Sicurezza

- Sicurezza dei sistemi informatici
- Virus, batteri, …
- Contromisure

Sicurezza dei sistemi informatici

- In termini generali la sicurezza non è solo un problema software, la sicurezza ha molti aspetti, due fra i più importanti sono:
  - la perdita dei dati
  - le intrusioni
- La perdita dei dati può avere molte cause:
  - Eventi accidentali: incendi, terremoti, guerre, topi, insetti ...
  - Errori hardware e software: malfunzionamenti della CPU, dei dischi, dei nastri; errori nei programmi, errori di comunicazione
  - Errori umani: dati non corretti, montaggio sbagliato di nastri o dischi, perdita di nastri ...

Sicurezza di rete

- Il campo della sicurezza di rete si occupa di:
  - malintenzionati che attaccano le reti di calcolatori
  - come difendere le reti dagli attacchi
  - come progettare architetture immuni da attacchi
- Internet non fu inizialmente progettato per la sicurezza
  - Visione originaria: “un gruppo di utenti che si fidavano l’uno dell’altro collegati a una rete trasparente”
  - I progettisti del protocollo Internet stanno recuperando

Minacce alla sicurezza

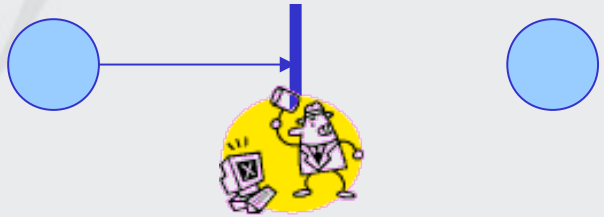
- Attacchi passivi
  - Accesso a informazioni riservate
  - Analisi del traffico
- Attacchi attivi
  - Masquerade
  - Replay
  - Modifica
  - Negazione del servizio

Minacce alla sicurezza

- Segretezza: proteggere i dati dagli attacchi passivi
- Integrità: richiede che le risorse di un sistema di elaborazione possano essere modificate solo da parti autorizzate
- Disponibilità: richiede che le risorse di un sistema di elaborazione possano essere accessibili solo da parti autorizzate
- Autenticità: richiede che un sistema di elaborazione possa verificare l'identità degli utenti
- Non-ripudio: impedire che mittente o destinatario neghino che sia stato trasmesso il messaggio
- Controllo di accesso: capacità di controllare e limitare l'accesso ai sistemi host
- …

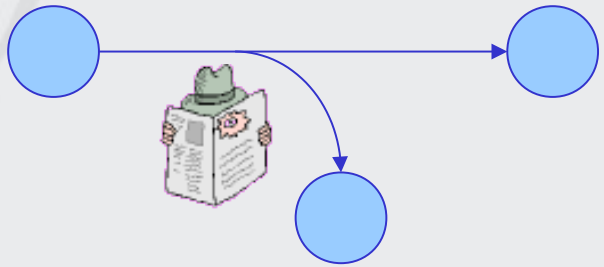
Tipi di minaccia

- **Interruzione**
  - **Una risorsa del sistema è distrutta o viene resa inutilizzabile**
  - **È un attacco alla disponibilità**
    - Distruzione di hardware
    - Taglio di una linea di comunicazione
    - Disabilitazione di software di gestione



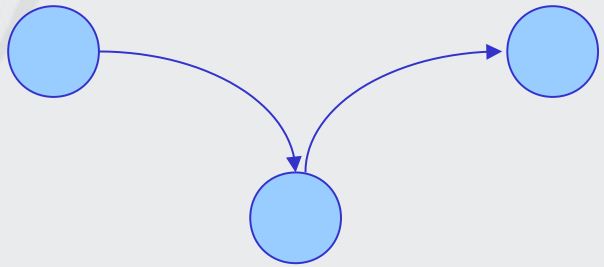
Tipi di minaccia

- **Intercettazione**
  - **Una parte non autorizzata ottiene l'accesso ad una risorsa**
  - **È un attacco alla riservatezza**
    - Intercettazione di dati in rete
    - Copia di dati e programmi non autorizzata



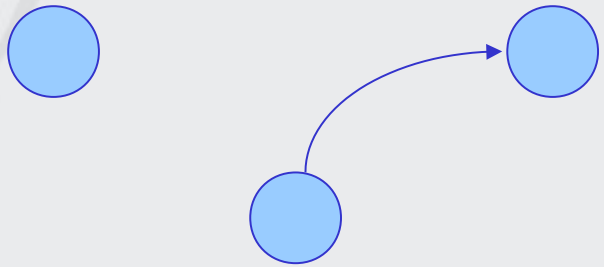
Tipi di minaccia

- **Modifica**
  - **Una parte non autorizzata non solo ottiene una risorsa, ma anche la modifica**
  - **È un attacco alla integrità**
    - Modificare un file
    - Alterare il comportamento di un programma
    - Modificare il contenuto di un messaggio in rete



Tipi di minaccia

- **Generazione**
  - **Una parte non autorizzata inserisce oggetti contraffatti**
  - **È un attacco alla autenticità**
    - Aggiungere record ad un file
    - Inserire messaggi falsi in rete



Programmi perniciosi

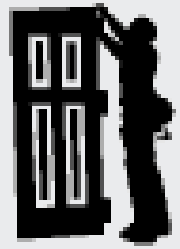
- Dipendenti da un programma ospite
  - Porzioni di programmi che non possono esistere indipendentemente da altri programmi, utility o programmi di sistema
- Indipendenti
  - Programmi indipendenti che possono essere eseguiti dal sistema operativo

Tassonomia dei programmi perniciosi

[Bowles and Pelaez, 1992]

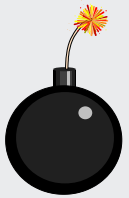
Trapdoor

- È un punto di ingresso nascosto nel sistema
- Spesso viene lasciato dall'autore stesso del programma (non necessariamente per scopi fraudolenti)
- È utilizzato per aggirare le comuni procedure di protezione
- Normalmente è molto difficile da rilevare



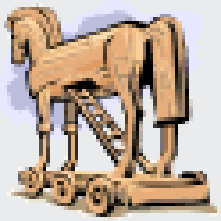
Bomba Logica

- Una porzione di codice che verifica il raggiungimento di particolari condizioni
- In caso positivo si attivano funzioni pericolose
- Esempi:
  - cancellare il disco rigido dopo una certa data o in seguito alla modifica di informazioni
  - un programma inserito in un database da un amministratore che si attiva in caso di licenziamento



Cavallo di Troia

- Un programma apparentemente utile che nasconde codice che realizza funzioni pericolose
- Il codice sfrutta il suo ambiente (i privilegi dell'utente)
- È spesso nascosto in programmi apparentemente innocui: login, e-mail, editor, giochi



Virus

- Frammenti di codice inseriti in un programma legittimo
- Progettato per propagarsi in altri programmi e/o nel sistema
- Comune soprattutto nei sistemi mono-utente
  - scarsa protezione dovuta all'architettura
  - negligenza dell'utente

Virus - Protezione

- Programmi antivirus (funzionano solo sui virus noti)
- Precauzioni:
  - utilizzare solo programmi acquistati da fonti fidate
  - evitare la condivisione dei media
  - attivare opzioni di protezione generalmente presenti nei programmi
  - aggiornare gli antivirus molto scrupolosamente

  Esempi:
  - disattivare macro in editor
  - disattivare l'esecuzione automatica nei programmi di mail
  - utilizzare ambienti di esecuzione protetti: esempio applet

Macro Virus

- Una macro è un programma eseguibile inserito in un documento di un word processor o in file di altro tipo
- Indipendenti dal sistema
  - La maggior parte riguarda Microsoft Word
- Infetta documenti, non codice eseguibile
- Si diffonde facilmente

E-mail Virus

- Sono attivati quando si attiva un documento allegato
- Spesso sono scritti in Visual Basic
- Si propagano sfruttando la lista di indirizzi e-mail noti

Batteri e Vermi

- **Batteri:**
  - Programmi che consumano le risorse del sistema replicandosi
  - Si riproducono esponenzialmente, fino a prendere possesso di tutte le risorse
- **Vermi:**
  - Programmi che si replicano e mandano copie di se stessi sulla rete
  - Oltre a replicarsi possono causare danni attivando funzioni pericolose

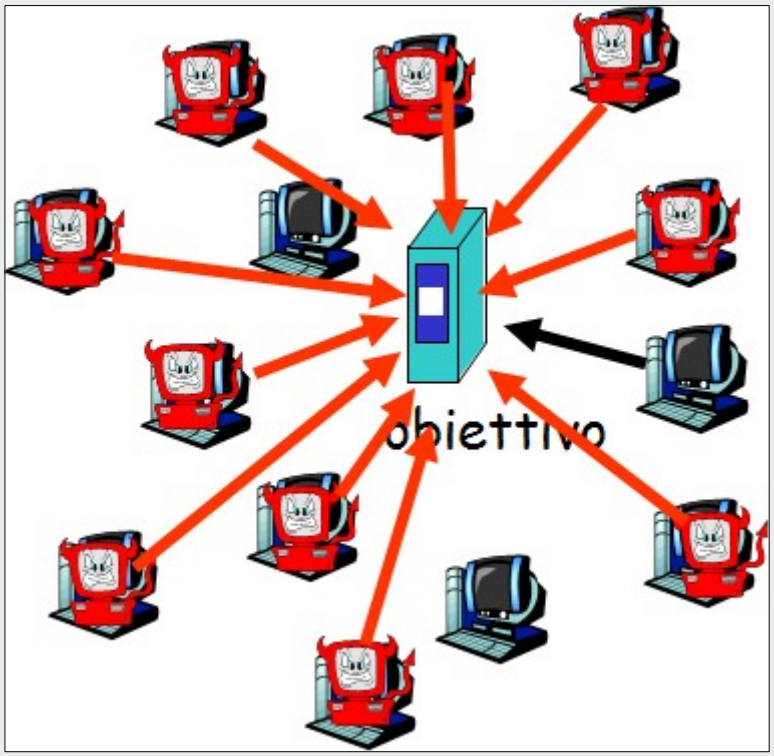
Il malware infetta gli host attraverso Internet

- Il malware può raggiungere gli host per mezzo di virus, worm o cavalli di Troia.
- Malware di spionaggio può registrare quanto viene digitato, i siti visitati e informazioni di upload.
- Gli host infettati possono essere “arruolati” in botnet, e usati per lo spamming e per gli attacchi di DDoS.
- Il malware è spesso auto-replicante: da un host infettato può passare ad altri host

DDoS (Distributed Dos)

- Gli host infettati possono essere “arruolati” in botnet, e usati per lo spamming e per gli attacchi di DDoS
- Gli attaccanti fanno sì che le risorse (server, ampiezza di banda) non siano più disponibili al traffico legittimo sovraccaricandole di traffico artefatto

1) Selezione dell’obiettivo
2) Irruzione negli host attraverso la rete
3) Invio di pacchetti verso un obiettivo da parte degli host compromessi



Password

- Il metodo più classico per controllare gli accessi ad un sistema è l'uso della coppia

  userid, password

- La parola d'ordine crittografata viene solitamente conservata in un file
- Con 7 caratteri ASCII si ottengono 95^7 circa $7x10^{13}$ combinazioni diverse
  con 1000 decriptazioni al secondo occorrono 2000 anni per ottenere un elenco completo
- Normalmente il problema ha una complessità notevolmente inferiore (per colpa degli utenti):
  le password effettivamente utilizzate sono spesso nomi comuni, date di nascita, targhe, sequenze brevi, ...

Problemi con le password

- Spesso è facile violarne la sicurezza
  - password desunta da un elenco di nomi probabili
  - password carpita *(shoulder surfing)*
  - network sniffing
  - condivisione di account
  - account multipli (stesso utente su macchine diverse)

Password: soluzioni

- password generate da programma (ma facili da ricordare)
- cambiamento regolare delle password
- password usa e getta
- password a domanda e risposta (eventualmente con algoritmi)
- identificazione fisica (biometria)
- perché sia efficace il sistema di protezione deve essere accettato dagli utenti (user friendly)

Biometria

- Le caratteristiche considerate devono essere:
  - Universali = tutti devono averle
  - Uniche = due o più individui non possono avere la stessa uguale caratteristica
  - Permanenti = le caratteristiche non variano nel tempo
  - Collezionabili = devono essere misurabili quantitativamente

- Le caratteristiche possono essere:
  - Fisiologiche (caratteristiche fisiche)
  - Comportamentali (azioni che normalmente l'individuo compie)

Caratteristiche fisiologiche

- impronte digitali
- altezza
- peso
- colore e dimensione dell'iride
- retina
- sagoma della mano
- palmo della mano
- vascolarizzazione
- forma dell'orecchio
- fisionomia del volto

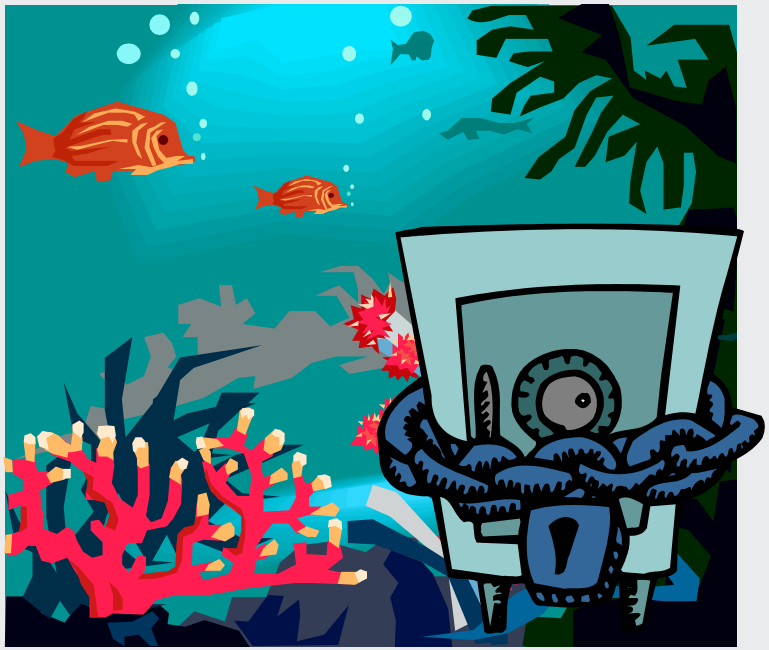
Caratteristiche comportamentali

- impronta vocale
- scrittura grafica
- firma
- stile di battitura sulla tastiera
- movimenti del corpo

Obiettivo della sicurezza

- Obiettivo della Sicurezza non è eliminare il totalmente rischio, ma “ridurlo” a livelli accettabili

- Un PC chiuso in una cassaforte senza chiave in fondo al mare è sicuro, ma non è più utilizzabile!



CVMLab
Computer Vision
& Multimedia Lab

La crittografia

- Motivazioni
- Obiettivi
- Terminologia
- Storia
- Steganografia

Università
degli Studi
di Pavia

Storia della crittografia

- Sparta (Plutarco) scytala
- Cifrario di Cesare (Svetonio)
- Medioevo in Oriente
- Rinascimento in Italia
  - Cicco Simonetta (Sforza) → Primo trattato di decrittazione
  - Serenissima (sala dei segreti)
  - Roma (disco di Leon Battista Alberti) - De cifris (Tre secoli!)
- XVII - XVIII secolo (Vienna, le camere nere)

Storia della crittografia

- Ottocento: Kasiski, Kerckhoffs e Babbage
  - Francia
- La seconda guerra mondiale
  - Codice Enigma (Tedesco)
  - A. M. Turing
- Inizio della criptografia moderna (1949): Claude Shannon pubblica Communication Theory of Secrecy Systems su Bell System Technical Journal
- Teoria dell'informazione e informatica
- Reti, algoritmi a chiave pubblica

Crittanalisi

- Le ipotesi fondamentali della crittanalisi sono due:
  - Eventuali attaccanti hanno una perfetta conoscenza dell'algoritmo utilizzato per cifrare il messaggio e di tutti i dettagli della sua realizzazione.
  - Eventuali attaccanti hanno completo accesso al canale di comunicazione e possono pertanto intercettare, interrompere, creare o modificare qualsiasi flusso di dati.
- I possibili attacchi vengono suddivisi nelle classi:
  - Ciphertext-only attack
  - Known-plaintext attack
  - Chosen-plaintext attack

Scopi della crittografia

- Si vuole garantire:
  - Confidenzialità: le informazioni sono accessibili solo da persone autorizzate
  - Autenticazione: l'identità dell'interlocutore è garantita
  - Integrità: garanzia della non alterazione dell'informazione
  - Non ripudiabilità: garanzia che nessun soggetto della comunicazione possa disconoscere di esserne l'autore

Criteri generali

- L'algoritmo di cifratura può essere noto (principio di Kerckhoffs)
- Nessun sistema è assolutamente sicuro
- Si deve rendere praticamente irrealizzabile l'attacco
  - Sistemi teoricamente sicuri (es. one-time pad) non praticabile come soluzione
  - Sistemi computazionalmente sicuri: è antieconomico tentare di aggirare le protezioni

Sistemi computazionalmente sicuri

- Il valore delle informazioni contenute nei messaggi cifrati non deve mai superare i costi stimati per violare l'algoritmo utilizzato
- Il periodo temporale durante il quale le informazioni cifrate devono essere mantenute confidenziali non deve superare il tempo stimato necessario per violare l'algoritmo

Terminologia

- Criptologia
  - scienza che studia i messaggi segreti
- Crittografia (κριπτοσγραφια): studio dei metodi per rendere un messaggio non intelleggibile a chiunque non sia il legittimo destinatario
  - Lo scopo NON è quello di nascondere un messaggio o di dissimularlo (steganografia)
- Crittanalisi: studio dei metodi per violare il segreto di un messaggio cifrato
  - Testo in chiaro vs. testo cifrato
  - Crittografo vs. crittanalista
  - Cifratura vs. decifratura oppure decrittazione

Steganografia

- Lo scopo è nascondere l'esistenza del messaggio
- Marcatura di caratteri: marcare caratteri con inchiostro speciale su un testo scritto o stampato su carta
- Inchiostro invisibile
- Perforazioni invisibili su carta

Steganografia: esempio

- Il formato Kodak Photo CD alla massima risoluzione visualizza 2048 X 3072 pixel a 24 bit.
  - Modificando a piacere il bit meno significativo posso nascondere 2.3 Mbyte di messaggio in una sola immagine
  - L'immagine però occupa 18Mbyte

Steganografia

- Svantaggi:
  - richiede molti dati per nascondere pochi bit di informazione
  - una volta scoperto il meccanismo, è da buttare
  - può essere sfruttato se le due parti che comunicano devono nascondere la loro connessione, piuttosto che il messaggio stesso
  - applicazione nel copyright
  - watermarking nelle immagini

Watermarking

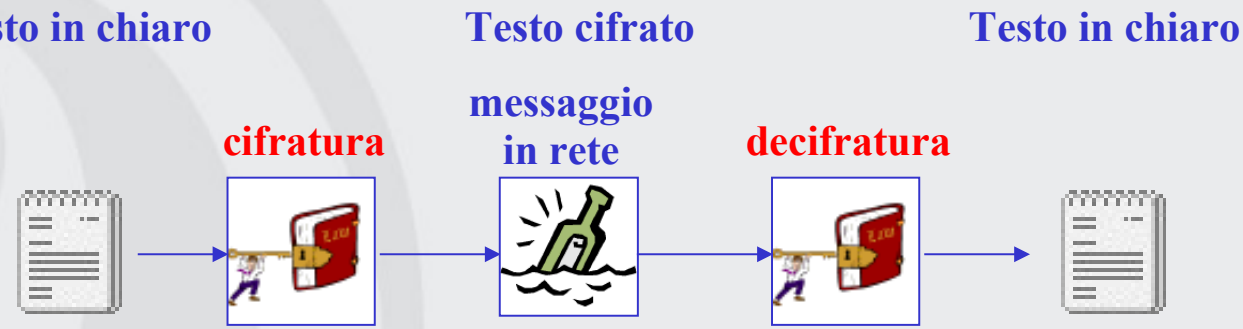
Crittografia

- **I sistemi crittografici sono generalmente classificati in base a tre criteri:**
  - **il tipo di operazioni per passare da testo in chiaro a testo cifrato (sostituzioni, trasposizioni, ecc.)**
  - **Il numero di chiavi usate (le funzioni di cifratura e di decifratura utilizzano una o più chiavi K per produrre il risultato).**
    - Algoritmi simmetrici o asimmetrici.
  - **Il modo in cui si elabora il testo in chiaro: a blocchi o a stream (sw, hw o real-time)**

Crittografia

- Si distinguono due campi della crittografia: crittografia convenzionale e a chiave asimmetrica
- Utilizzando una notazione matematica ed indicando con M il testo in chiaro, con C il testo cifrato, con E( ) la funzione di cifratura e con D( ) quella di decifratura, un sistema convenzionale basato su una sola chiave k può essere descritto dalle equazioni:
  - $E_K(M) = C$
  - $D_K(C) = M$
- Con la proprietà che:
  - $D_K(E_K(M)) = M$
- Si suppone che un crittanalista conosca E e D, e cerchi di stimare M, K o entrambe.

Cifratura a Chiave Simmetrica



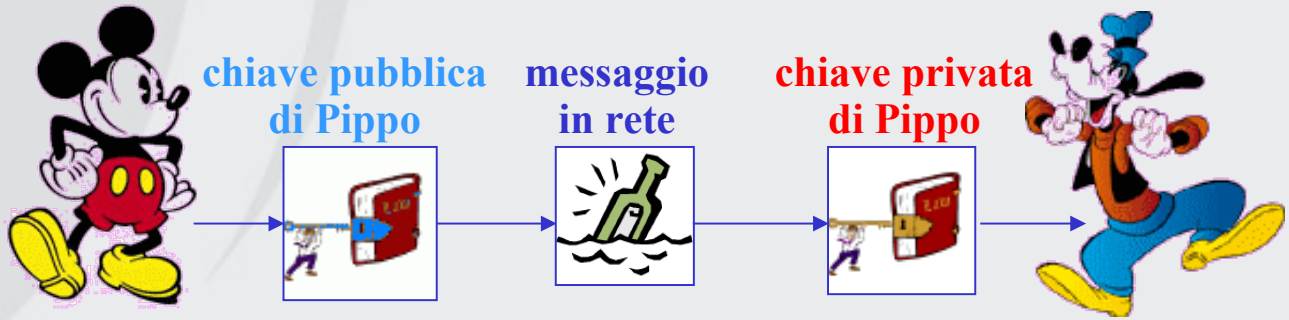
Pippo e Topolino
condividono
la stessa chiave

Problema: come condividere la chiave

Il problema della scalabilità

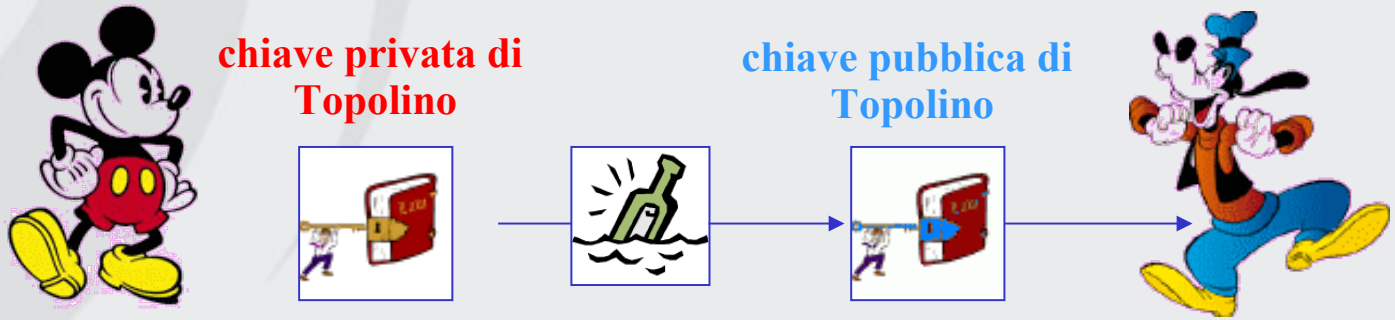
Cifratura a chiave pubblica

- Topolino vuole mandare un messaggio segreto a Pippo
  - Topolino usa la chiave pubblica di Pippo per cifrare il messaggio
  - Solo Pippo è in grado di decodificare il messaggio
  - Pippo tuttavia non può essere sicuro dell'identità di Topolino



Messaggi firmati

- Topolino vuole mandare un messaggio firmato a Pippo
  - Topolino usa la sua chiave privata per cifrare il messaggio
  - Pippo è in grado di decodificare il messaggio usando la chiave pubblica di Topolino
  - Solo Topolino poteva inviare quel messaggio
  - Il messaggio però non è segreto tutti lo possono leggere



Messaggi firmati

Hash( )

D(Hash( ))

chiave pubblica di Pippo

chiave privata di Topolino

Messaggio in rete

chiave privata di Pippo

Hash( )

Sono uguali?

D(Hash( ))

chiave pubblica di Topolino

Funzioni hash

- Dato un messaggio di lunghezza arbitraria produce una stringa di lunghezza predefinita
- Data una stringa hash è difficile trovare un messaggio compatibile
- Funzioni hash comuni:
  - MD5 (Message Digest Rivest 1992) 128 bit
  - SHA1 (Secure Hash Algorithm NIST 1995) 160 bit
    - Sha256 256 bit
    - Sha512 512 bit

Funzioni hash

```
$ md5sum <<< ciao
5f423b7772a80f77438407c8b78ff305 *-

$ md5sum <<< Ciao
Bba5159eba60f759a28b36834acf656c *-

$ sha1sum <<< ciao
953ed62a3246f2dbd96cdbfc0ec0d92b5cb2f5a8 *-

$ sha256sum <<< ciao
6f0378f21a495f5c13247317d158e9d51da45a5bf68fc2f366e450deafdc8302 *-

$ sha512sum <<< ciao
d380e3a08107af3a45bbe2539d9cc8d05a3eaf4a82a91bcc46bf8ca33fb72d37c2ec89893da
7ba76d9f2794155896760a23d5fe937de2e7a8cda52d0b8a0d62e *-
```

Problema: *uomo nel mezzo*

Tecniche convenzionali

- Cifrari a sostituzione: una lettera del testo in chiaro è sostituita da una o più lettere o numeri o simboli.
- Se il testo in chiaro è visto come una sequenza di bit, allora ciò implica la sostituzione di blocchi di bit (pattern) in chiaro con pattern di bit cifrati.
- Esempio storico: il cifrario di Cesare
  - chiaro:

    incontriamoci alle sette
  - ogni lettera è sostituita dalla lettera di tre posti successivi nell'alfabeto:

    LQFRQWULDPRFLDOOHVHWWH

Tecniche convenzionali

- Assumendo un valore numerico a ogni lettera, per ogni lettera del testo in chiaro p si sostituisce la lettera cifrata C tale che
  - C = E(p) = (p + 3) mod 26
  - C = E(p) = (p + k) mod 26 k assume valori da 1 a 25
  - La decifrazione è p = D(C) = (C - k) mod 26
- Possibile crittanalisi di tipo brute - force
  - gli algoritmi di E e D sono noti
  - la chiave k assume un numero di valori limitato
  - il linguaggio del testo in chiaro è noto

Cifrature monoalfabetiche

- Per aumentare lo spazio delle chiavi si esegue una sostituzione arbitraria

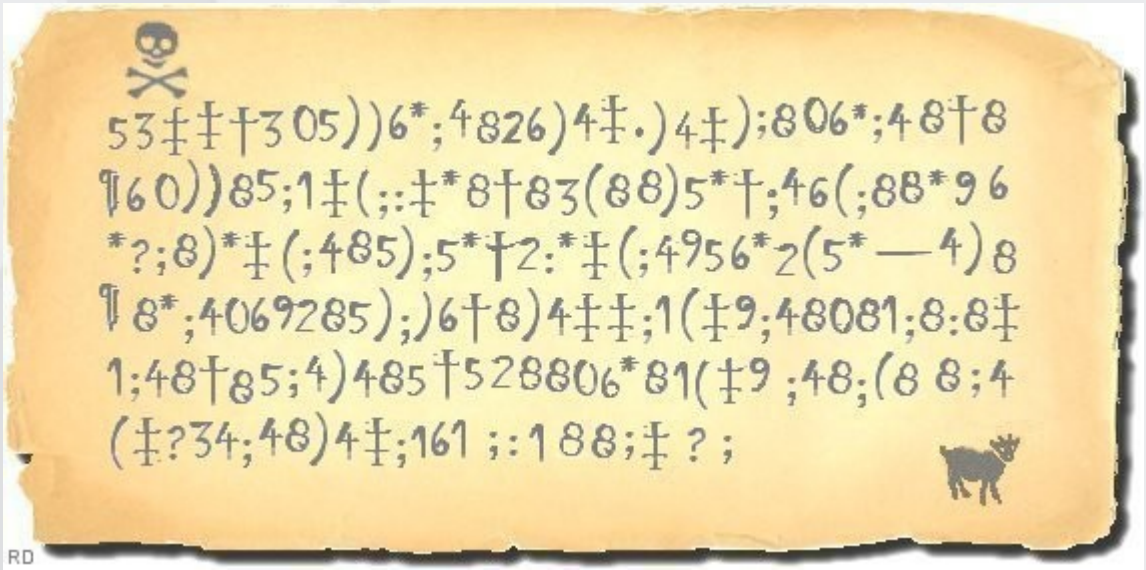
```
a b c d e f g h i l m n o p q r s t u v w x y z
h k l p o u t r e d f s w q a z c v b n m .....
```

- In questo caso il testo cifrato può essere ottenuto a una qualunque delle permutazioni di 26 caratteri, ovvero 26! = 4 X 10^{26} possibili chiavi.
- Non è ancora abbastanza sicuro perché si sfrutta la regolarità del linguaggio naturale

E 12.75	S 6.00	P 2.75	K 0.50
T 9.25	D 4.25	Y 2.75	X 0.50
R 8.50	H 3.50	G 2.00	Q 0.50
N 7.75	C 3.50	L 3.75	J 0.25
I 7.75	F 3.00	W 1.50	Z 0.25
O 7.50	U 3.00	V 1.50	
A 7.25	M 2.75	B 1.25	

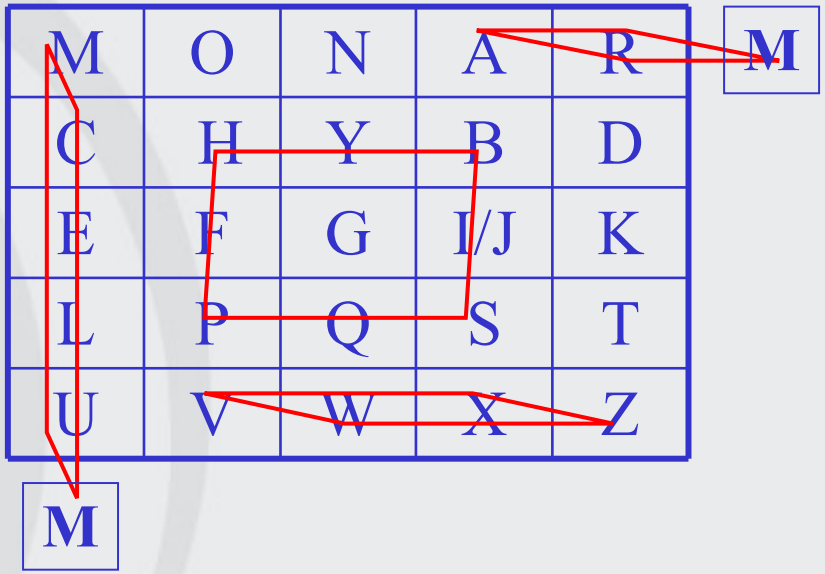
Cifrature monoalfabetiche

- Vedi lo Scarabeo d'oro – Edgar Alan Poe



Cifrario Playfair

- Da una parola chiave si crea una matrice del tipo



Le doppie nel testo in chiaro sono separate da una lettera "filler"

cc → CZC

bp → HS

vx → WZ; ar → RM; mu → CM (righe e colonne si considerano periodiche)

Cifrari polialfabetici

- Partono da un insieme di cifrari monoalfabetici.
  - Una chiave determina quale cifrario usare
- Esempio: cifrario di Vigenére
  - Si tratta di una tabella di 26 cifrari di Cesare
  - Data una lettera chiave x e una lettera in chiaro y, la lettera cifrata corrispondente è quella corrispondente all'intersezione tra x e y

Cifrari polialfabetici

- Devo avere una chiave lunga quanto il testo da cifrare (soluzione: ripetizione)

```
chiave:           paviapaviapavia
testo chiaro:     dalleduealletre
testo cifrato:    sajtesuci.......
```

```
A: ABCDEFGHIJKLMNOPQRSTUVZ
B: BCDEFGHIJKLMNOPQRSTUVZA
C: CDEFGHIJKLMNOPQRSTUVZAB
...
I: IJKLMNOPQRSTUVZABCDEFGH
...
P: PQRSTUVZABCDEFGHIJKLMNO
...
V: VZABCDEFGHIJKLMNOPQRSTU
```

Tecniche a trasposizione

- I cifrari a trasposizione non effettuano sostituzioni, ma una permutazione delle lettere del testo in chiaro (implementazione: macchine a rotori)

```
chiave:        4 3 1 2 5 6 7
chiaro:        a t t a c k p
               o s t p o n e
               d u n t i l t
               w o a m x y z
cifrato: ttnaaptmtsuoaodwcoixknlypetz
```

Un cifrario perfetto

One-time pad, Gilbert Vernam, 1917

$$C = M \oplus K$$

0 1 1 0 1 0 0 1 0 1 1 1	**messaggio**
1 0 1 0 0 0 1 1 1 0 1 0	**chiave** (sequenza di bit casuale)
1 1 0 0 1 0 1 0 1 1 0 1	**testo cifrato**

M e C sono indipendenti (il testo cifrato non dà alcuna informazione utile sul messaggio)

Messaggio e chiave hanno la stessa lunghezza
La chiave si può usare una sola volta

Un cifrario perfetto

- Si pensi ad un cifrario polialfabetico con chiave lunga come il testo:
  - Testo criptato: wg ubsokwebalk a swqiu
  - Possibile testo: ci incontriamo a Pavia
  - Possibile testo: li incontriamo a Crema
- Qualunque testo della stessa lunghezza è lecito

DES (Data Encryption Standard)

- adottato nel 1977 come standar dal NIST (National Institute of Standards and Technology)
- utilizza una chiave simmetrica di 56 bit
- codifica blocchi di 64 bit

- Attacco brute-force
  - Un'operazione di cifratura DES per μs: 2^{55} μs = 1142 anni
  - 10^6 operazioni di cifratura DES per μs 10.01 h

- oggi è considerato obsoleto

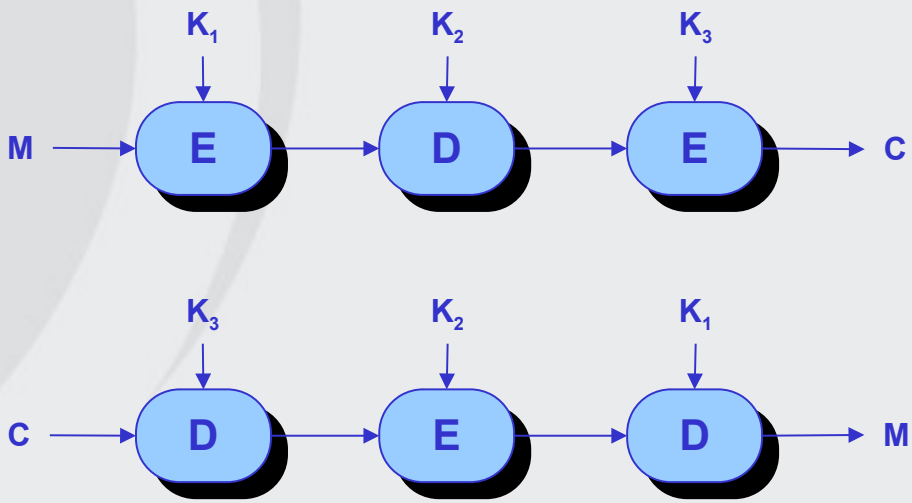
Tempo medio per una ricerca completa

Dimensione della chiave in bit	Numero di possibili chiavi	Tempo necessario	
		1 decifratura/μs	10^6 decifrature/μs
32	4.3×10^9	36 minuti	2.1 ms
56	7.2×10^{16}	1142 anni	10 ore
128	3.4×10^{38}	5.4×10^{24} anni	5.4×10^{18} anni
168	3.7×10^{50}	5.9×10^{36} anni	5.9×10^{30} anni

$$T_{medio} = \frac{1}{2} 2^{nbit} / \text{decifrature\_per\_secondo}$$

Triplo DEA

- **Si usano tre chiavi e tre esecuzione dell'algoritmo DES (cifratura-decifratura-cifratura)**
  - $C = E_{K3}(D_{K2}(E_{K1}(M)))$
    - $E_K(X)$ = cifratura di X con la chiave K
    - $D_K(Y)$ = decifratura di Y con la chiave K
- **Lunghezza effettiva della chiave: 168 bit**



Cifratura a chiave pubblica

- L'algoritmo RSA prende il nome dai tre inventori: Ron Rivest, Adi Shamir, Len Adleman (MIT)
- La chiavi sono due coppie (D, N) e (E, N) dove N è il prodotto di due numeri primi p e q con
  - $ED \bmod (p-1)(q-1) = 1$
  - $C = m^E \bmod N$
  - $D = C^D \bmod N = m = m^{ED} \bmod N$

- La conoscenza dell'algoritmo, di una delle chiavi e di esempi di testo cifrato non è sufficiente per determinare l'altra chiave
  - Noti N e D è computazionalmente difficile ricavare E
  - Si sfrutta la funzione di Eulero $\Phi(N)$ (numero di interi positivi minori di N e primi rispetto a N, $\Phi(N)= (p-1)(q-1)$)

RSA: cifratura e decifratura

- Testo in chiaro: M < n
  - p=7,q=17,e=5, d=77, n=119, M=19
- Testo cifrato: $C=M^e \bmod n$
  - $19^5 \,\%\, 119 = 2476099 \bmod 119 = 66$
- Testo in chiaro: $M=C^d \bmod n$
  - $66^{77} \bmod 119 = 19$

Intermediario di fiducia

Problema per la crittografia a chiave simmetrica:

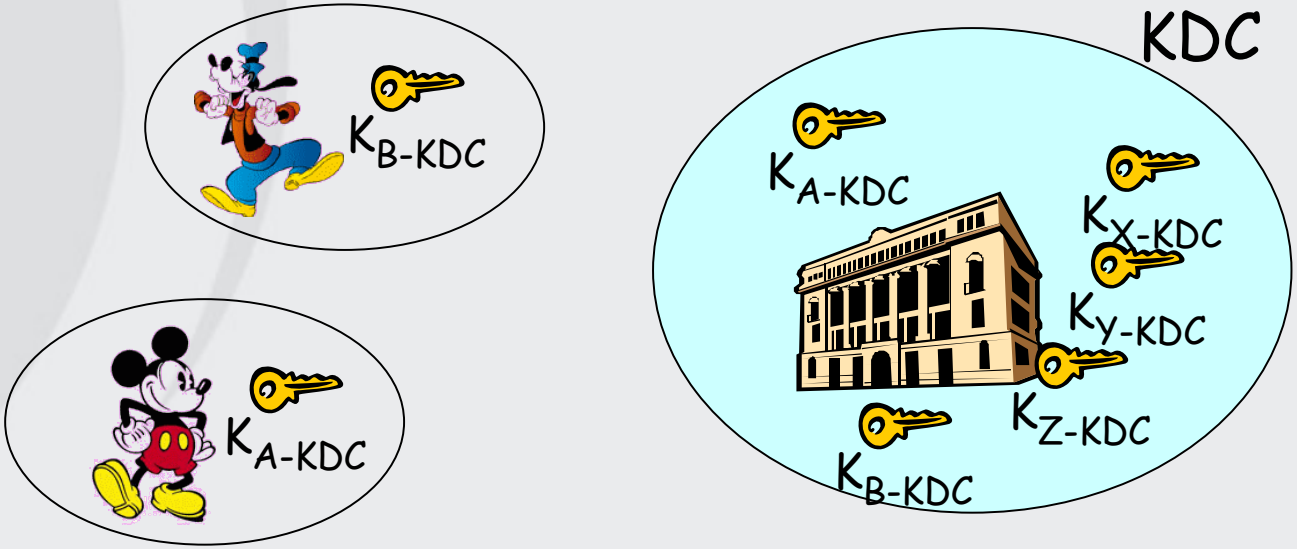
- Come possono le due parti concordare le chiavi prima di comunicare?
- Soluzione:
  - Un centro di distribuzione delle chiavi (KDC, key distribution center) di fiducia funge da intermediario tra le due entità

Problema per la crittografia a chiave pubblica:

- Quando Topolino riceve la chiave pubblica di Pippo (attraverso un CD, il sito web o via e-mail), come fa a sapere che è veramente la chiave pubblica di Pippo?
- Soluzione:
  - Autorità di certificazione (CA, certification authority)

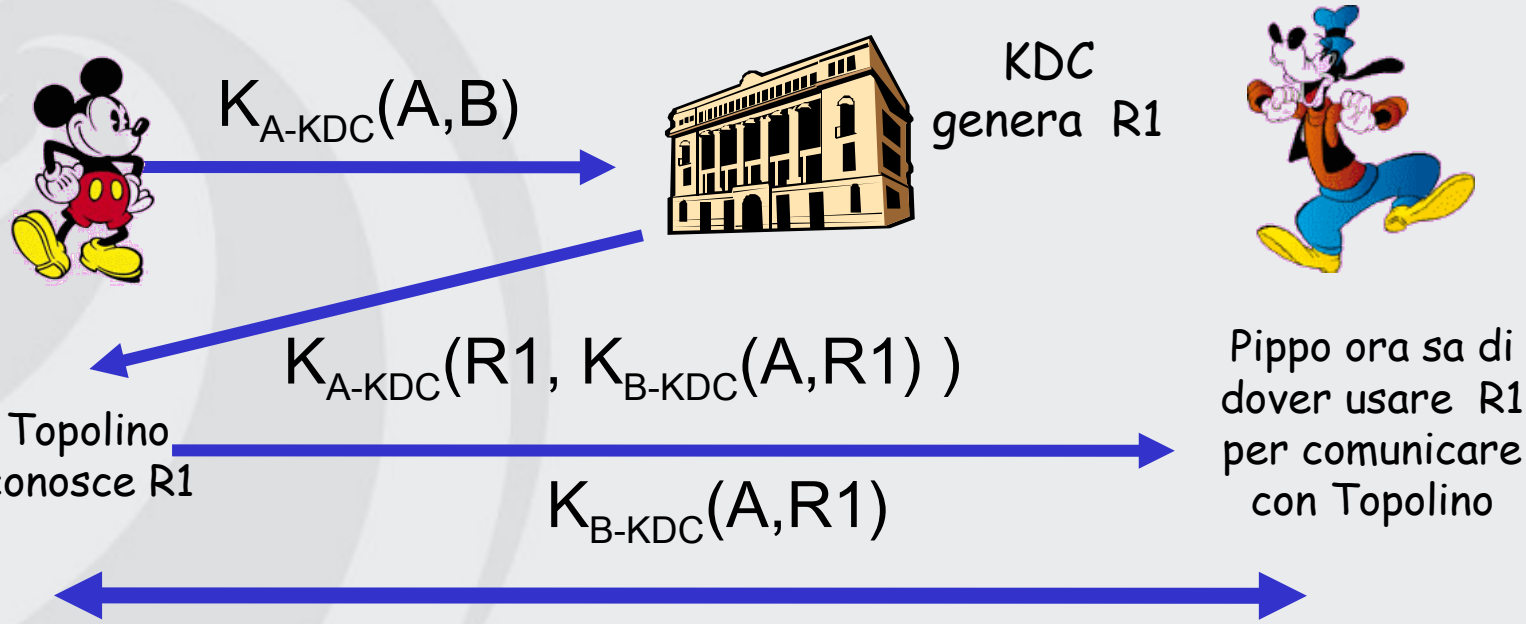
Centro di distribuzione delle chiavi (KDC)

- Topolino e Pippo vogliono comunicare protetti dalla crittografia a chiave simmetrica, ma non sono in possesso di una chiave segreta condivisa.
- KDC: è un server che condivide diverse chiavi segrete con ciascun utente registrato (molti utenti)
- Topolino e Pippo conoscono solo la propria chiave individuale, $K_{A\text{-}KDC}$ $K_{B\text{-}KDC}$, per comunicare con KDC



Centro di distribuzione delle chiavi (KDC)

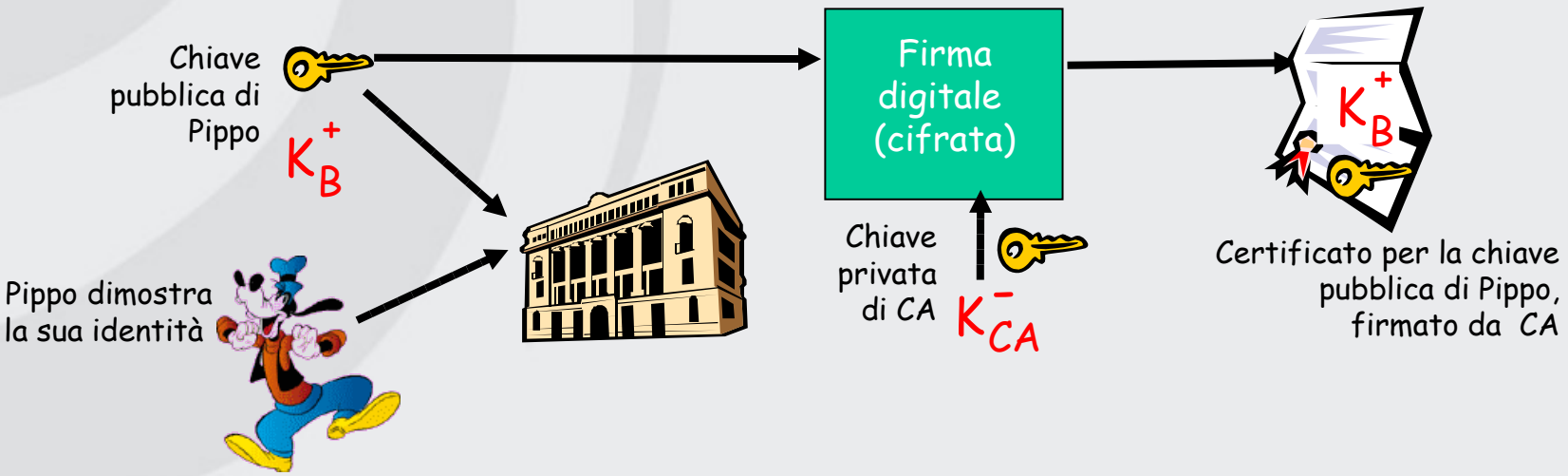
In che modo KDC consente a Topolino e Pippo di determinare la chiave segreta simmetrica condivisa per comunicare tra loro?



Topolino e Pippo comunicano usando R1 come chiave di sessione per la cifratura simmetrica condivisa

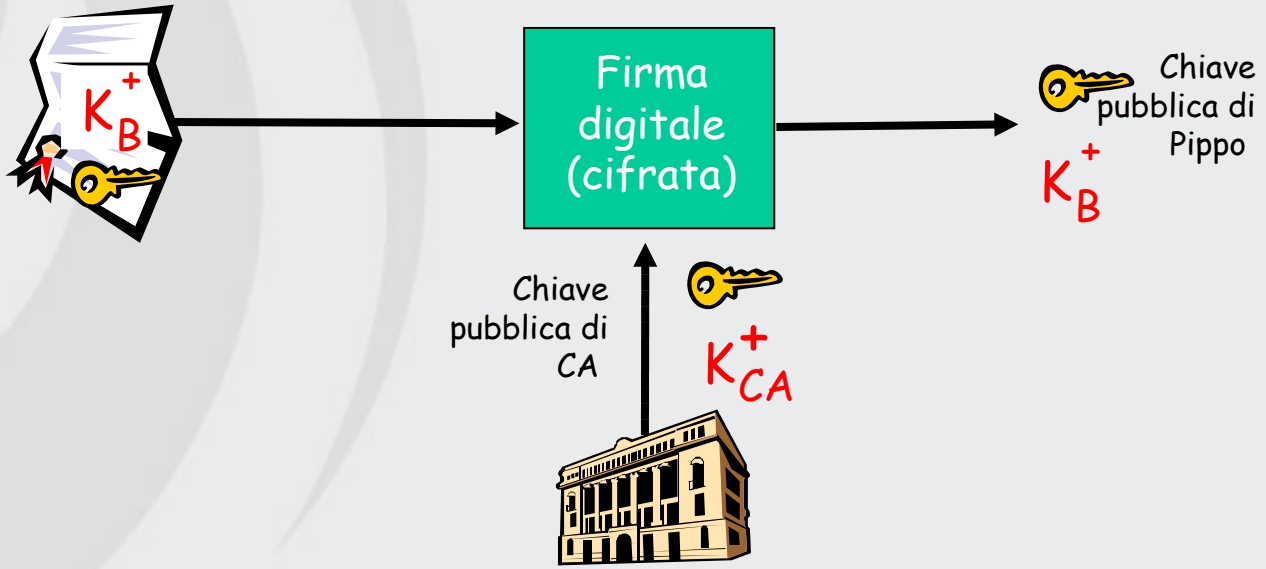
Autorità di certificazione

- 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")



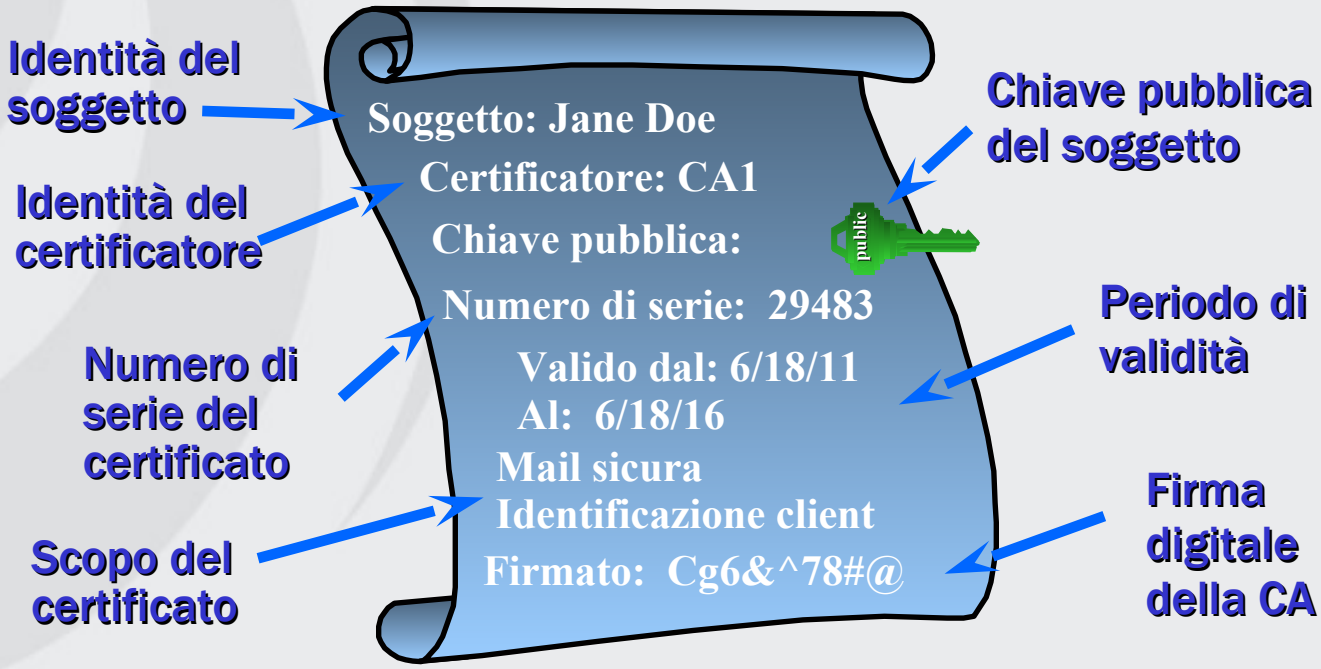
Autorità di certificazione

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



Certificati

- Legano l'identità di un soggetto ad una chiave pubblica
  - La chiave pubblica del soggetto è criptata con la chiave privata di CA (CA firma il certificato)



Certification Authority

- Una CA può erogare certificati a:
  - Se stessa (Root)
  - Un'altra CA (Subordinate)
  - Soggetti finali (utenti, computer)
- Una CA "fidata" deve fornire
  - Una prova della sua identità
  - Lista dei certificati revocati
  - Politiche di erogazione dei certificati

CVMLab
Computer Vision
& Multimedia Lab

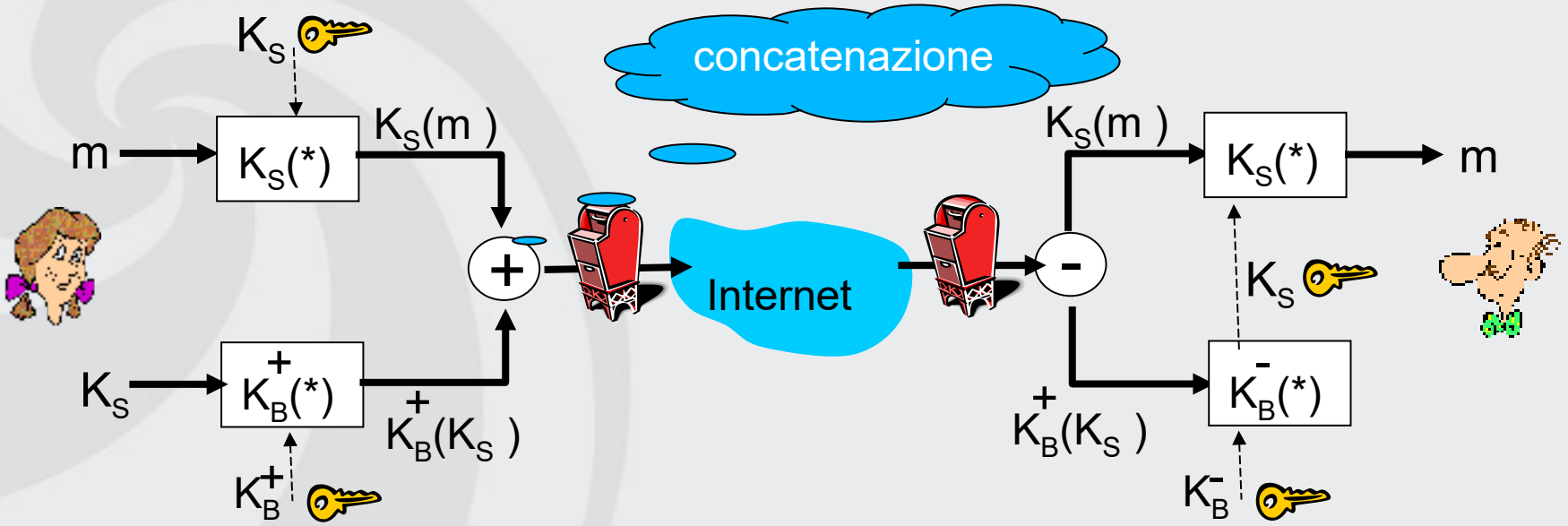
E-Mail sicura

- Kurose 8.4

Università
degli Studi
di Pavia

E-Mail sicura - mittente

Alice vuole spedire una e-mail segreta a Bob

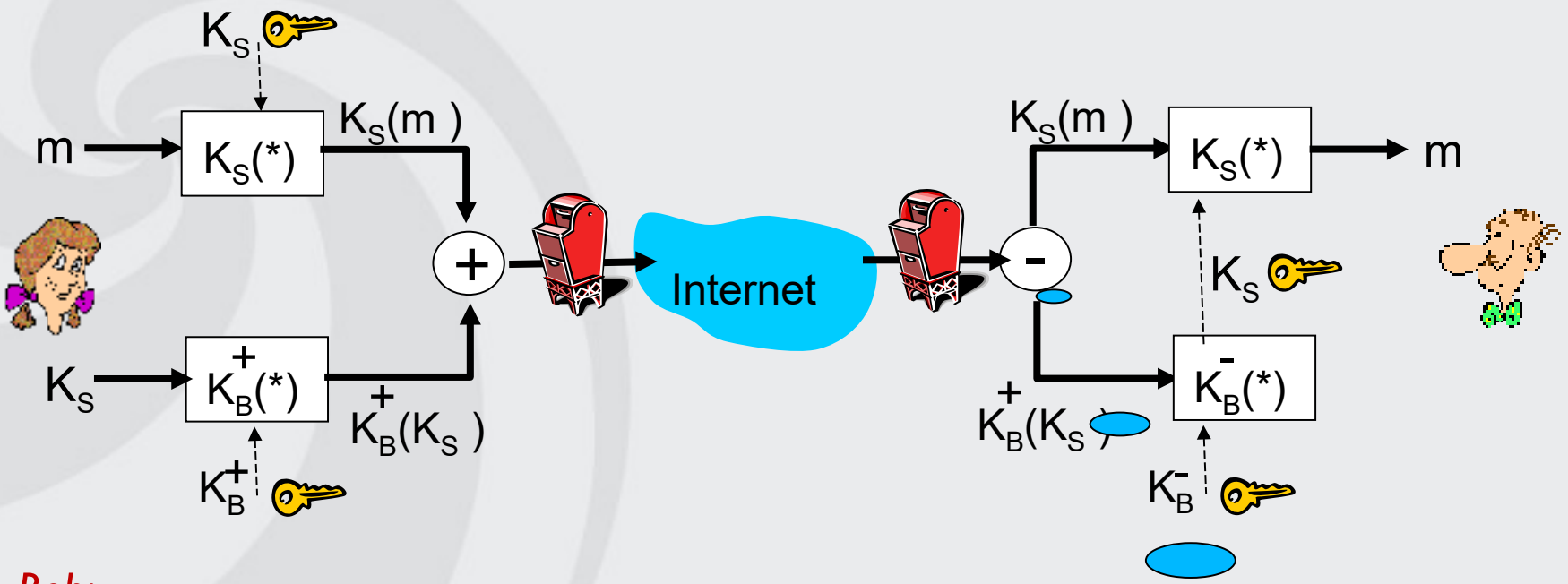


Alice:

- Genera casualmente una chiave simmetrica K_S
- Codifica il messaggio con K_S (per efficienza)
- Codifica K_S con la chiave pubblica di Bob
- Spedisce $K_S(m)$ e $K_B^+(K_S)$ a Bob

E-Mail sicura - destinatario

Alice vuole spedire una e-mail segreta a Bob



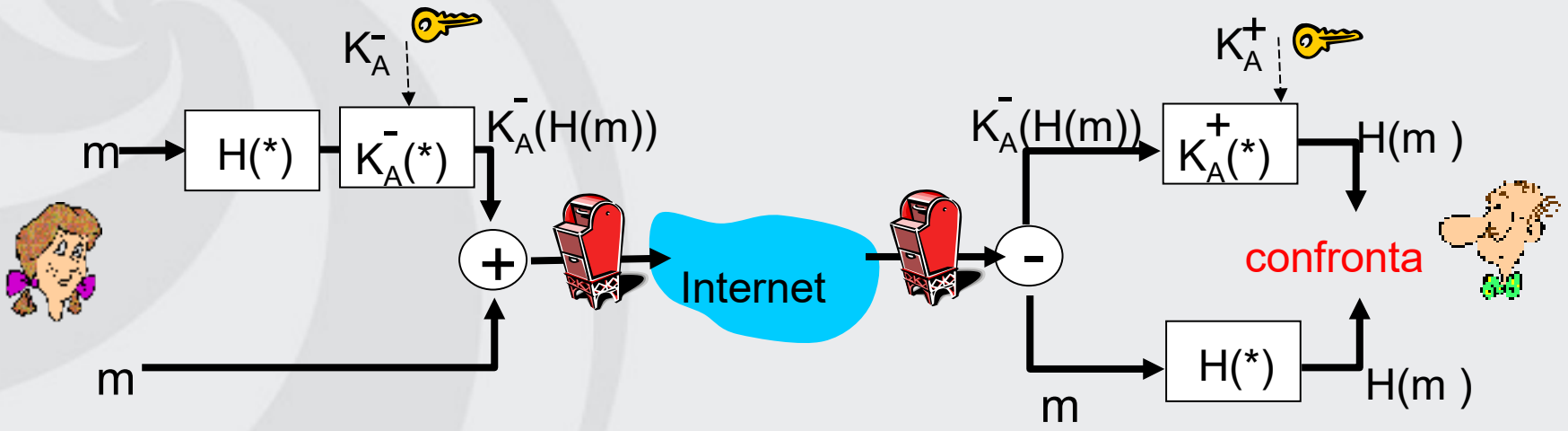
Bob:

- Usa la sua chiave privata per ottenere K_S
- Usa K_S per decifrare $K_S(m)$ e ottenere m

Operazione opposta alla concatenazione

E-mail autenticata

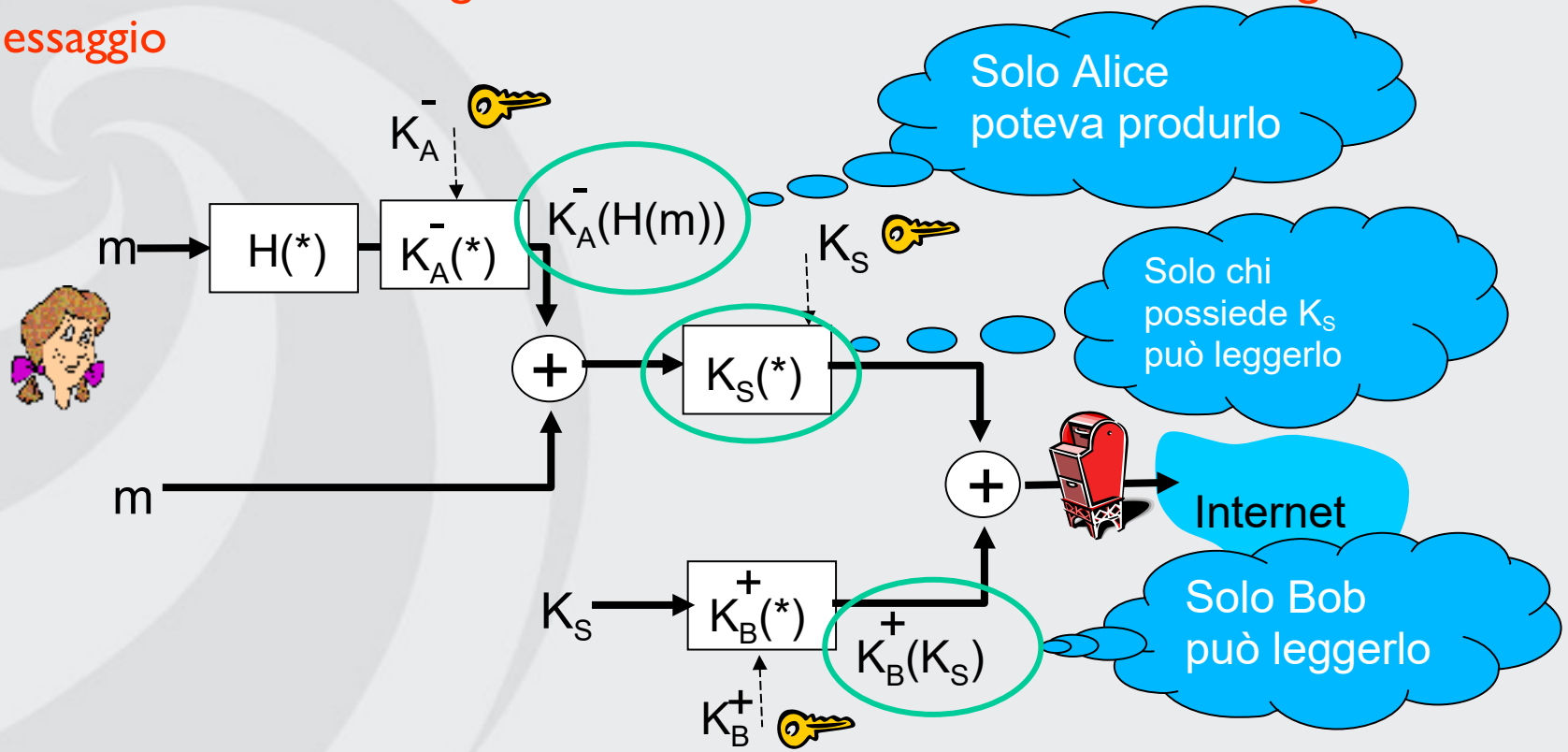
Alice vuole garantire autenticazione del mittente, integrità del messaggio



- Alice usa una firma digitale (hash) del messaggio
- Spedisce messaggio e firma (in chiaro)

E-mail sicura (versione finale)

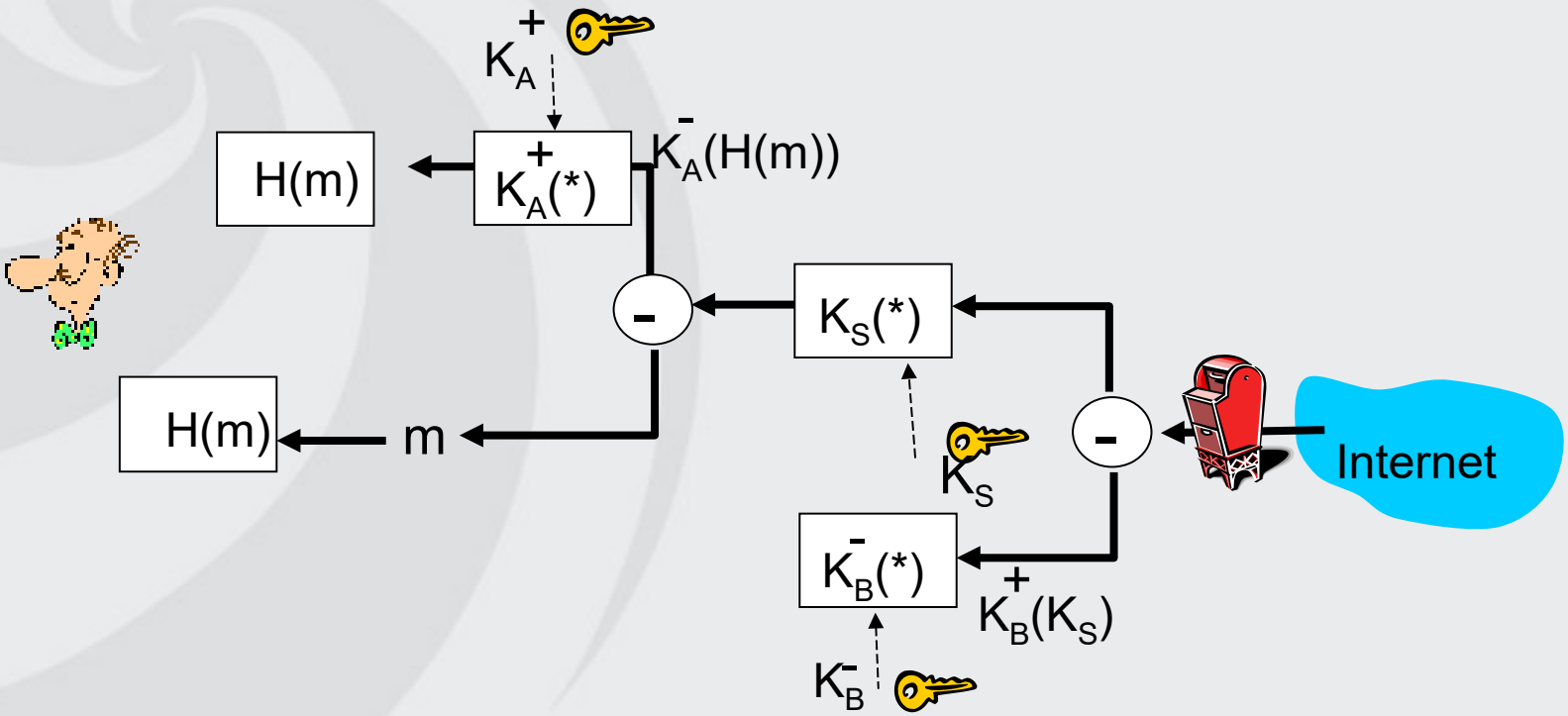
Alice vuole ottenere segretezza, autenticazione del mittente, integrità del messaggio



Alice usa tre chiavi: la sua chiave privata, la chiave pubblica di Bob, una chiave simmetrica creata per l'occasione

E-mail sicura (versione finale)

Alice vuole ottenere segretezza, autenticazione del mittente, integrità del messaggio

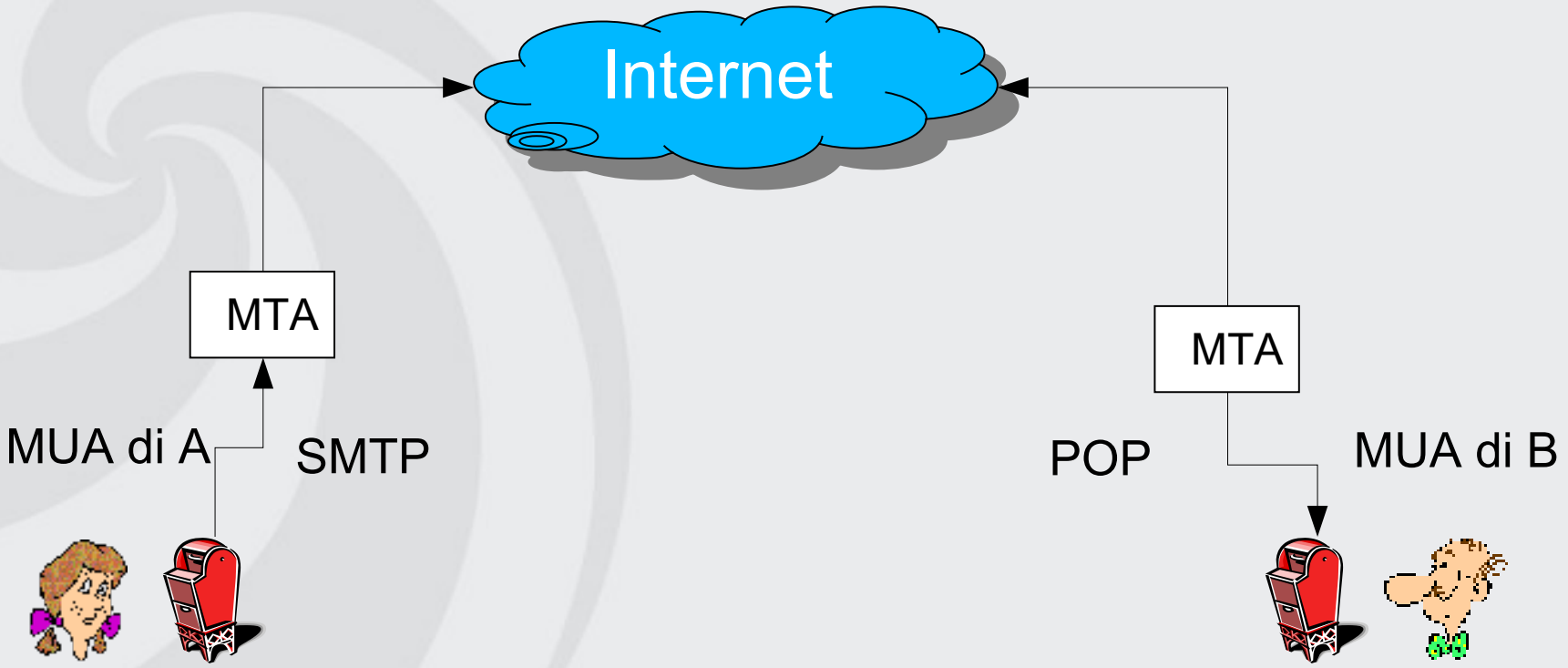


Bob userà tre chiavi: la sua chiave privata, la chiave simmetrica ricevuta, la chiave pubblica di Alice

Posta Elettronica Certificata (PEC)

- La PEC è un sistema di posta elettronica con la quale si fornisce al mittente documentazione elettronica, con valore legale, attestante l'invio e la consegna di documenti informatici
- "Certificare" l'invio significa fornire al mittente, dal proprio gestore di posta, una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio
- "Certificare" la ricezione significa inviare al mittente la ricevuta di avvenuta (o mancata) consegna con precisa indicazione temporale

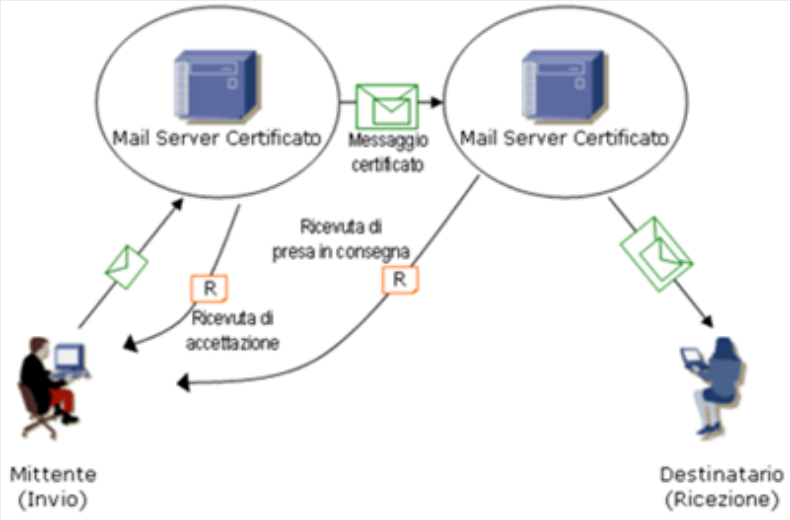
Posta elettronica ‘ordinaria’



PEC sistema di invio e di ricezione

- Rispetto allo schema generale della posta elettronica “ordinaria” ora gli MTA (Mail Transfer Agent) sia del mittente che del destinatario sono entrambi certificati secondo procedure e regolamenti stabiliti per legge

- Le varie ricevute (accettazione, presa in consegna e ricezione) sono garantite dal sistema



PEC sistema di invio e di ricezione

- Da un punto di vista più tecnico i messaggi di posta elettronica certificata utilizzano il protocollo S/MIME, la sicurezza del colloquio tra mittente e destinatario viene garantita in tutte le fasi dall'invio alla ricezione della mail certificata
  - Il mittente deve identificarsi presso il gestore di PEC (autenticazione)
  - L'integrità e la confidenzialità delle connessioni tra il gestore di PEC e l'utente devono essere garantite mediante l'uso di protocolli sicuri (utilizzo di protocolli quali TLS - Transport Layer Security)
  - I messaggi generati dal sistema di PEC sono sottoscritti dai gestori mediate la firma digitale del gestore di posta elettronica certificata
  - Il colloquio tra i gestori deve avvenire con l'impiego del protocollo SMTP su trasporto TLS
  - Il destinatario deve identificarsi presso il gestore di PEC (autenticazione) per potere leggere le mail in arrivo

Quadro normativo

- Il DPR n.68 del 11 febbraio 2005 stabilisce i principi che regolamentano l'uso della Posta Elettronica Certificata
- Queste norme, insieme ad altre ne stabiliscono la validità legale, le regole e le modalità di utilizzo

- il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore

Utilizzi

- La PEC può essere paragonata ad una raccomandata con ricevuta di ritorno con alcune differenze:
  - La conoscenza del mittente cioè della casella del mittente (nel caso della raccomandata non è noto il mittente)
  - La certificazione che il contenuto ricevuto è esattamente quello che era stato inviato

- La PEC può essere utilizzata nella dematerializzazione dei documenti nella pubblica amministrazione garantendone la autenticità, temporalità e producendo documenti che hanno valore legale

Comunicazione privato cittadino - PA

- Il privato cittadino può richiedere su base volontaria una casella di posta elettronica certificata ed utilizzarla (previa dichiarazione) nell'ambito di ciascun procedimento con la Pubblica Amministrazione (PA)

- Il privato cittadino può utilizzare la PEC per le comunicazioni con la PA ad esempio richiesta di certificati, contestazione di multe, richieste relative ad attività produttive (ristrutturazione, cessazione, riattivazione), esecuzione di opere interne a fabbricati ad uso di impresa, dichiarazioni di inizio attività etc..

Che cosa si certifica

- **Che cosa viene certificato con un messaggio inviato tramite servizio di PEC:**

1) **Autenticazione del mittente (provenienza certa del messaggio)**
2) **Autenticità del contenuto del messaggio (sia in termini di correttezza formale cioè assenza da virus, sia in termini di garanzia del contenuto e assenza di alterazioni durante la trasmissione)**
3) **Avvenuta/mancata ricezione del messaggio da parte del provider del destinatario**
4) **Marcatura temporale opponibile a terzi**

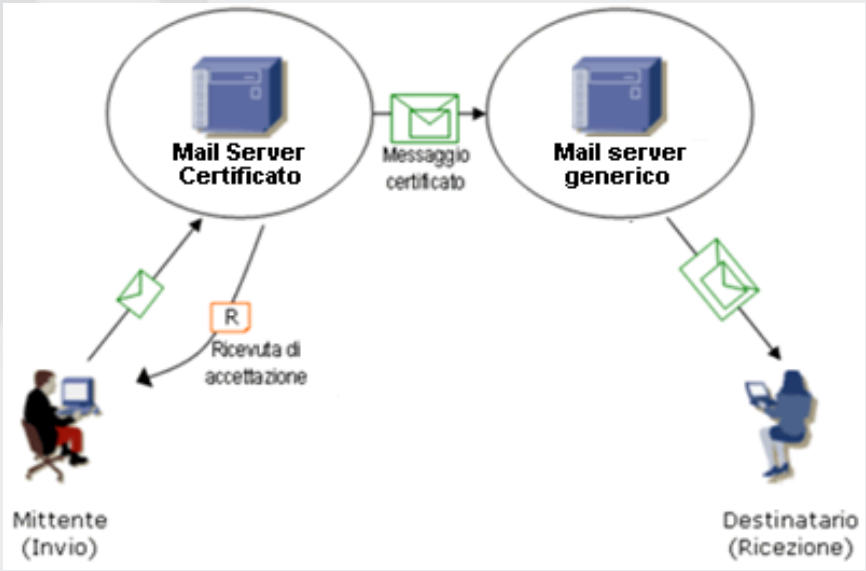
Che cosa si certifica

- Il servizio di PEC si dice “completo” cioè produce certificazioni a valore legale solo se sia mittente che destinatario utilizzano caselle di posta elettronica certificata (in questo caso il documento inviato con marcatura temporale è equivalente ad una raccomandata con ricevuta di ritorno e pertanto opponibile a terzi)

- É comunque possibile inviare mail da indirizzo di posta elettronica certificata ad un indirizzo normale in questo caso l’unica ricevuta prodotta dal sistema è quella di accettazione. L’invio di mail da un indirizzo ordinario a un indirizzo PEC invece potrebbe o non essere accettato dal gestore di PEC oppure arrivare al destinatario ma all’interno di una busta di anomalia

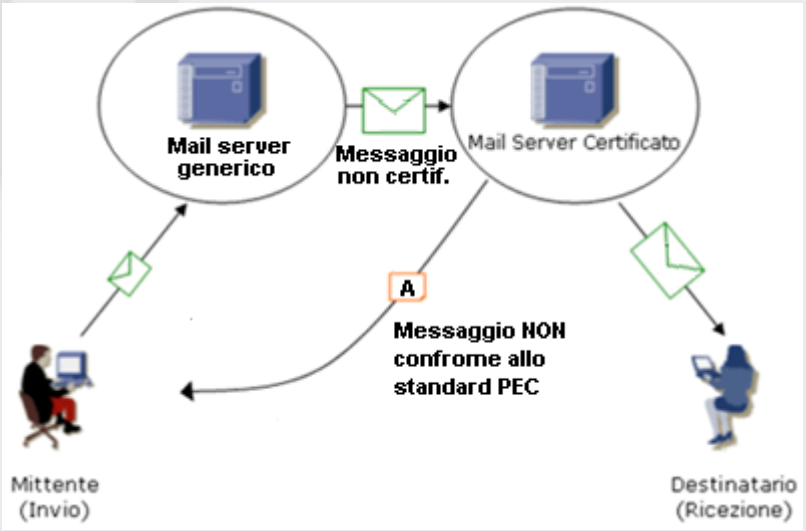
Invio da PEC a server ordinario

- Invio di messaggio da server di posta elettronica certificata a server di posta ordinaria
- Il mittente ha solo evidenza dell'avvenuta ricezione (temporalmente valida) da parte del mail server di invio ma non della presa in consegna e lettura del messaggio da parte mail server del ricevente



Invio da server ordinario a server PEC

- Invio di messaggio da server di posta elettronica generica a server di PEC
- Il server PEC del ricevente può rigettare la mail ricevuta (quindi il destinatario PEC non la leggerà) oppure ha la facoltà di inserirla in una busta di anomalia (non di errore) la quale segnala al mittente che il messaggio è leggibile ma non conforme allo standard PEC



PEC vantaggi

- Certificazione dell'avvenuta consegna del messaggio
- Certificazione degli allegati del messaggio
- Possibilità di allegare al messaggio qualsiasi tipologia di informazione/documento in formato digitale
- Archiviazione (per 30 mesi) da parte del gestore di tutti gli eventi con le ricevute ed esclusione dei messaggi originali
- Semplicità di trasmissione, inoltro e ricerca dei messaggi
- Economicità rispetto alla raccomandata tradizionale
- Possibilità di invio multiplo a più destinatari
- Tracciabilità della casella del mittente
- Velocità di consegna (come la e-mail tradizionale)
- Consultazione della casella di posta anche al di fuori del proprio ufficio/abitazione
- Garanzia di privacy e sicurezza