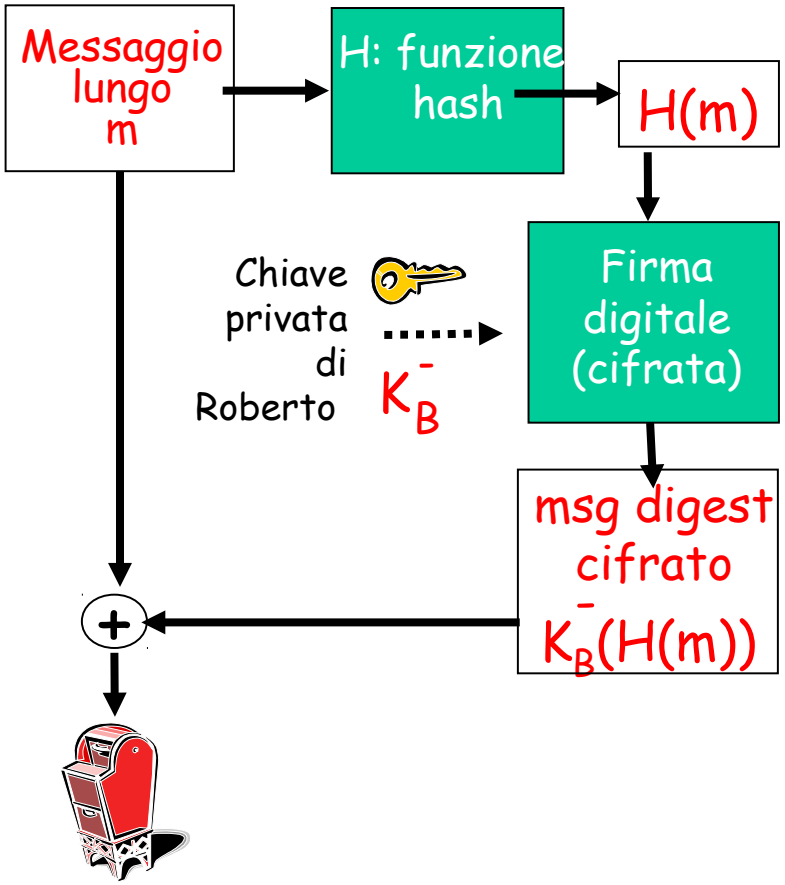
Messaggio	Rappresentaz. ASCII
I O U 1	49 4F 55 31
0 0 . 9	30 30 2E 39
9 B O B	39 42 D2 42
	B2 C1 D2 AC

Messaggio	Rappresentaz. ASCII
I O U 9	49 4F 55 39
0 0 . 1	30 30 2E 31
9 B O B	39 42 D2 42
	B2 C1 D2 AC

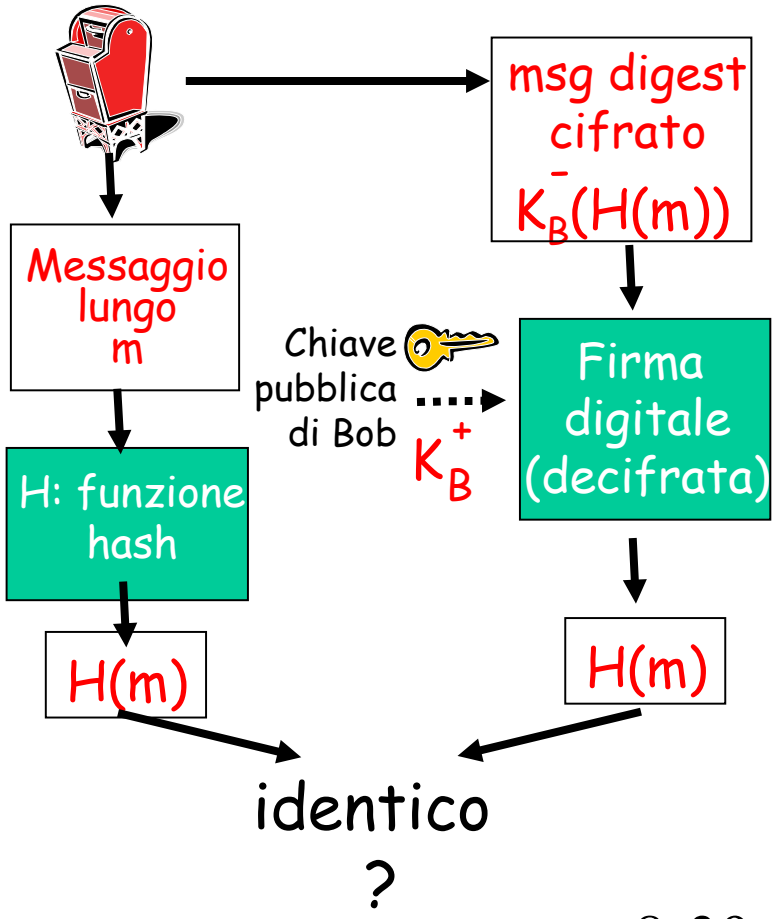
Messaggi diversi ma checksum identica!

Firma digitale = digest firmati

Bob invia un messaggio con la firma digitale:



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



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 SHA-1
  - Standard statunitense [NIST, FIPS PUB 180-1]
  - Produce una sintesi del messaggio di 160 bit

Certificazione della chiave pubblica

Problema per la crittografia a chiave pubblica:

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

Esempio

Trudy crea un ordine per e-mail

- Caro Pizza Store, per favore, mi spedisca quattro pizze ai funghi. Grazie, Bob.

Trudy firma digitalmente l'ordine con la sua chiave privata

Trudy invia l'ordine a Pizza Store

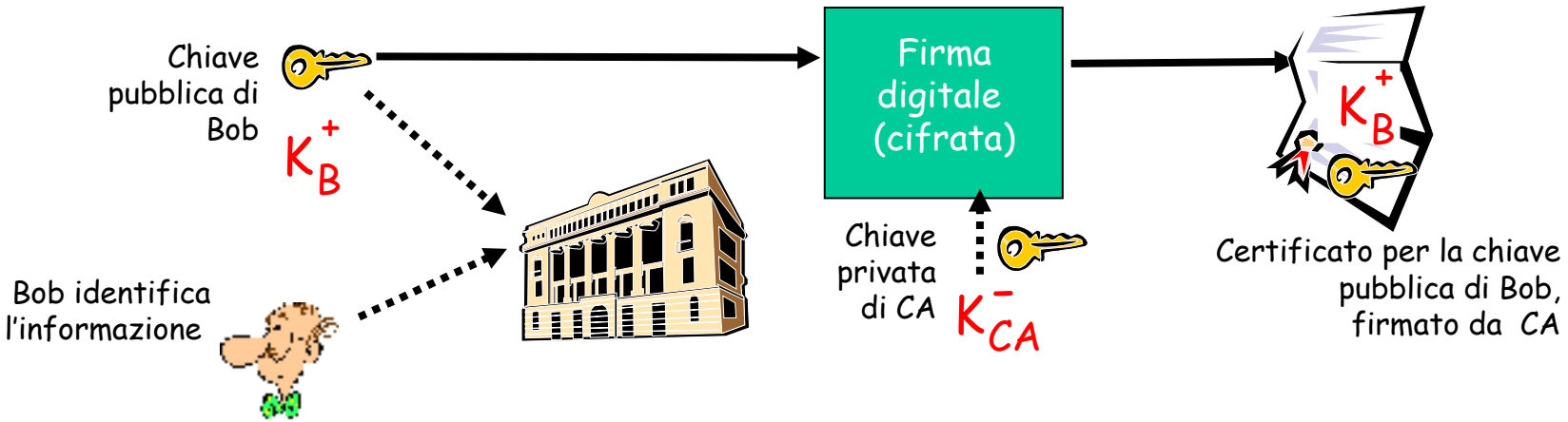
Trudy invia a Pizza Store la sua chiave pubblica, ma dice che è quella di Bob.

Pizza Store verifica la firma digitale, poi invia le quattro pizze a Bob

A Bob non piace la pizza ai funghi

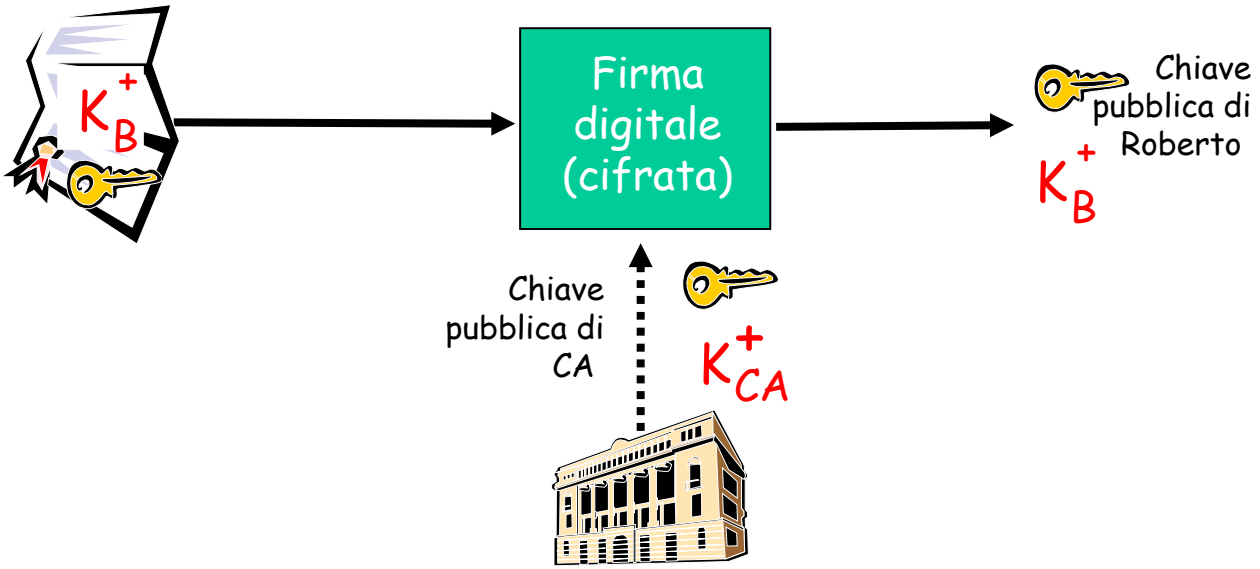
Autorità di certificazione

- 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")



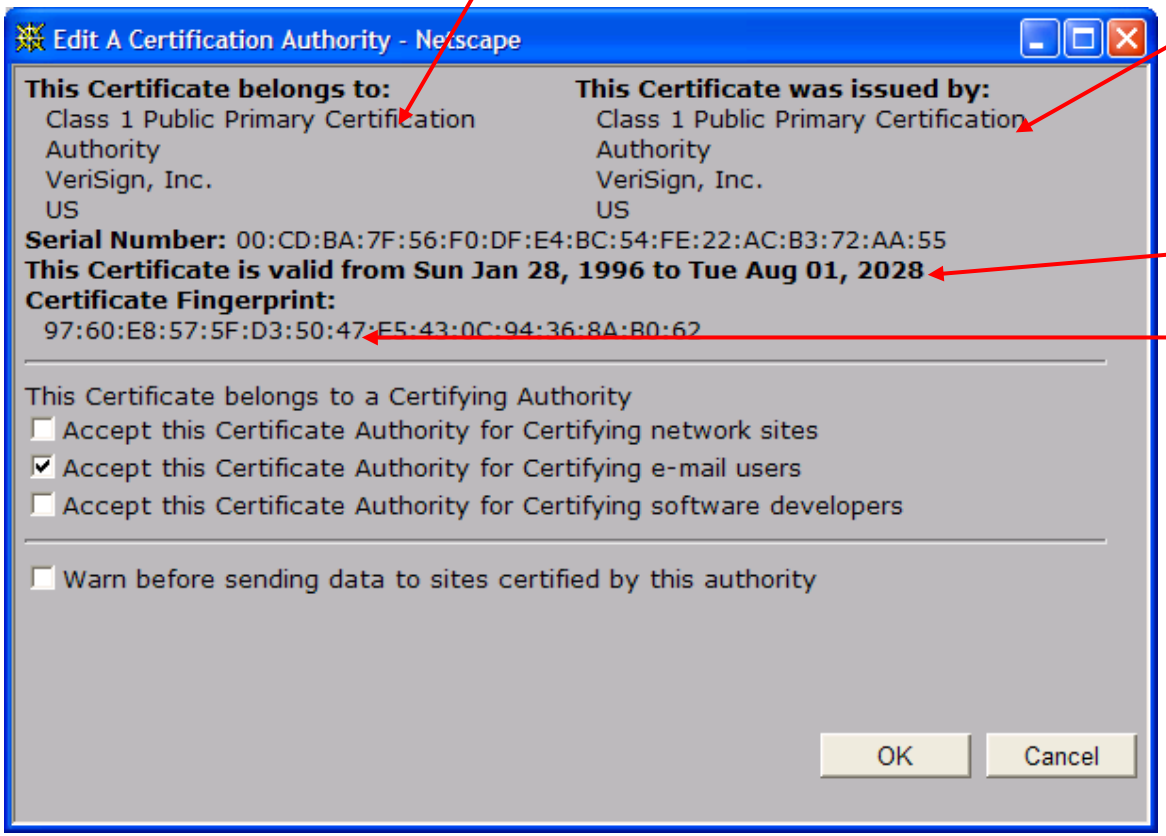
Autorità di certificazione

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



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
8.7 Sicurezza a livello di rete: IPSec
8.8 Sicurezza nelle LAN wireless
8.9 Sicurezza operativa: firewall e sistemi di rilevamento delle intrusioni

Autenticazione

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

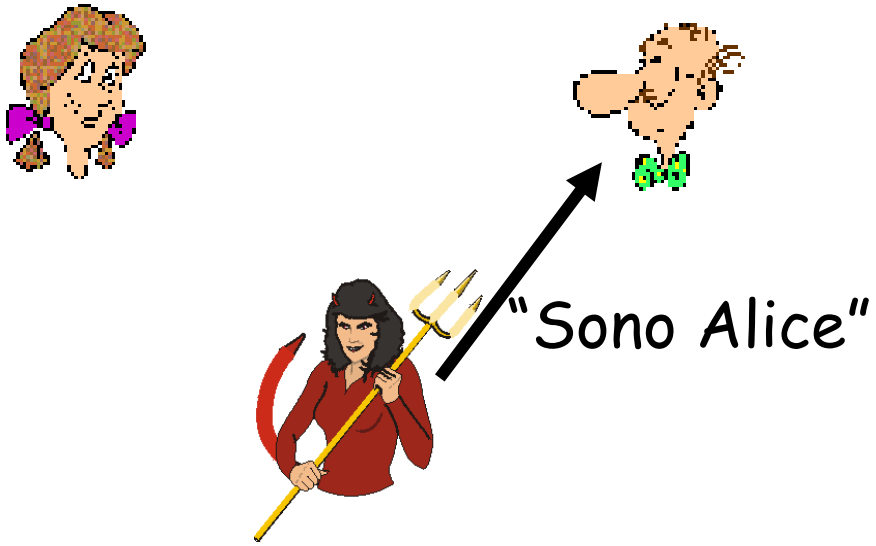
Protocollo ap1.0: Alice dice "Sono Alice"

Scenario con fallimento??

Autenticazione

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

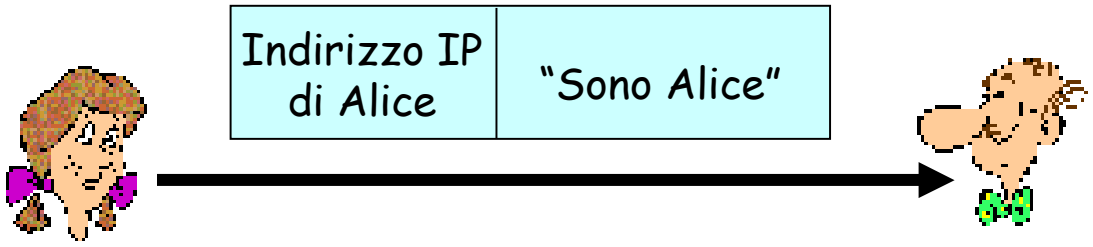
Protocollo ap1.0: Alice dice "Sono Alice"



in una rete,
Bob non può "vedere"
Alice, e Trudy può
semplicemente
autenticarsi come Alice

Autenticazione: un altro tentativo

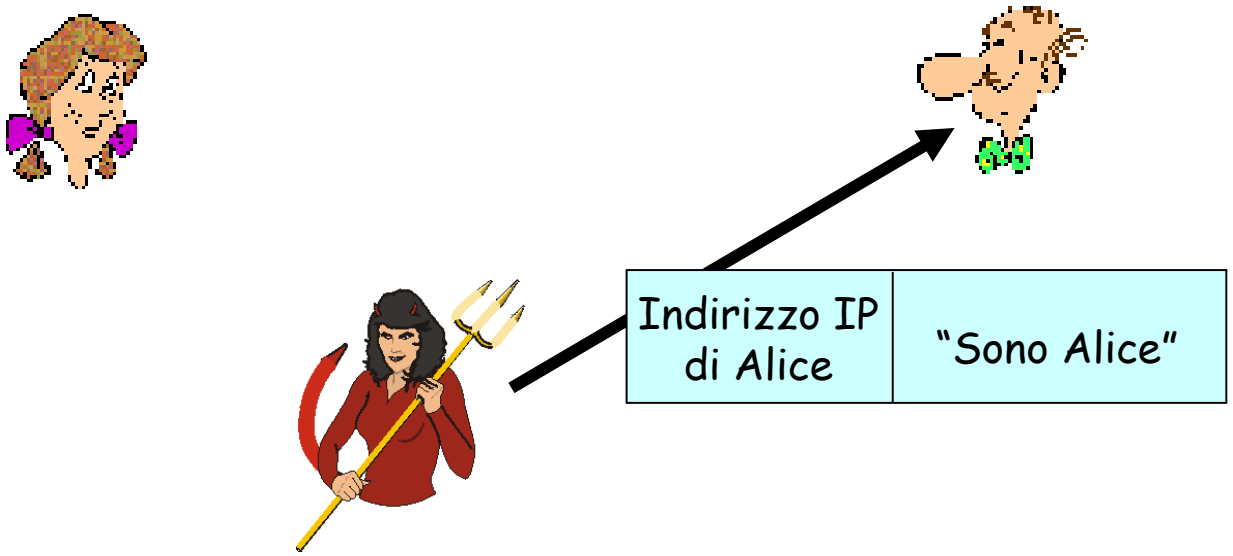
Protocollo ap2.0: Alice dice "Sono Alice" in un pacchetto IP che contiene il suo indirizzo IP sorgente



Scenario con fallimento??

Autenticazione: un altro tentativo

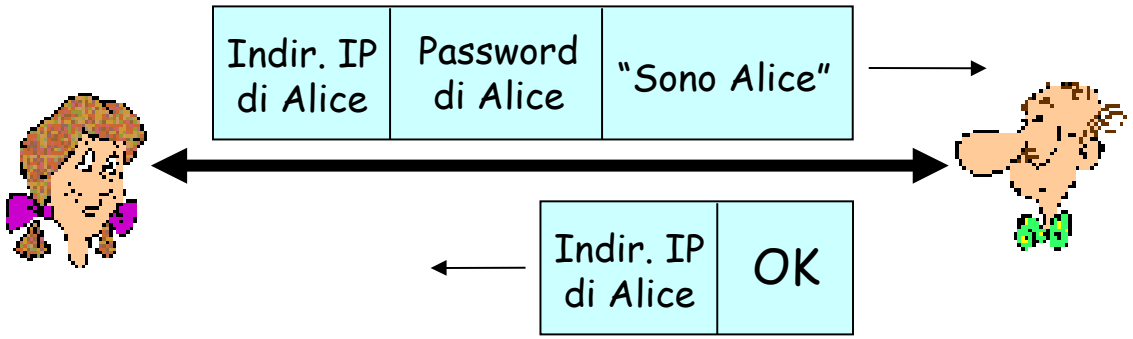
Protocollo ap2.0: Alice dice "Sono Alice" in un pacchetto IP che contiene il suo indirizzo IP sorgente



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

Autenticazione: un altro tentativo

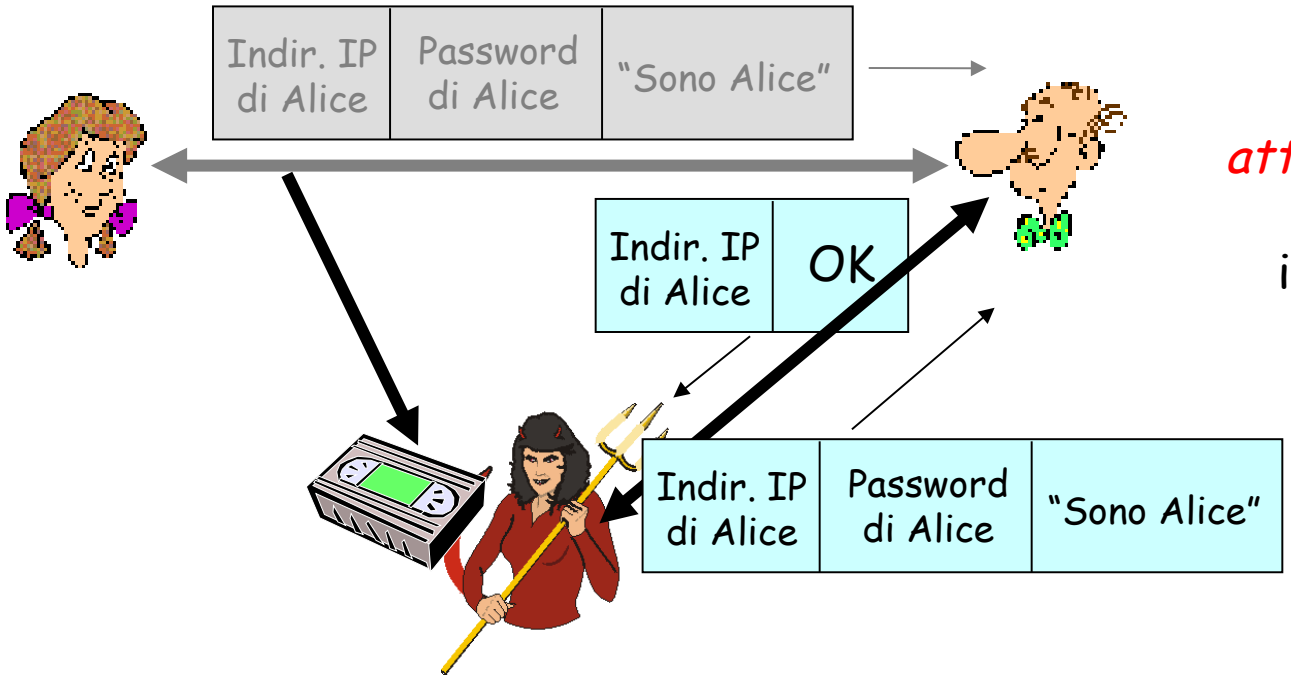
Protocollo ap3.0: Alice dice "Sono Alice" e invia la sua password segreta per "dimostrarlo"



Scenario con fallimento??

Autenticazione: un altro tentativo

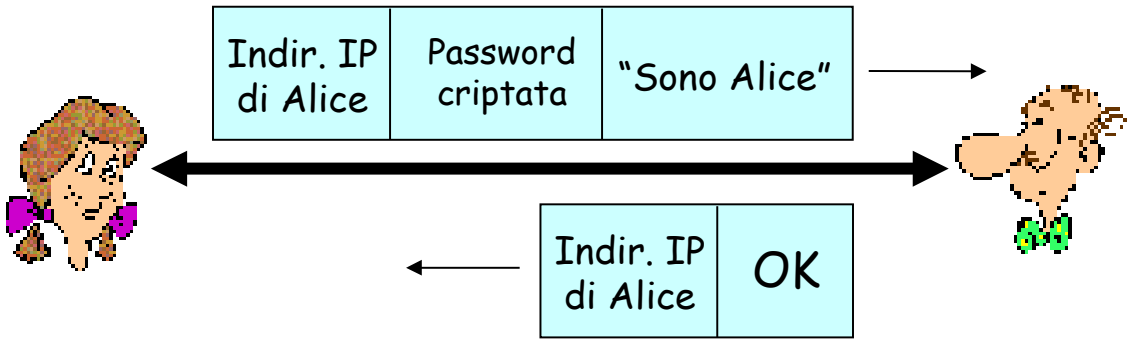
Protocollo ap3.0: Alice dice "Sono Alice" e invia la sua password segreta per "dimostrarlo"



attacco di replica: Trudy registra il pacchetto di Alice e lo riproduce successivamente trasmettendolo a Bob

Autenticazione: ancora un altro tentativo

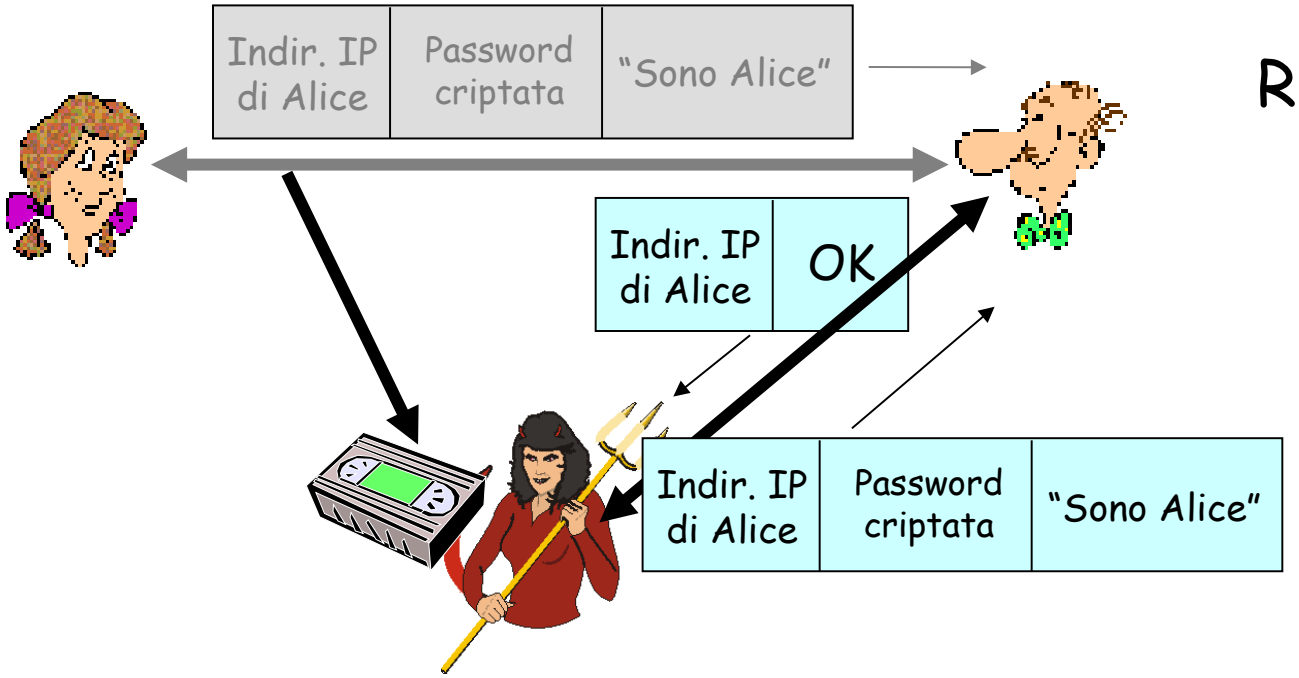
Protocollo ap3.1: Alice dice "Sono Alice" e invia la sua password segreta criptata per "dimostrarlo".



Scenario con fallimento??

Autenticazione: ancora un altro tentativo

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



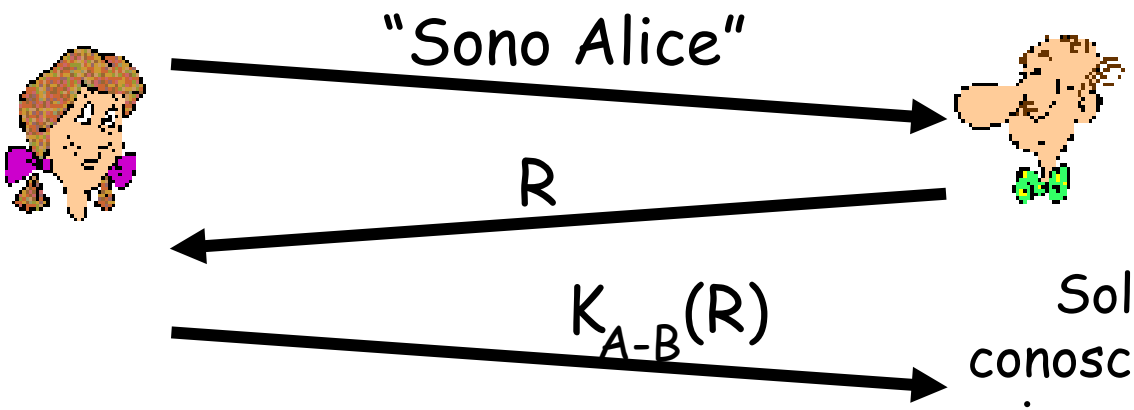
Registrazione e riproduzione funzionano ancora!

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", Bob sceglie e manda ad Alice un nonce, R.
Alice reinvia il nonce R, criptato utilizzando la chiave simmetrica segreta.



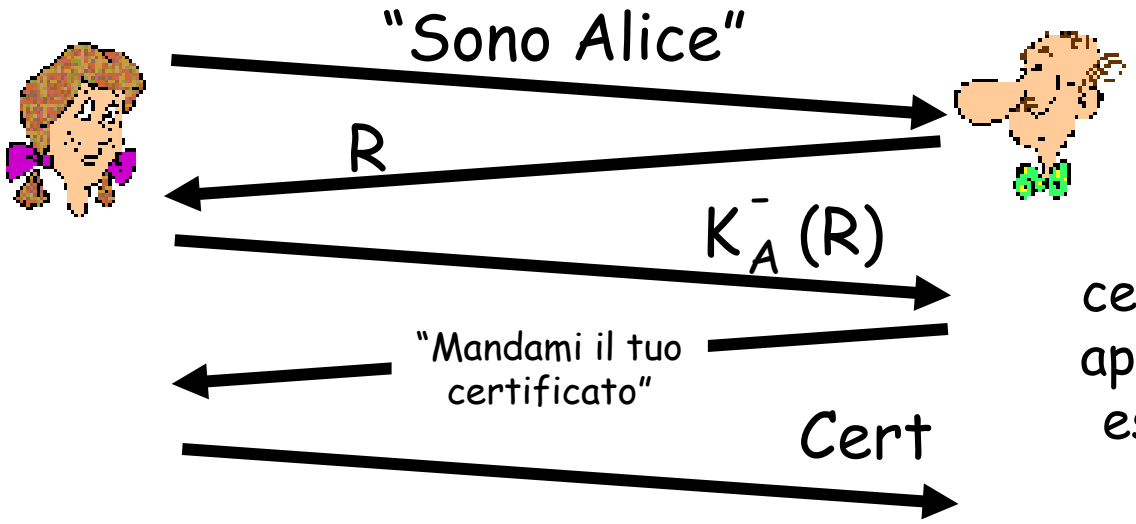
Attacco fallito?

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



Bob controlla che il certificato sia valido ed appartenga ad Alice, poi estrae $K^+_A(R)$ e calcola

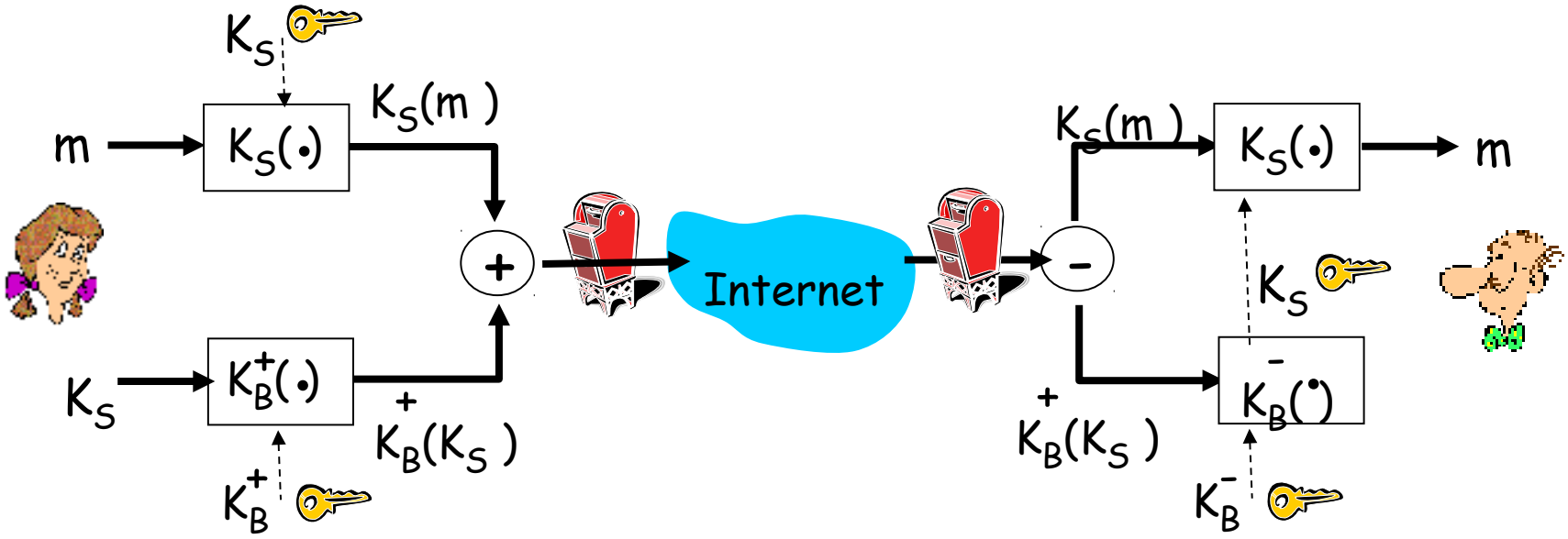
$$K_A^+(K_A^-(R)) = R$$

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
8.7 Sicurezza a livello di rete: IPSec
8.8 Sicurezza nelle LAN wireless
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.

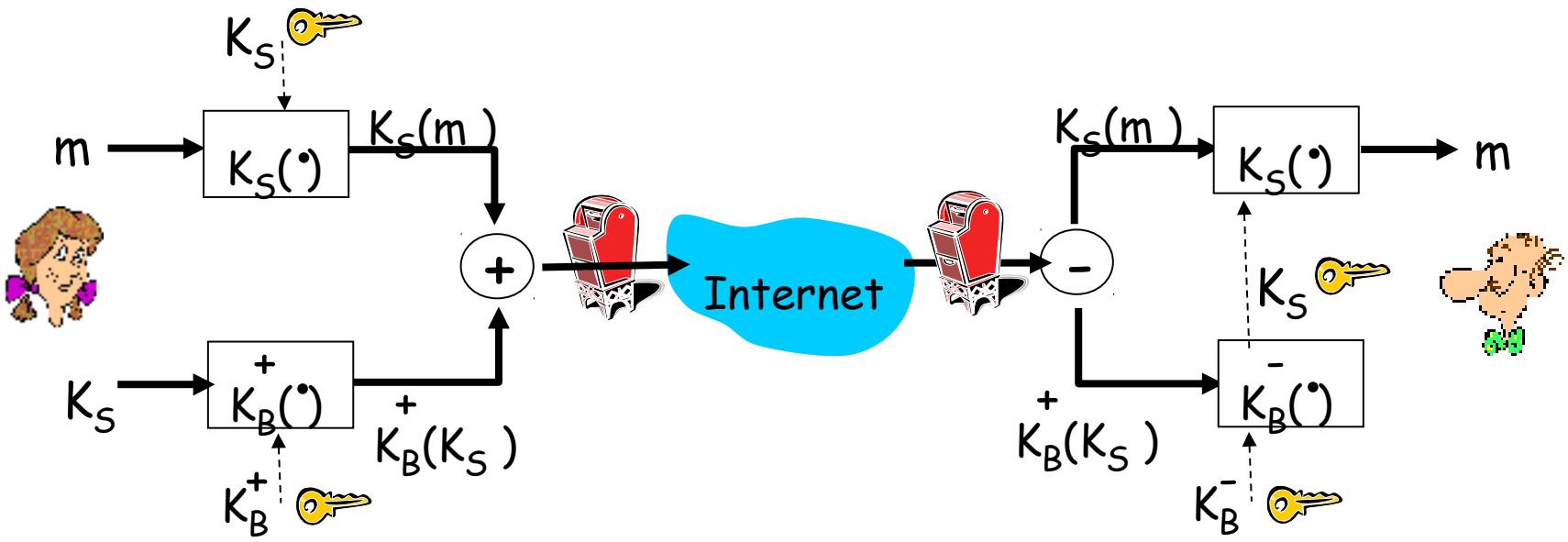


Alice:

- 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.

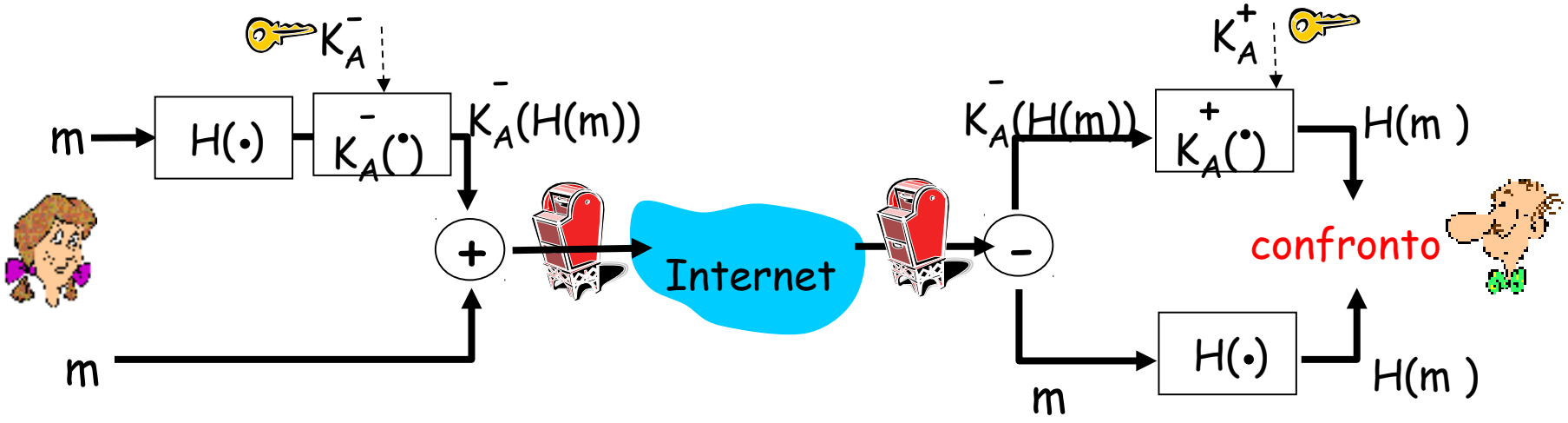


Bob:

- 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)

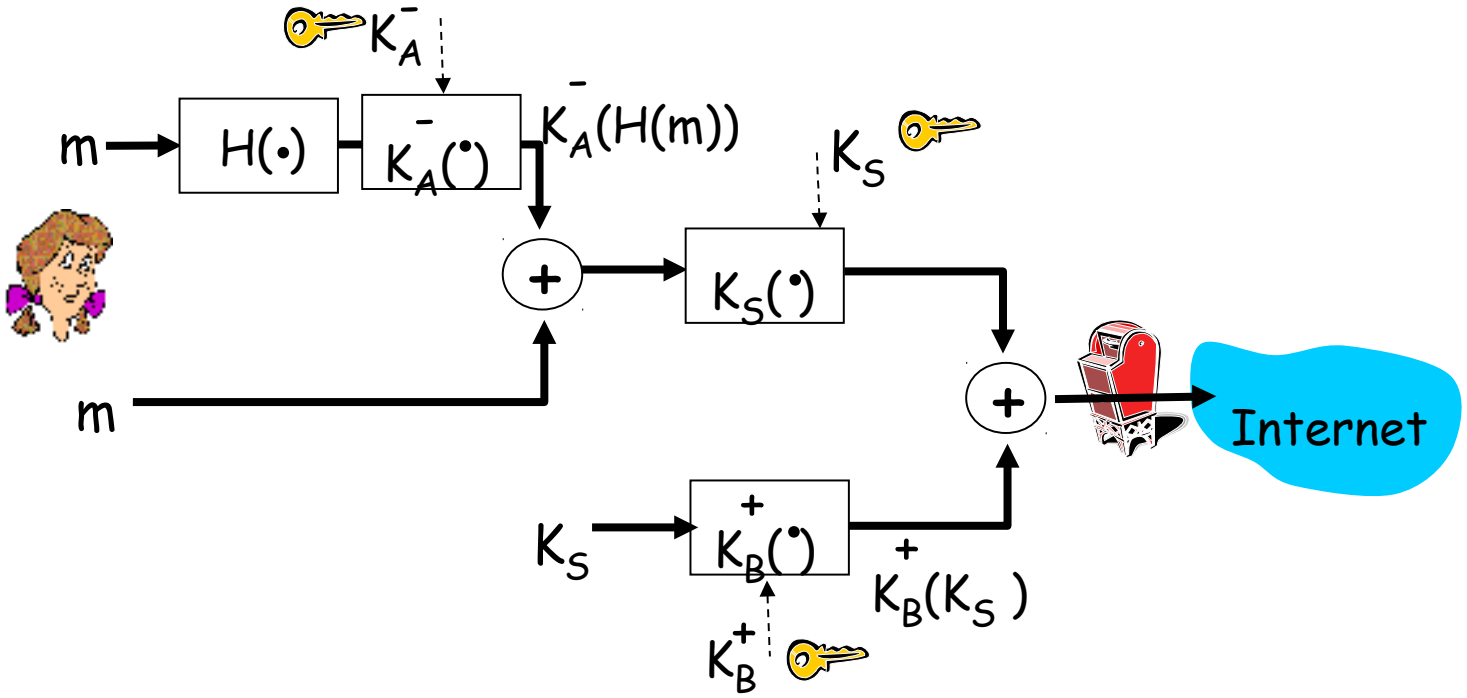
• Alice vuole autenticarsi come mittente e garantire l'integrità del messaggio



• 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 Bob 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.
- GPG (Gnu Privacy Guard) è la versione open-source di PGP.

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---
```

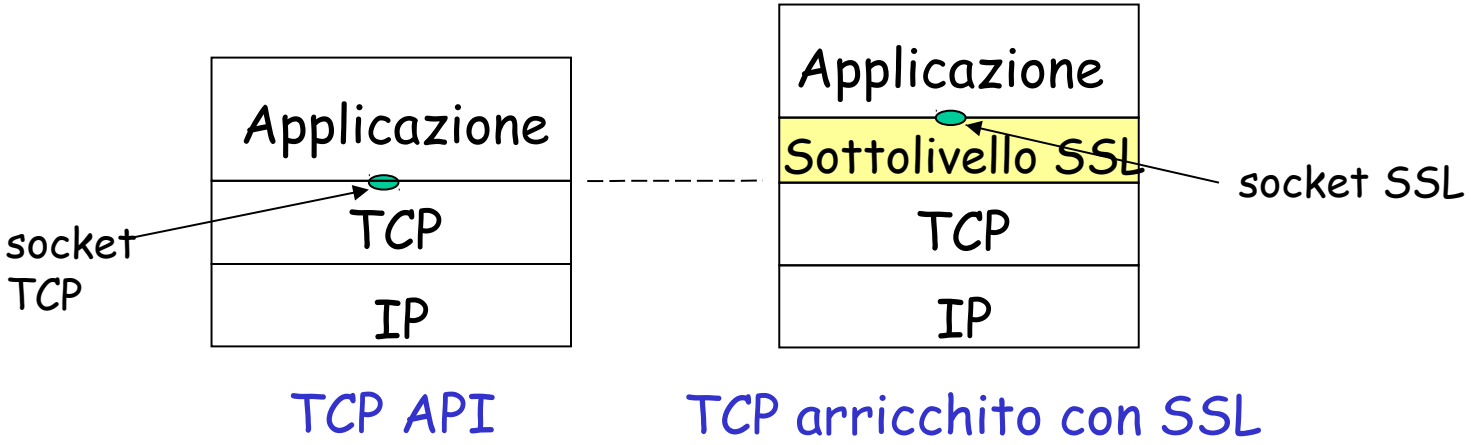
Le slide che seguono non sono ancora state aggiornate alla 6^ edizione del libro di testo.

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
8.7 Sicurezza a livello di rete: IPSec
8.8 Sicurezza nelle LAN wireless
8.9 Sicurezza operativa: firewall e sistemi di rilevamento delle intrusioni

Livello di socket sicura (SSL)

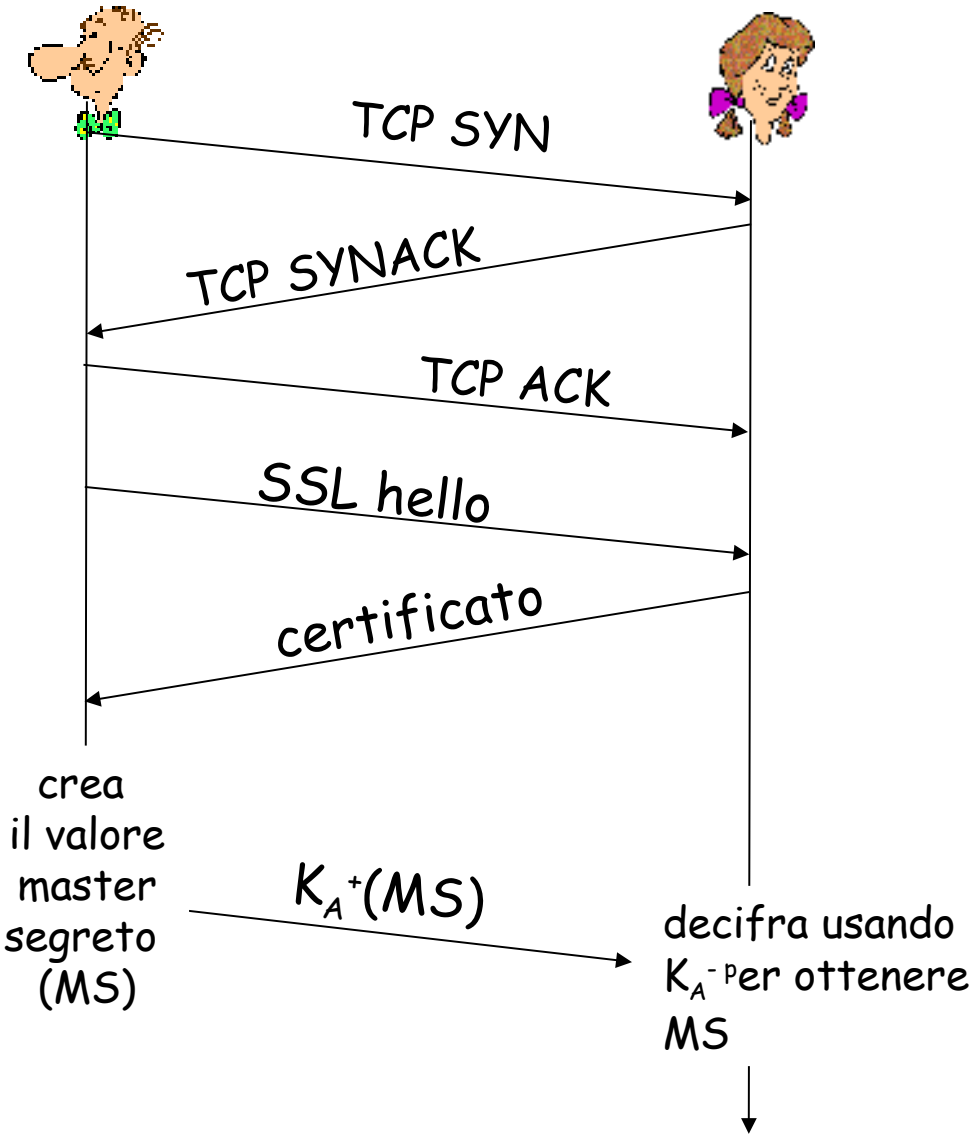
- Costituisce la base del protocollo di sicurezza a livello di trasporto.
  - Ampiamente utilizzato nelle transazioni commerciali e finanziarie su Internet (https)
- Servizi di sicurezza:
  - Autenticazione del server, cifratura dei dati, autenticazione del client (opzionale)



SSL: tre fasi

1. Handshake:

- Roberto crea una connessione TCP con Alice
- autentica Alice con un certificato firmato dalla CA
- crea, cifra (usando la chiave pubblica di Alice), e invia il valore master segreto ad Alice
  - il nonce scambiato non viene mostrato



SSL: tre fasi

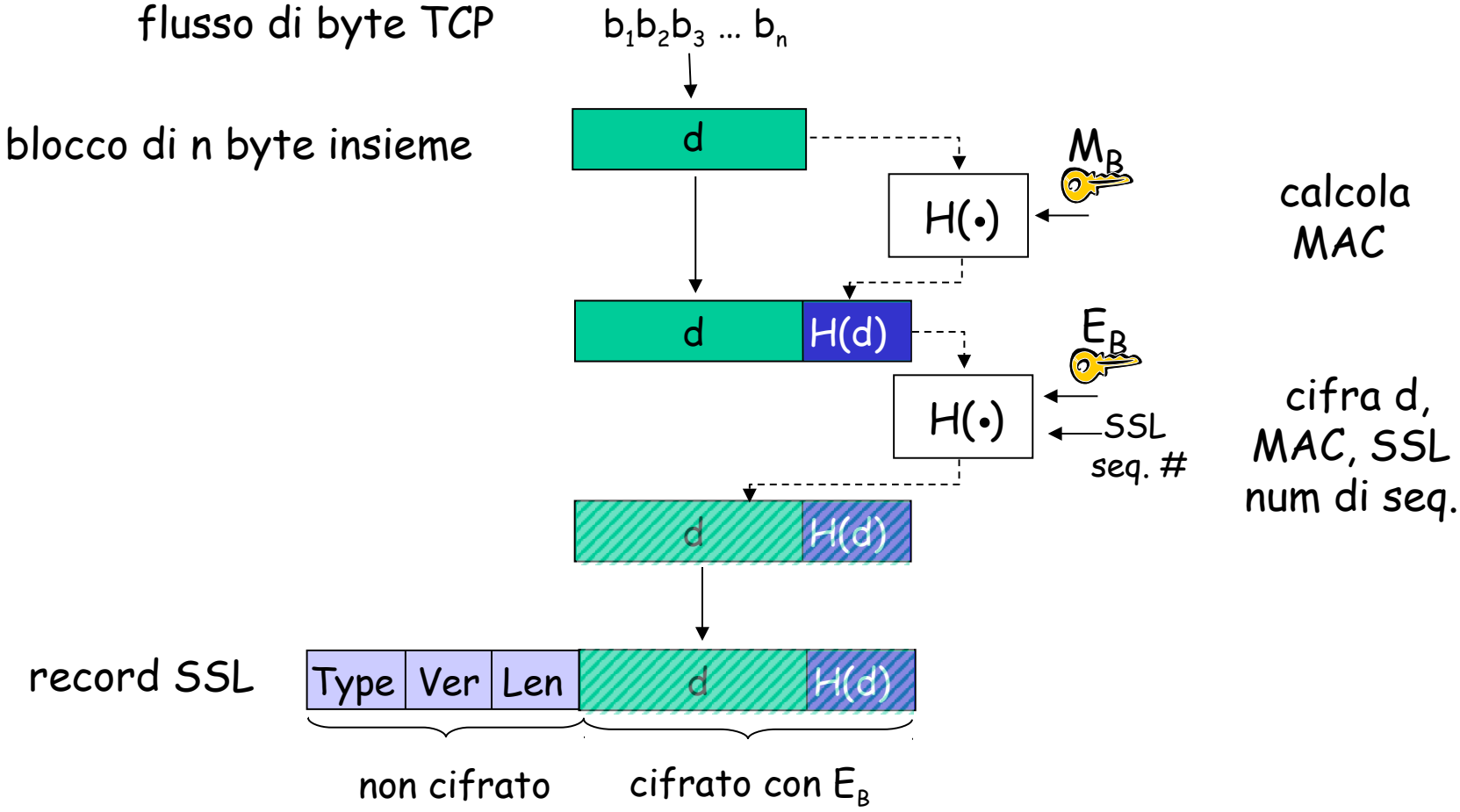
2. Derivazione delle chavi:

- Alice e Roberto usano il segreto condiviso (MS) per generare 4 chiavi:
  - E_R: chiave di cifratura di sessione per i dati inviati da Roberto ad Alice
  - E_A: chiave di cifratura di sessione per i dati inviati da Alice a Roberto
  - M_R: chiave MAC di sessione per i dati inviati da Roberto ad Alice
  - M_A: chiave MAC di sessione per i dati inviati da Alice a Roberto

- Cifratura e algoritmi MAC negoziabili tra Roberto e Alice
- Perché 4 chiavi?

SSL: tre fasi

3. Trasferimento dati



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
8.7 Sicurezza a livello di rete: IPSec
8.8 Sicurezza nelle LAN wireless
8.9 Sicurezza operativa: firewall e sistemi di rilevamento delle intrusioni

Protocollo di sicurezza IP (IPsec)

- Sicurezza a livello di rete:
  - L'host mittente cifra i dati nel datagramma IP
  - Segmenti TCP e UDP; messaggi ICMP e SNMP.
- Autenticazione a livello di rete:
  - L'host di destinazione autentica l'indirizzo IP sorgente.
- Due principali protocolli:
  - Intestazione per l'autenticazione (AH).
  - Incapsulamento sicuro del carico utile (ESP).
- L'host sorgente e quello di destinazione si scambiano l'handshake:
  - Creano un canale logico a livello di rete chiamato Associazione di sicurezza (SA).
- Ciascuna SA è unidirezionale.
- Le SA sono contraddistinte da:
  - Protocollo di sicurezza (AH o ESP)
  - Indirizzo IP sorgente
  - ID di connessione a 32 bit

Protocollo AH (intestazione per l'autenticazione)

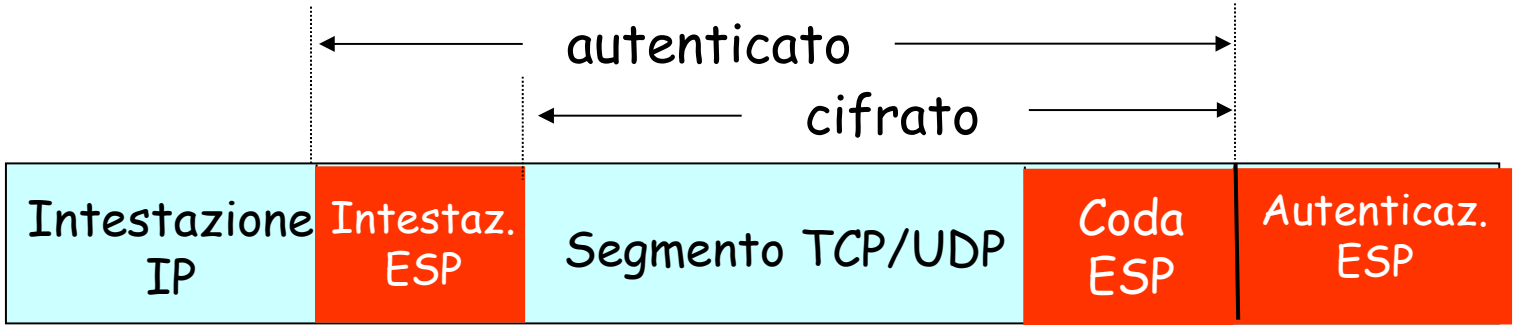
- Fornisce l'autenticazione della sorgente e l'integrità dei dati ma non la riservatezza.
- L'intestazione AH è inserita fra i dati del diagramma originale e l'intestazione IP.
- Il protocollo è contraddistinto dal valore 51.
- I router intermedi si limitano all'instradamento in funzione dell'indirizzo IP.

L'intestazione AH comprende:

- identificatore di connessione
- Autenticazione dati: digest del messaggio firmato dal mittente, calcolato in base al datagramma IP originario.
- Campo intestazione successiva: specifica il tipo di dati (es.: TCP, UDP, ICMP)

Protocollo ESP

- Fornisce autenticazione della sorgente, integrità dei dati e riservatezza.
- I dati e il campo ESP sono codificati.
- Il campo intestazione successiva è nella coda.
- L'autenticazione ESP è simile all'autenticazioe AH.
- Protocollo = 50.



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
8.7 Sicurezza a livello di rete: IPSec
8.8 Sicurezza nelle LAN wireless
8.9 Sicurezza operativa: firewall e sistemi di rilevamento delle intrusioni

Sicurezza in IEEE 802.11

- Quante sono le reti wireless "visibili" dall'esterno degli edifici nella baia di San Francisco?
  - Più di 9000 sono accessibili dalla strada.
  - L'85% di queste non utilizza meccanismi di sicurezza.
  - Analisi dei pacchetti e svariati attacchi risultano estremamente facili!
- Rendere sicuro il protocollo IEEE 802.11
  - Cifratura e autenticazione.
  - Primo tentativo di porre in sicurezza 802.11: Wired Equivalent Privacy (WEP): un fallimento.
  - Attuale tentativo: 802.11i

Wired equivalent privacy (WEP):

- L'autenticazione è effettuata come nel protocollo *ap4.0*
  - L'host richiede l'autenticazione da un punto di accesso.
  - Il punto di accesso invia un nonce a 128 byte.
  - L'host codifica il nonce con la chiave simmetrica condivisa e lo ritrasmette.
  - Il punto d'accesso decifra il nonce e autentica l'host wireless.
- Nessun meccanismo di distribuzione delle chiavi.
- Autenticazione: è sufficiente conoscere la chiave condivisa.

Cifratura con WEP

- Host e AP condividono una chiave segreta simmetrica semi-permanente a 40 bit, K_s.
- Viene aggiunto un vettore di inizializzazione a 24 bit, IV, creando una chiave di 64 bit.
- IV cambia da un frame all'altro, ognuno sarà criptato con una chiave diversa , k_i^{IV}
- k_i^{IV} è usata per cifrare i byte di dati, d_i, per ottenere il byte del testo cifrato c_i:

$$c_i = d_i \text{ XOR } k_i^{IV}$$

- IV e i byte cifrati, c_i , inviati nel frame

Protocollo WEP 802.11

Cifratura WEP dal lato mittente

Attacco al protocollo WEP 802.11

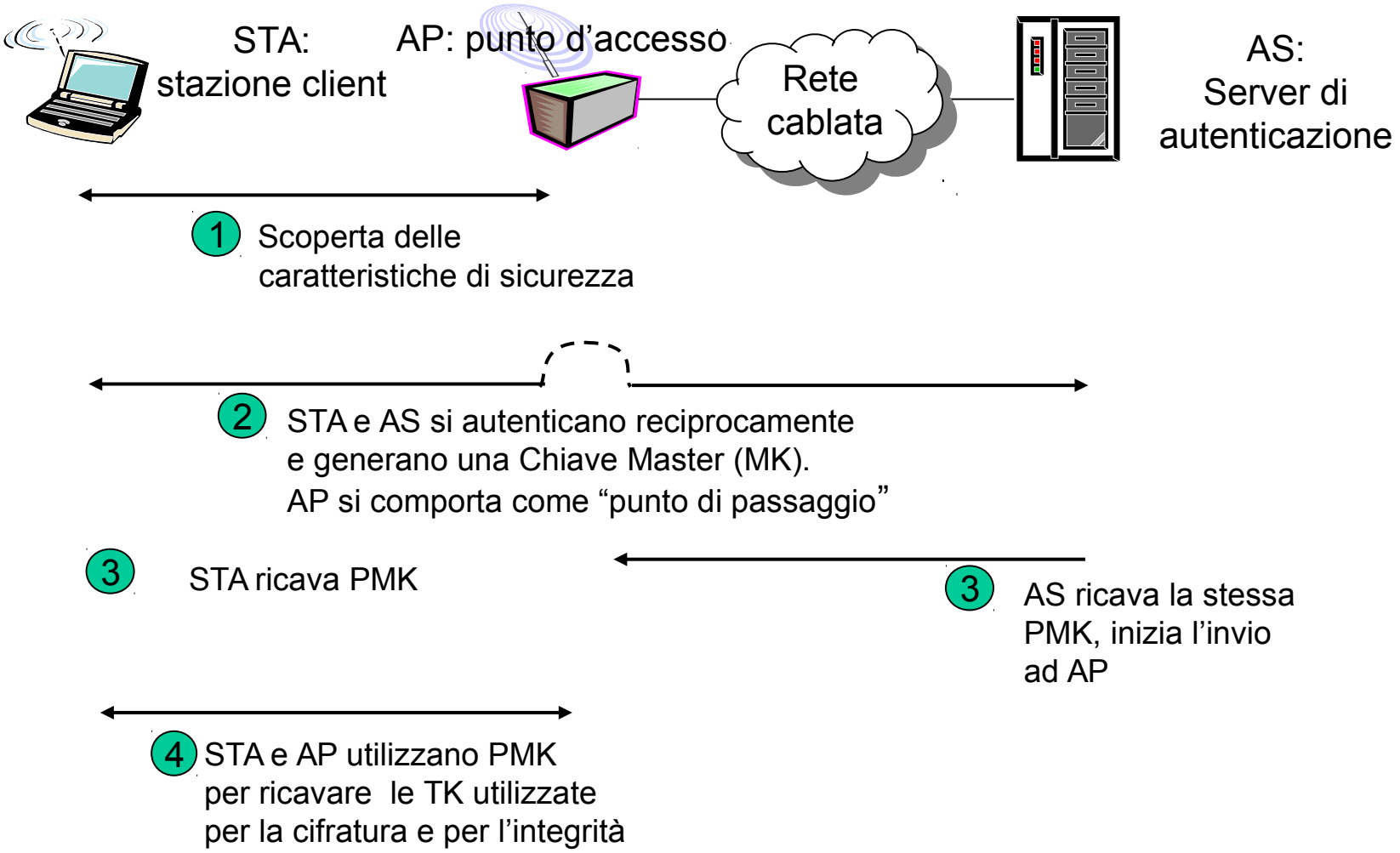
Bachi:

- IV a 24-bit, un IV per frame -> IV può essere riutilizzato
- IV è trasmesso in chiaro -> il riutilizzo di IV è individuato
- **Attacchi:**
  - Tommaso fa sì che Alice cifri il suo testo in chiaro
  - $d_1\ d_2\ d_3\ d_4$ …
  - Tommaso osserva che: $c_i = d_i$ XOR k_i^{IV}
  - Tommaso conosce c_i d_i, quindi è in grado di calcolare k_i^{IV}
  - Tommaso conosce la sequenza di chiavi criptate $k_1^{IV}\ k_2^{IV}\ k_3^{IV}$ …
  - La prossima volta che IV sarà usato, Tommaso sarà in grado di decifrarlo!

802.11i: la sicurezza è più efficace

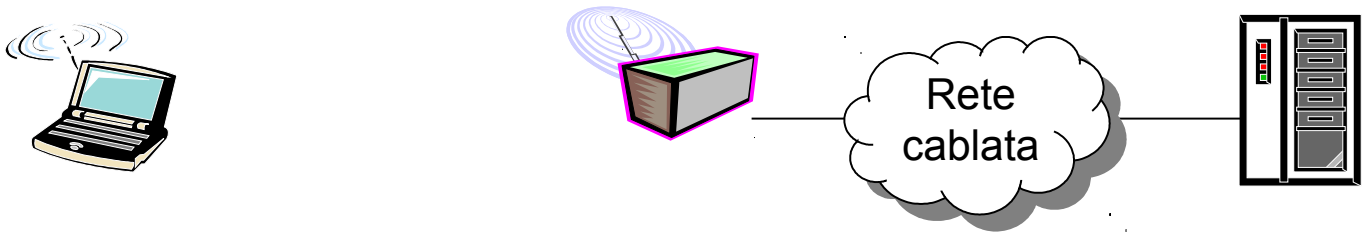
- Schema crittografico più solido
- Fornisce un metodo di distribuzione delle chiavi
- Definisce un server di autenticazione con il quale ciascun AP può comunicare.

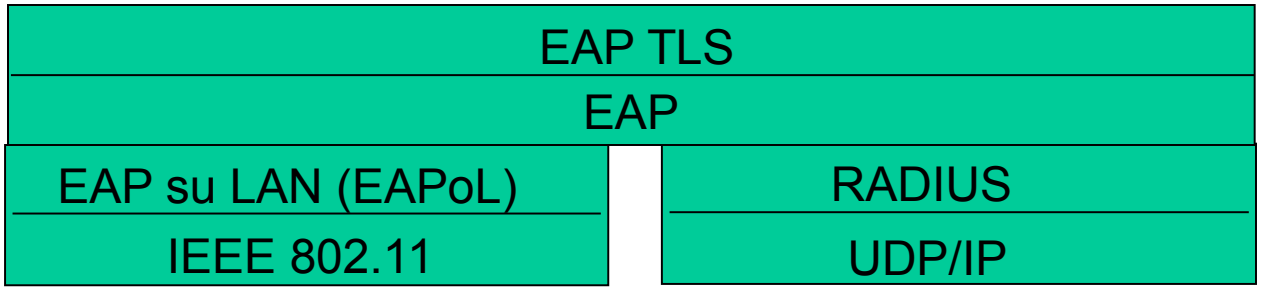
802.11i: operazione in quattro fasi



Protocollo di autenticazione estendibile (EAP)

- EAP: definisce i messaggi punto-punto utilizzati nell'intestazione tra client/server di autenticazione
- I messaggi EAP sono inviati su link separati
  - Da mobile ad AP (EAP over LAN)
  - Da AP al server di autenticazione (RADIUS over UDP)



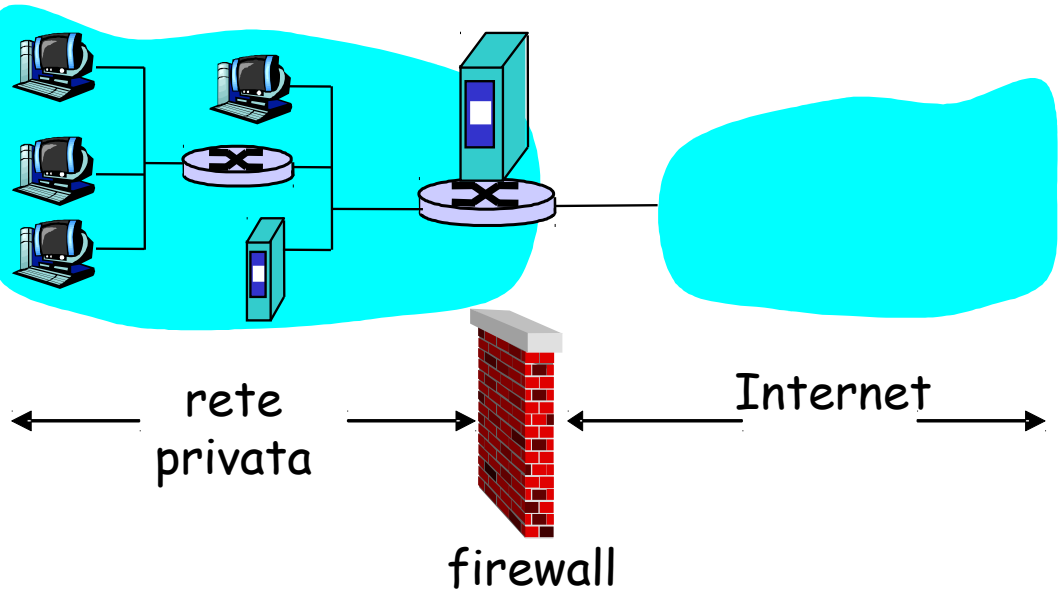


Capitolo 8 La sicurezza nelle reti

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
8.7 Sicurezza a livello di rete: IPSec
8.8 Sicurezza nelle LAN wireless
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.

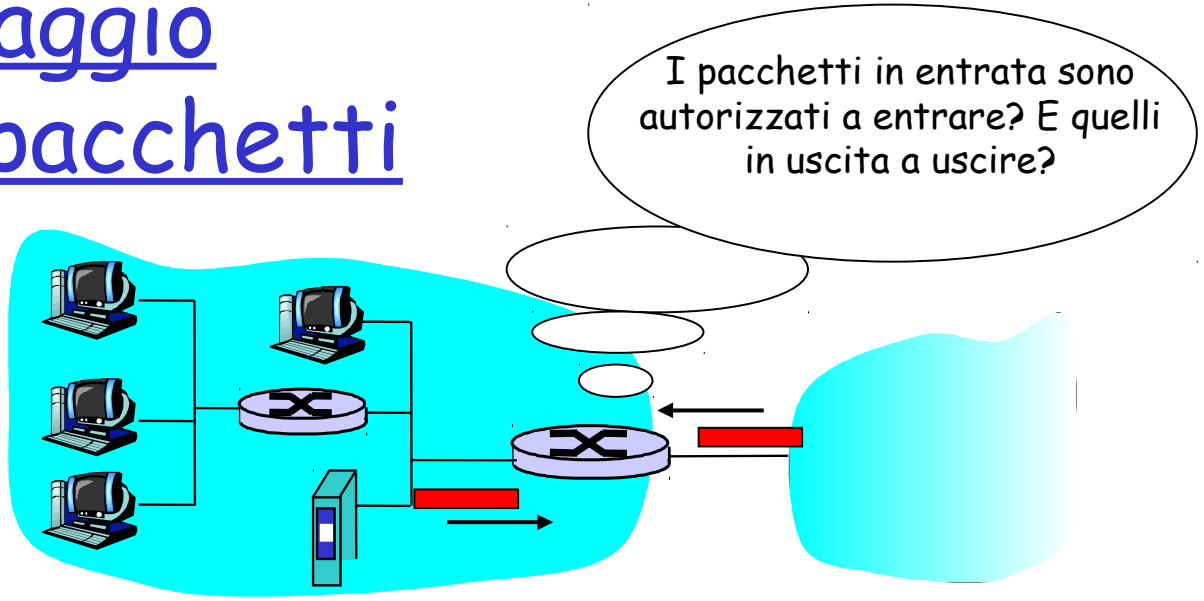
- es., l'intruso può sostituire l'homepage del MIUR con qualcos'altro.

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)

Filtraggio dei pacchetti



- Una rete privata è collegata a Internet mediante un router
- Il router è responsabile del filtraggio dei pacchetti e determina quali pacchetti devono essere bloccati o quali possono passare in base a:
  - Indirizzo IP sorgente o destinazione
  - Porte sorgente e destinazione TCP o UDP
  - Tipo di messaggio ICMP
  - Bit TCP SYN o ACK

Filtraggio di pacchetti: un esempio

- Esempio 1: blocco sui datagrammi in entrata e in uscita con IP protocol field = 17 e il cui numero di porta sorgente o destinazione = 23.
  - Tutti i segmenti UDP e tutte le connessioni Telnet sono bloccate.
- Esempio 2: bloccare i segmenti delle comunicazioni TCP con ACK=0.
  - Espediente utile se si vuole che i client interni possano collegarsi a server esterni, evitando però l'operazione inversa.

Filtraggio di pacchetti: ulteriori esempi

Politica	Configurazione del firewall
Nessun accesso Web all'esterno.	Bloccare tutti i pacchetti IP uscenti con porta dest. 80 e qualsiasi indirizzo IP dest.
Nessuna connessione TCP entrante, eccetto quelle dirette al solo server Web pubblico dell'organizzazione	Bloccare tutti i pacchetti TCP SYN entranti verso quals.indirizzo IP 130.207.244.203, con porta destinazione 80
Evitare che le radio Web intasino la banda disponibile	Bloccare tutti i pacchetti UDP entranti, eccetto i pacchetti DNS
Evitare che la rete possa essere usata per un attacco DoS	Bloccare tutti i pacchetti ICMP ping diretti a un indirizzo broadcast (es. 130.207.255.255).
Evitare che la rete possa essere rilevata tramite Traceroute	Bloccare tutti i messaggi ICMP con TTL esaurito uscenti

Access Control Lists

- *ACL:* tabella di regole da applicare integralmente ai pacchetti entranti.

azione	indirizzo sorgente	indirizzo dest	protocollo	porta sorgente	porta destinaz.	bit di flag
consenti	222.22/16	al di fuori di 222.22/16	TCP	> 1023	80	qualsiasi
consenti	al di fuori di 222.22/16	222.22/16	TCP	80	> 1023	ACK
consenti	222.22/16	al di fuori di 222.22/16	UDP	> 1023	53	---
consenti	al di fuori di 222.22/16	222.22/16	UDP	53	> 1023	----
blocca	tutto	tutto	tutto	tutto	tutto	tutto

Filtri di pacchetti con memoria dello stato

- Filtraggio tradizionale: strumento poco flessibile
  - Ammette pacchetti che "non hanno senso," es. dest port = 80, bit ACK anche se non vi è alcuna connessione TCP.

azione	source address	indirizzo dest	protocollo	porta sorgente	porta destinaz	bit di flag
consenti	Al di fuori di 222.22/16	222.22/16	TCP	80	> 1023	ACK

- *Filtraggio con memoria dello stato:* tiene traccia dello stato di tutte le connessioni TCP
  - Traccia l'impostazione del collegamento (SYN) e la terminazione (FIN): può così determinare se i pacchetti in entrata o in uscita "hanno senso"

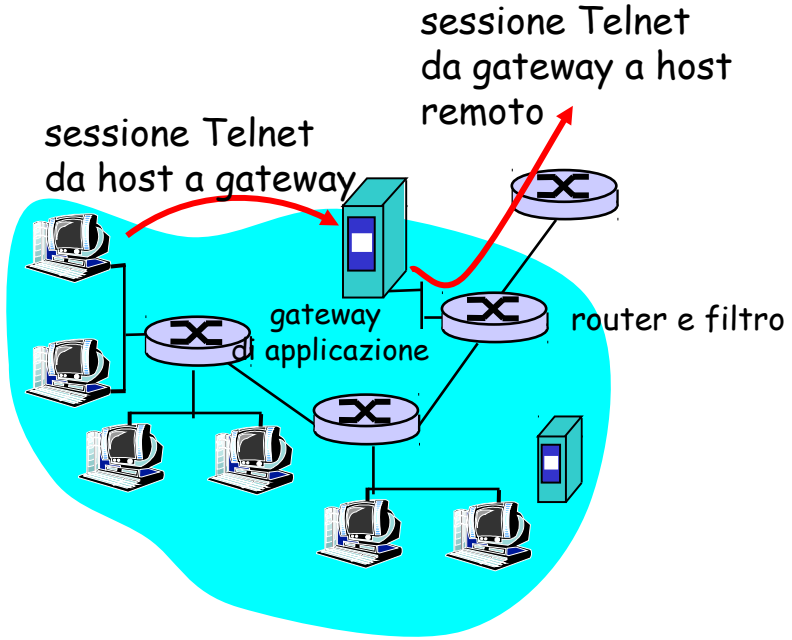
Filtri di pacchetti con memoria dello stato

- Nuova colonna di verifica della connessione

azione	indirizzo sorgente	indirizzo dest	Protoc	porta sorgente	porta destinaz.	bit di flag	controllo conness.
consenti	222.22/16	al di fuori di 222.22/16	TCP	> 1023	80	qualsiasi	
consenti	al di fuori di 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
consenti	222.22/16	al di fuori di 222.22/16	UDP	> 1023	53	---	
consenti	al di fuori di 222.22/16	222.22/16	UDP	53	> 1023	----	X
blocca	tutto	tutto	tutto	tutto	tutto	tutto	

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

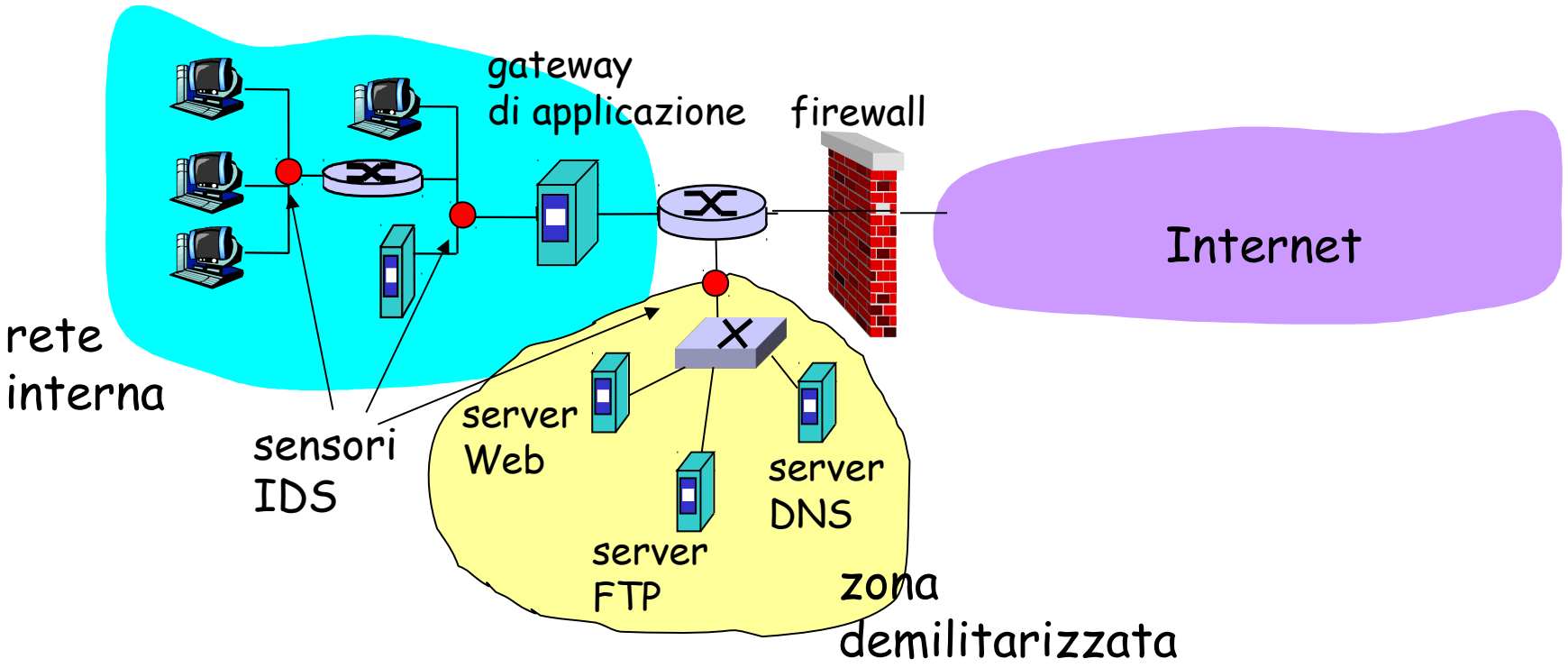
- IP spoofing: azione utilizzata per nascondere la vera identità dell'aggressore.
- Se più applicazioni necessitano di un trattamento speciale, ciascuna avrà il suo gateway di applicazione.
- Il software del client deve sapere come contattare il gateway.
  - Es. deve impostare l'indirizzo IP del proxy 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 tra pacchetti multipli
    - 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)
- IPsec
- 802.11

Sicurezza operativa: firewall e IDS