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

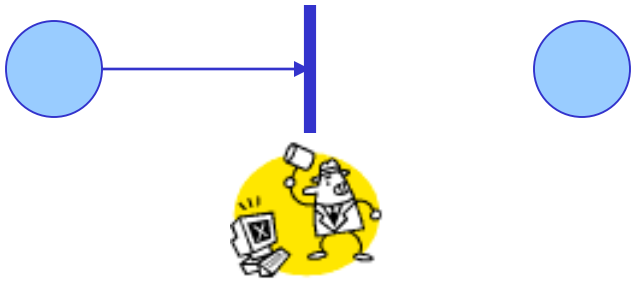
- Attacchi passivi
  - Accesso a informazioni riservate
  - Analisi del traffico
- Attacchi attivi
  - Masquerade
  - Replay
  - Modifica
  - Negazione del servizio (DoS Denial of Service)

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

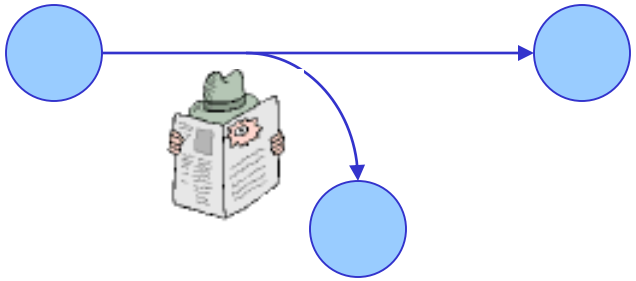
Tipi di minaccia

- 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



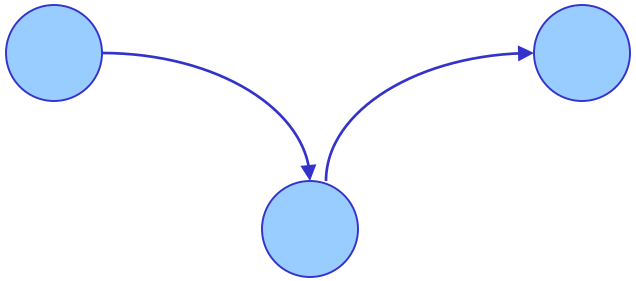
Tipi di minaccia

- 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
    - Packet sniffing



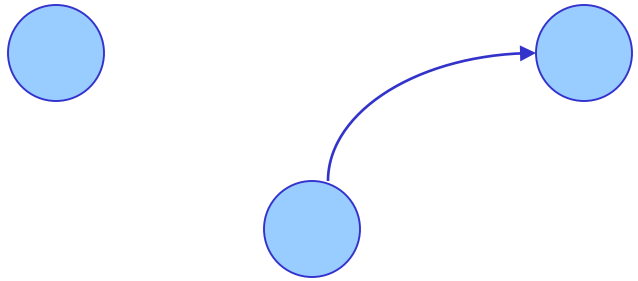
Tipi di minaccia

- 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

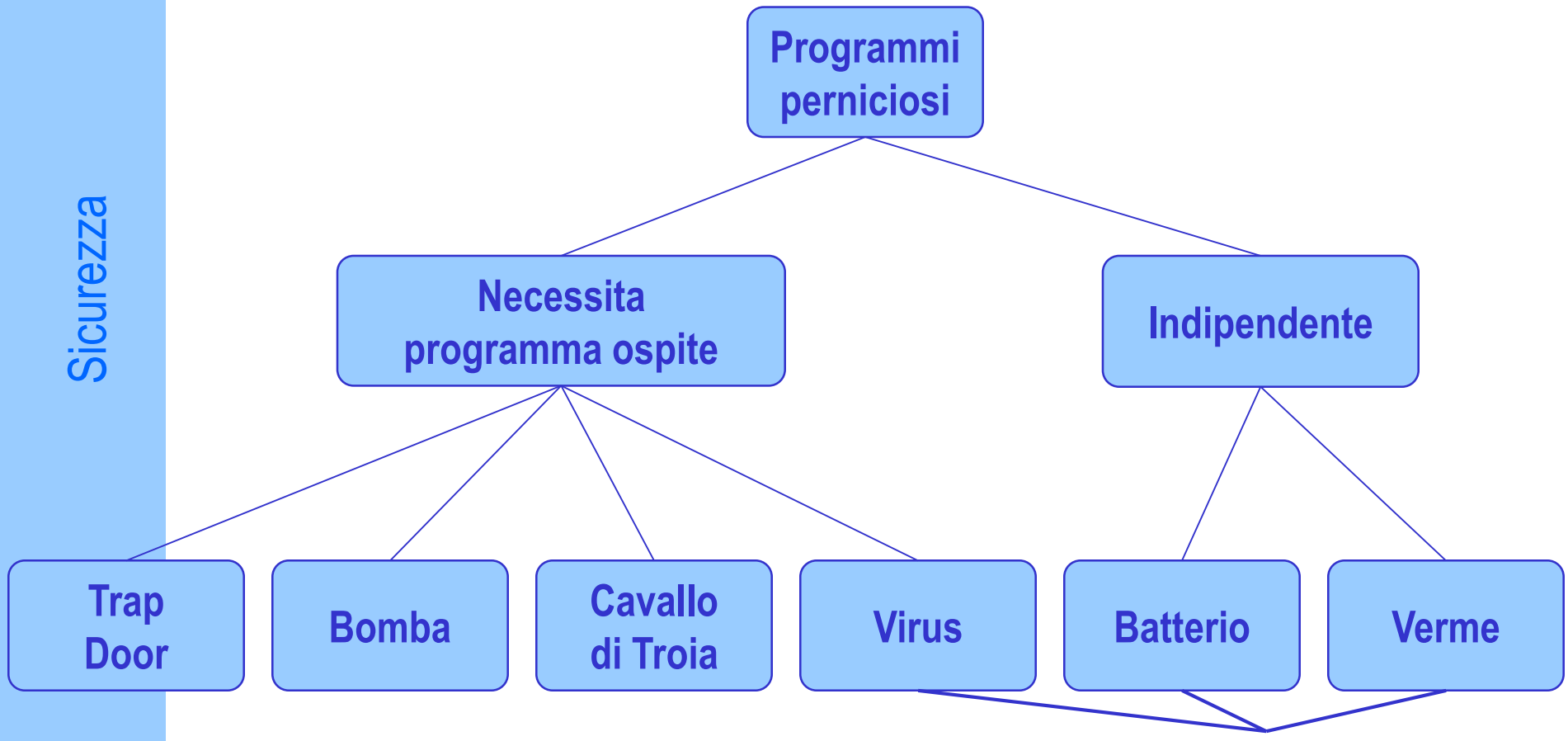
- Generazione
  - Una parte non autorizzata inserisce oggetti contraffatti
  - È un attacco alla autenticità
    - Aggiungere record ad un file
    - Inserire messaggi falsi in rete



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

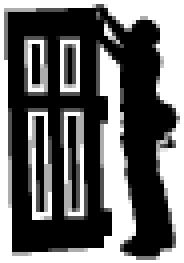
Tassonomia dei programmi perniciosi



[Bowles and Pelaez, 1992]

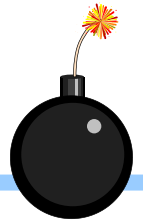
Si replicano!

Trapdoor



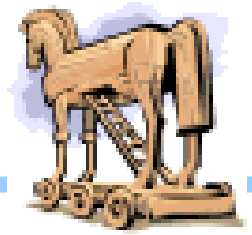
- È un punto di ingresso nascosto nel sistema
- Spesso viene lasciato dall'autore stesso del programma (non necessariamente per scopi fraudolenti)
- È utilizzato per aggirare le comuni procedure di protezione
- Normalmente è molto difficile da rilevare

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
  - esempio: esecuzione di 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 Office
- 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

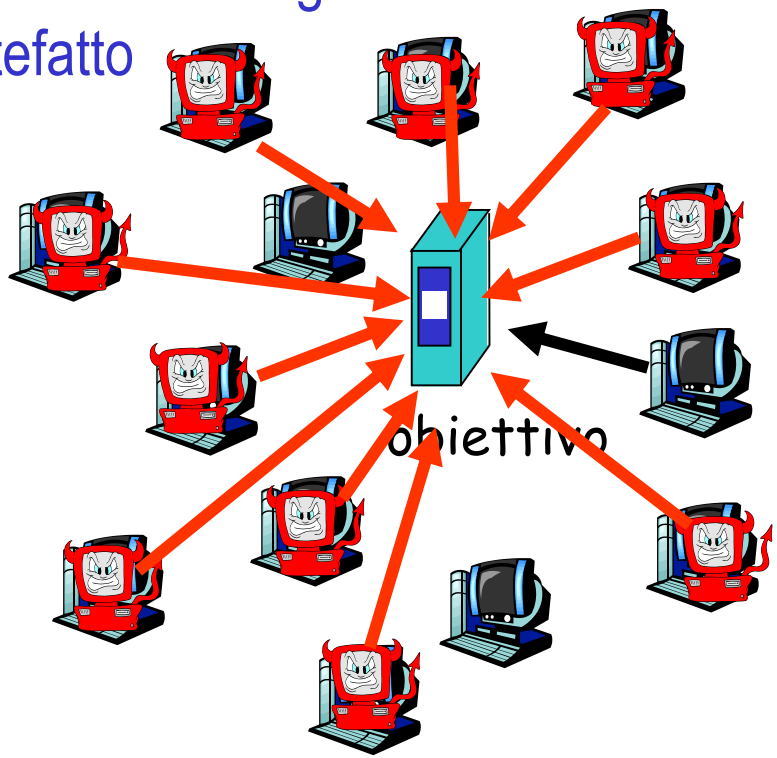
Il malware infetta gli host attraverso Internet

- 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



Sicurezza

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 (più utenti sullo stesso 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)
- 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
- l'altezza
- il peso
- colore e dimensione dell'iride
- retina
- sagoma della mano
- palmo della mano
- vascolarizzazione
- forma dell'orecchio
- fisionomia del volto

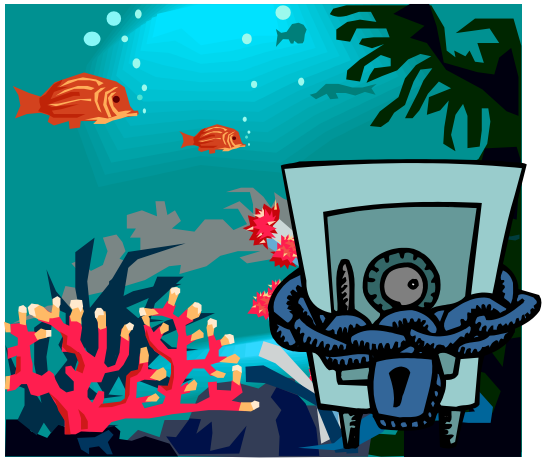
Sicurezza

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 rischio totalmente, ma "ridurlo" a livelli accettabili
- Un PC chiuso in una cassaforte senza chiave in fondo al mare è sicuro, ma non è più utilizzabile!



La crittografia

Motivazioni

Obiettivi

Terminologia

Storia

Steganografia

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
- 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 segreta e pubblica

Crittanalisi

- Le ipotesi fondamentali della crittanalisi sono due:
  - Gli attaccanti hanno una perfetta conoscenza dell'algoritmo utilizzato per cifrare il messaggio e di tutti i dettagli della sua realizzazione
  - Gli 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 seguenti 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
  - Disponibilità: garanzia che il sistema di comunicazione sicuro sia disponibile non appena soggetti autorizzati ne facciano richiesta

Criteri generali

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

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 ⇔ testo cifrato
  - Crittografo ⇔ crittanalista
  - Cifratura ⇔ 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

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.

Sicurezza

Cifratura a Chiave Simmetrica

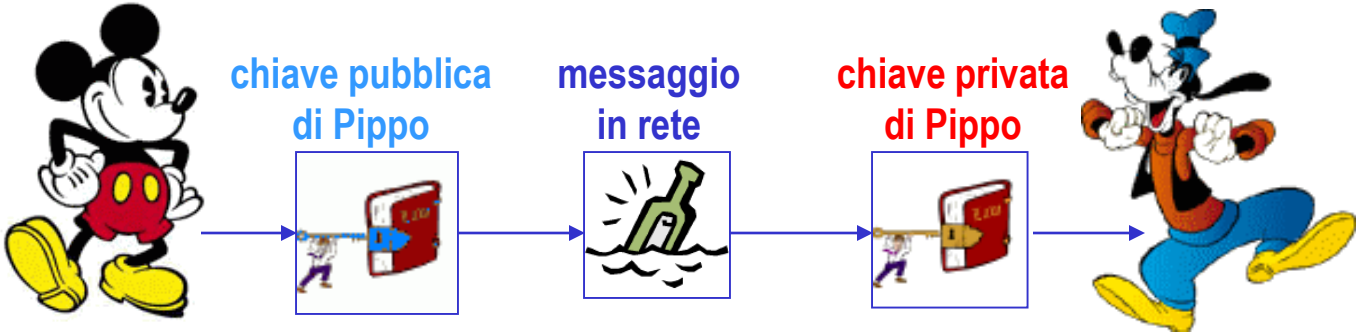
Pippo e Topolino condividono la stessa chiave

Problema: come condividere la chiave

Il problema della scalabilità

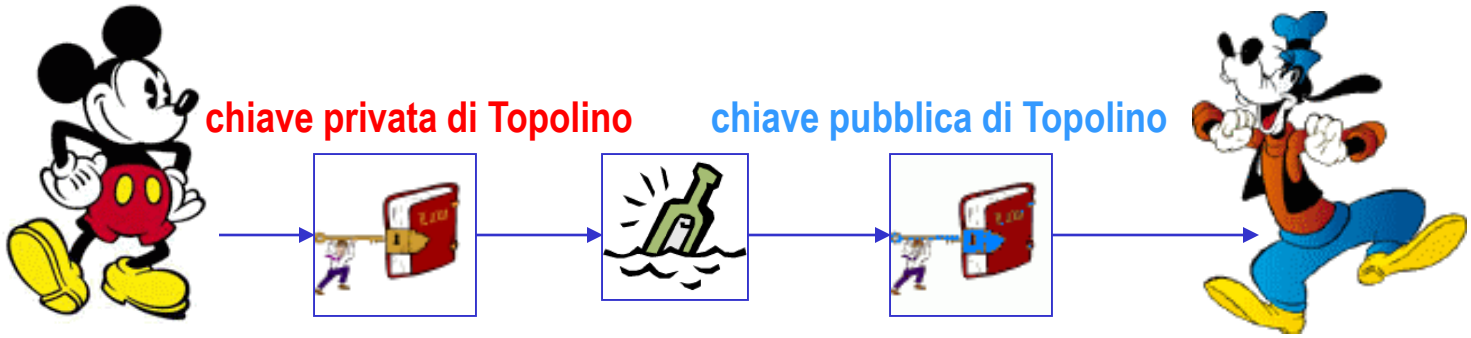
Cifratura a chiave pubblica

- 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

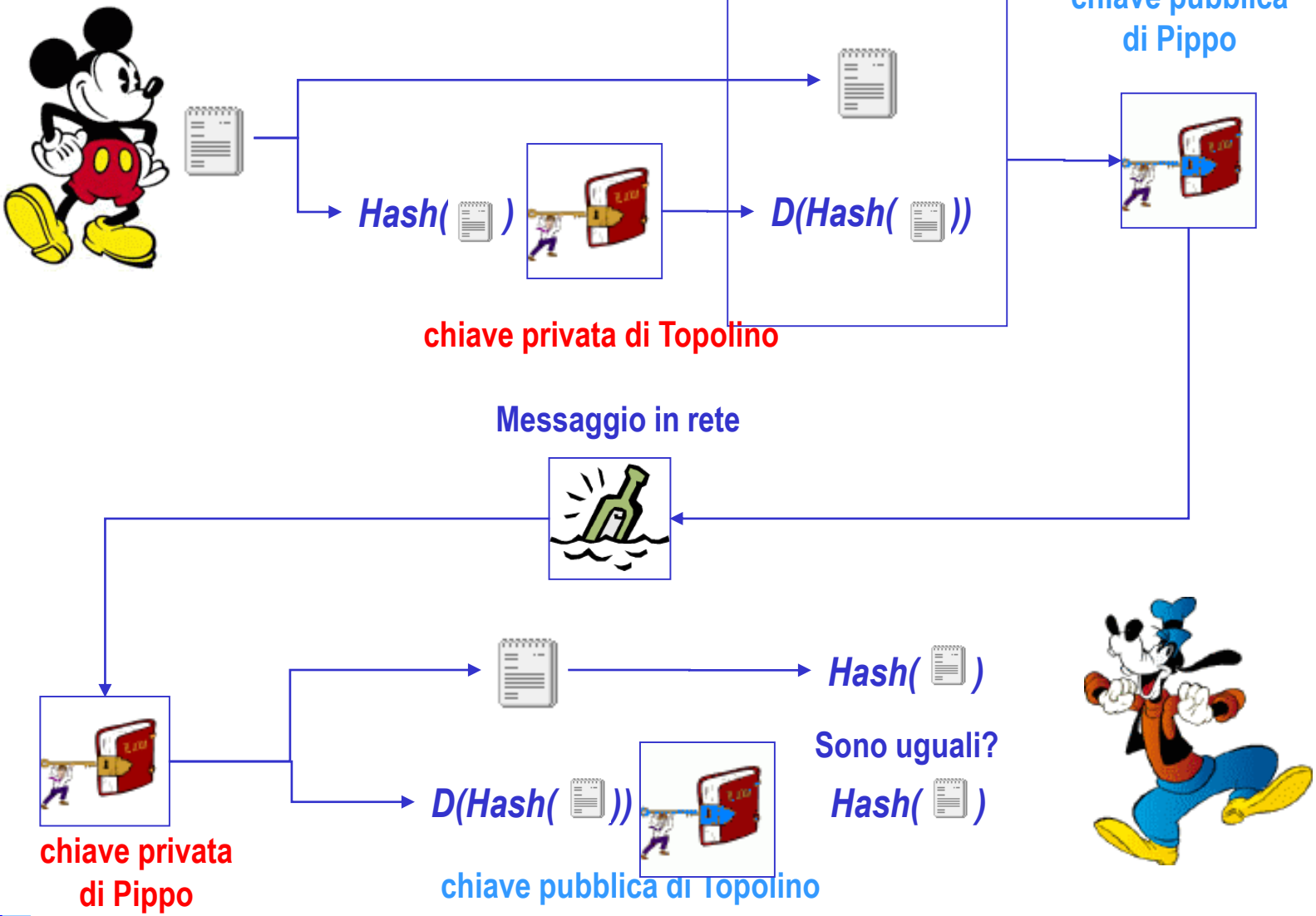


Messaggi firmati

- 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



Funzioni Hash

- Obiettivo elaborare una “impronta digitale”, di lunghezza prefissata, facile da computare
  - applicare la funzione hash H al messaggio m, e ottenere una sintesi del messaggio, H(m), di lunghezza prefissata.
- Proprietà della funzione hash:
  - molti-a-1
  - crea messaggi di dati di lunghezza prefissata (fingerprint)
  - deve essere computazionalmente impossibile trovare due messaggi x e y diversi, tali che H(x) = H(y)

Algoritmi per le funzioni hash

- MD5 è un algoritmo molto utilizzato nella sintesi dei messaggi
  - Calcola una sintesi di 128 bit con un processo a quattro fasi.
  - Non è più un metodo consigliato in quanto sono stati sviluppati algoritmi per trovare «collisioni» in tempi ragionevoli.
- SHA-1 è un altro importante algoritmo di sintesi
  - Standard federale statunitense
  - Produce una sintesi del messaggio più lunga: 160 bit

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 (1)

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

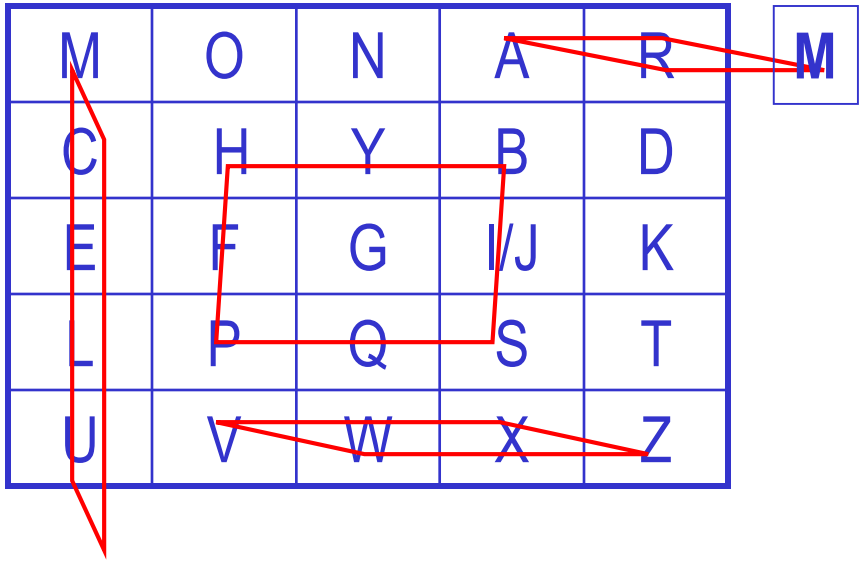
```
a b c d e f g h i l m n o p q r s t u v w x y z
h k l p o u t r e d f s w q a z c v b n m .....
```

- 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	

Cifrario Playfair

- Da una parola chiave (monarchy) 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 periodici)**

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:     sagtesvzi.......
```

```
A: ABCDEFGHIJKLMNOPQRSTUVZ
B: BCDEFGHIJKLMNOPQRSTUVAZ
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: ttnaptmtsuoaodwcoixknlypetz
```

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

- Il NIST (National Institute of Standards and Technology) ha adottato nel 1977 il metodo DES (Data Encryption Standard) come standard
- Utilizza una chiave simmetrica lunga 56 bit e codifica blocchi di 64 bit
  - Con una chiave di 56 bit si hanno 2^{56} possibili chiavi, ovvero circa $7.2X10^{16}$ chiavi
- Nel 1960 l'IBM inizia un progetto ad opera di Horst Feistel. Termina nel 1971 con LUCIFER (chiave di 128 bit)
- Nel 1973 il National Bureau of Standards avvia la gara per uno standard di crittografia: vince l'algoritmo IBM, ma con una chiave ridotta per poter essere mappata in hardware (single chip) (94-99, NIST)

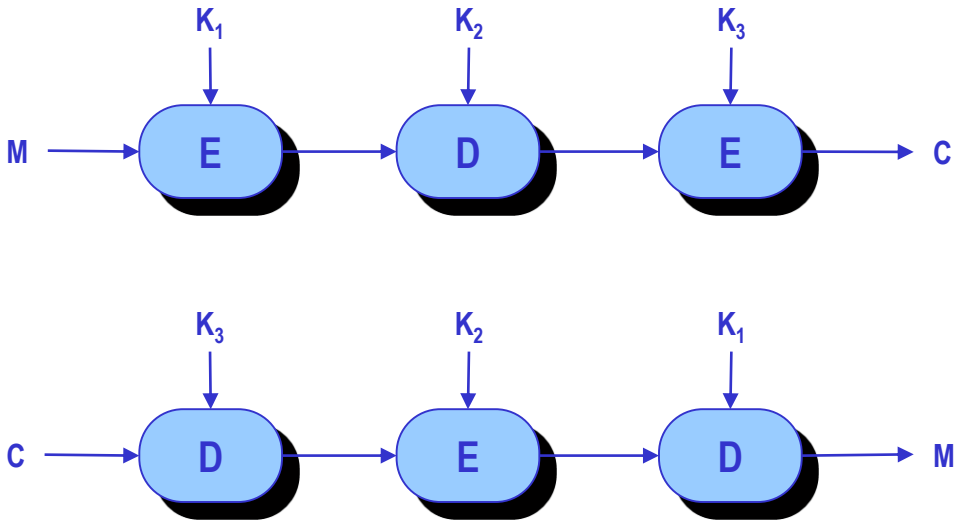
DES

- Attacco brute-force
  - Un'operazione di cifratura DES per microsecondo:

    2^{55} μsec = 1142 anni
  - 10^6 operazioni di cifratura DES per μsec 10.01 h
  - Stima del 1993:
    - DES violabile in 3.5 ore con spesa di 1M $.
  - Luglio 1999:
    - Annuncio di un hardware dedicato da $ 220000 in grado di violare il DES in 4.5 giorni.
    - Costo per successiva macchina $ 50000.
- Oggi il DES è considerato obsoleto.

Triplo DEA

- Si usano tre chiavi e tre esecuzione dell'algoritmo DES (cifr.-decifr.-cifr.)
  - $C = E_{K3}[D_{K2}[E_{K1}[M]]]$
    - $E_K[X]$ = 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 mod (p-1)(q-1) = 1
  - $C = m^e \bmod n$
  - $D = C^d \bmod n = m$
- 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 noti *e* e *d* che sono scambiabili fra di loro (cioè posso anche usare *d* per cifrare ed *e* per decifrare)

Esempio

- Testo in chiaro: M < n
  - p=7,q=17,e=5, d=77, n=119, M=19
- Testo cifrato: $C=M^e \bmod n$
  - $19^5 \bmod 119 = 2476099 \bmod 119 = 66$
    - Nota: 2476099 mod 119 = 66 significa che il resto della divisione di 2476099 per 119 è 66 (potete trovare anche 2476099 % 119)
- Testo in chiaro: $M=C^d \bmod n$
  - $66^{77} \bmod 119 = 19$

Intermediario di fiducia

Problema per la crittografia a chiave simmetrica:

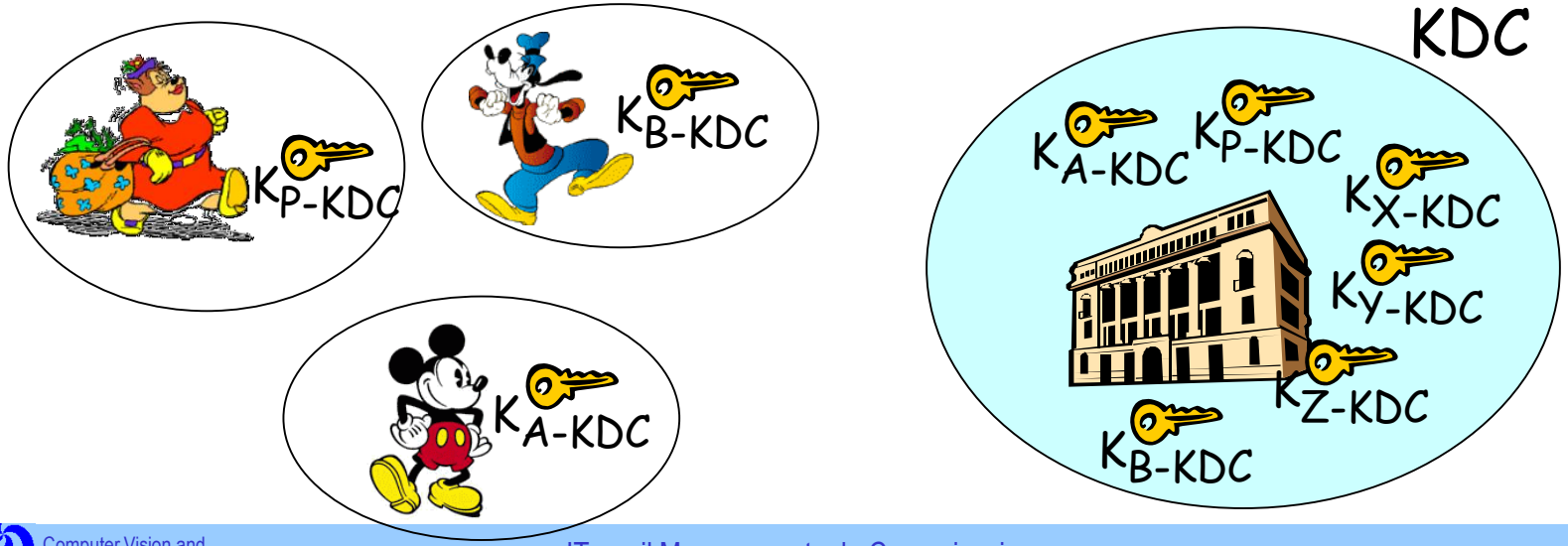
- Come possono le due parti concordare le chiavi prima di comunicare?
- Soluzione:
  - Un centro di distribuzione delle chiavi (KDC, key distribution center) di fiducia funge da intermediario tra le due entità

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)

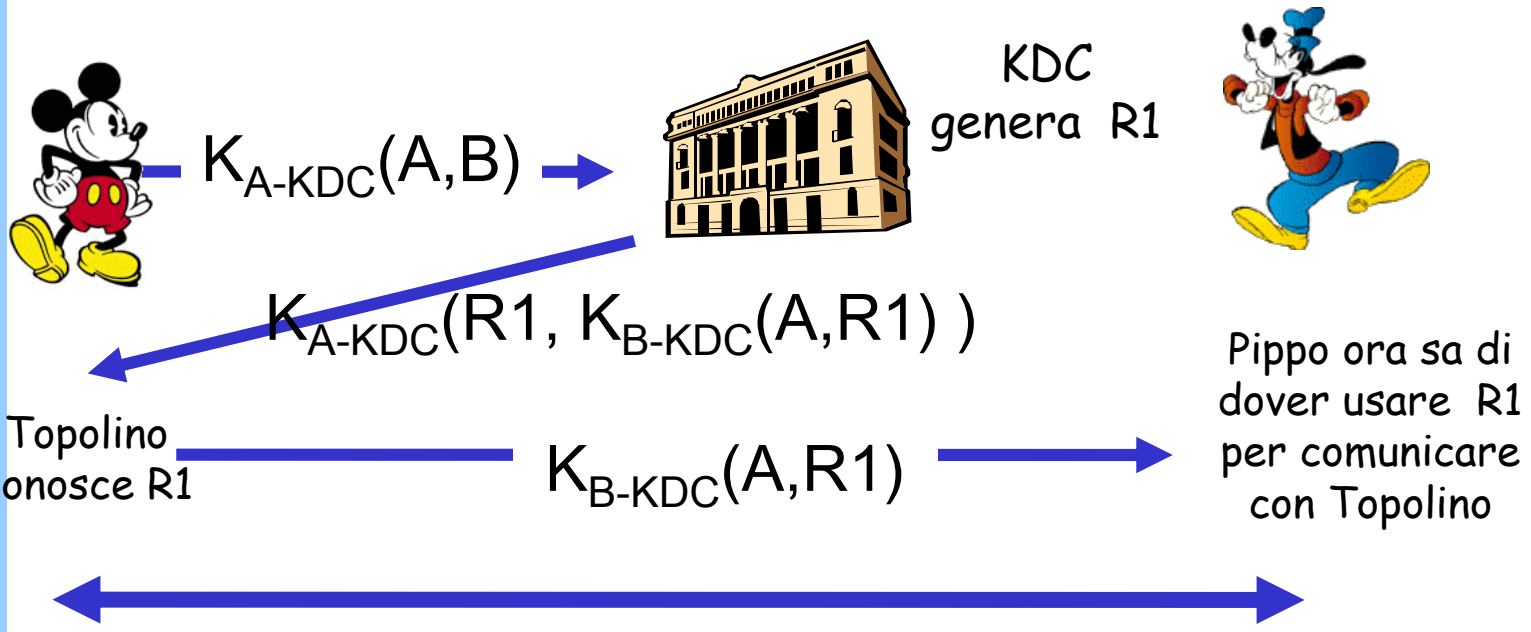
Centro di distribuzione delle chiavi (KDC)

- 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)

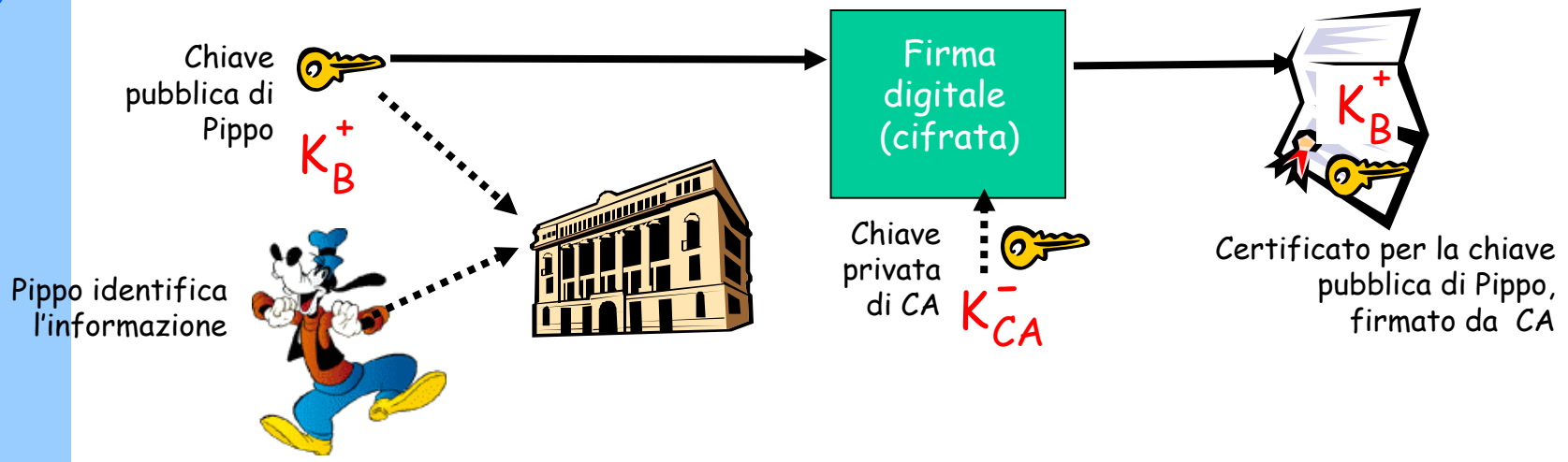
In che modo KDC consente a Topolino e Pippo di determinare la chiave segreta simmetrica condivisa per comunicare tra loro?



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

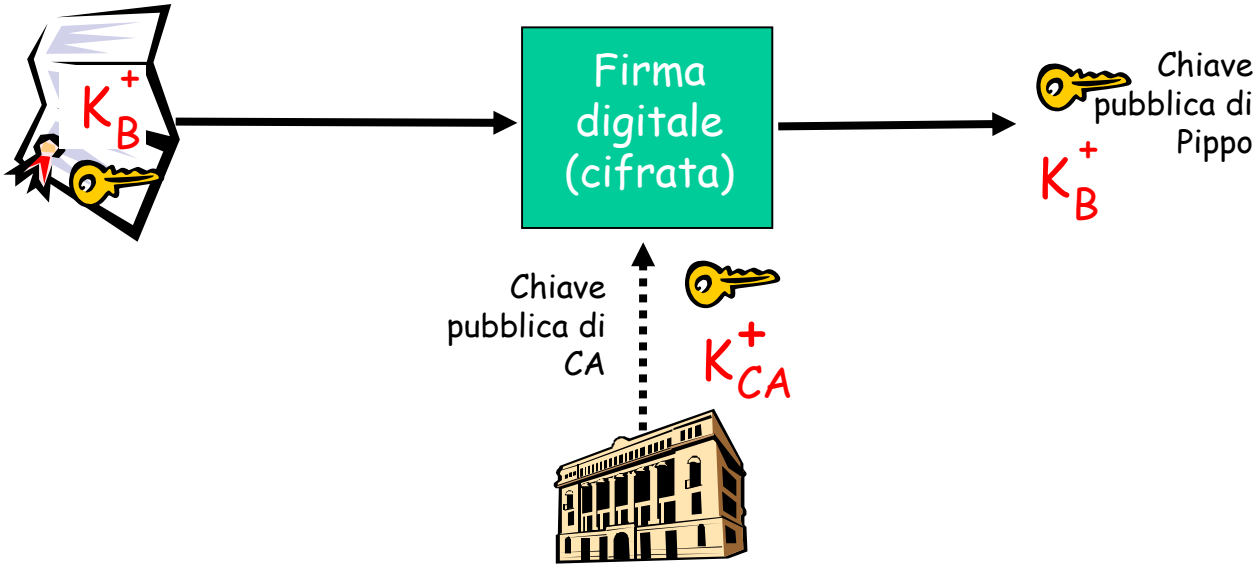
Autorità di certificazione

- 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")

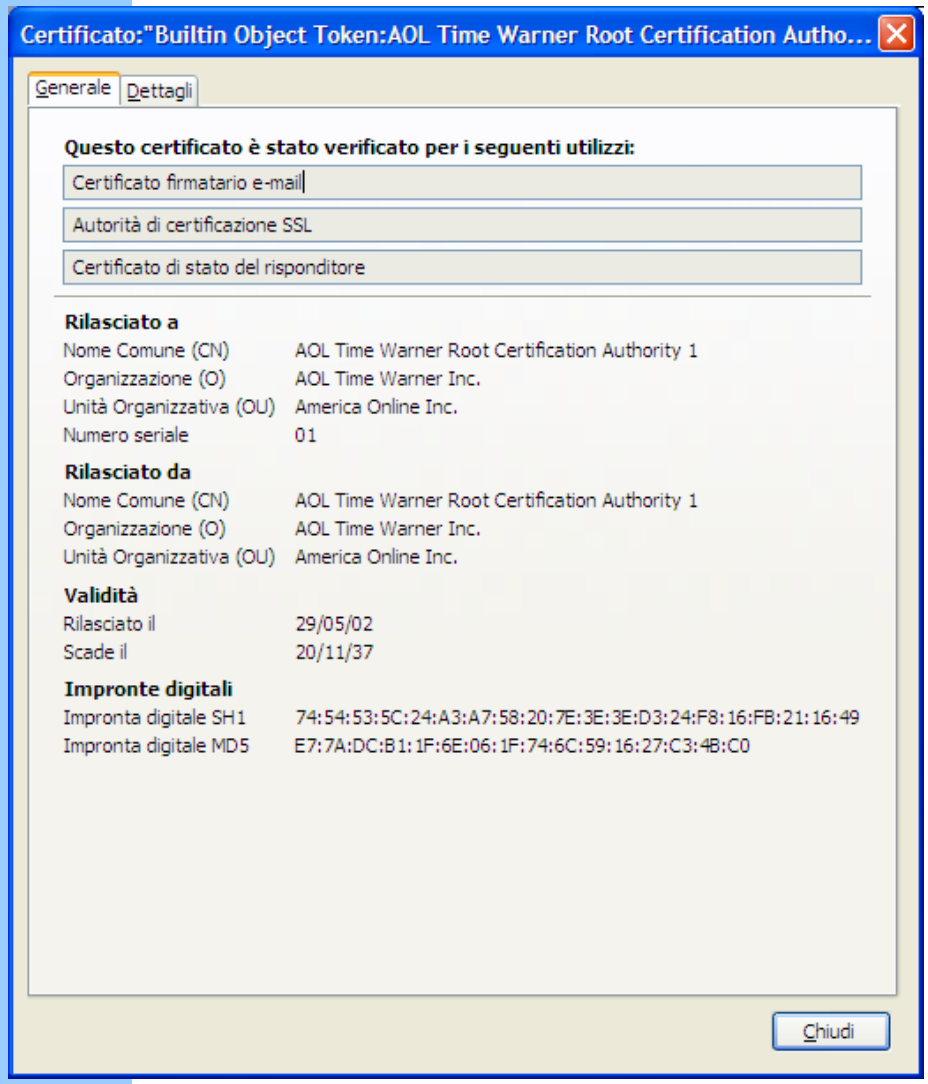


Autorità di certificazione

- 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



Un certificato contiene:



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