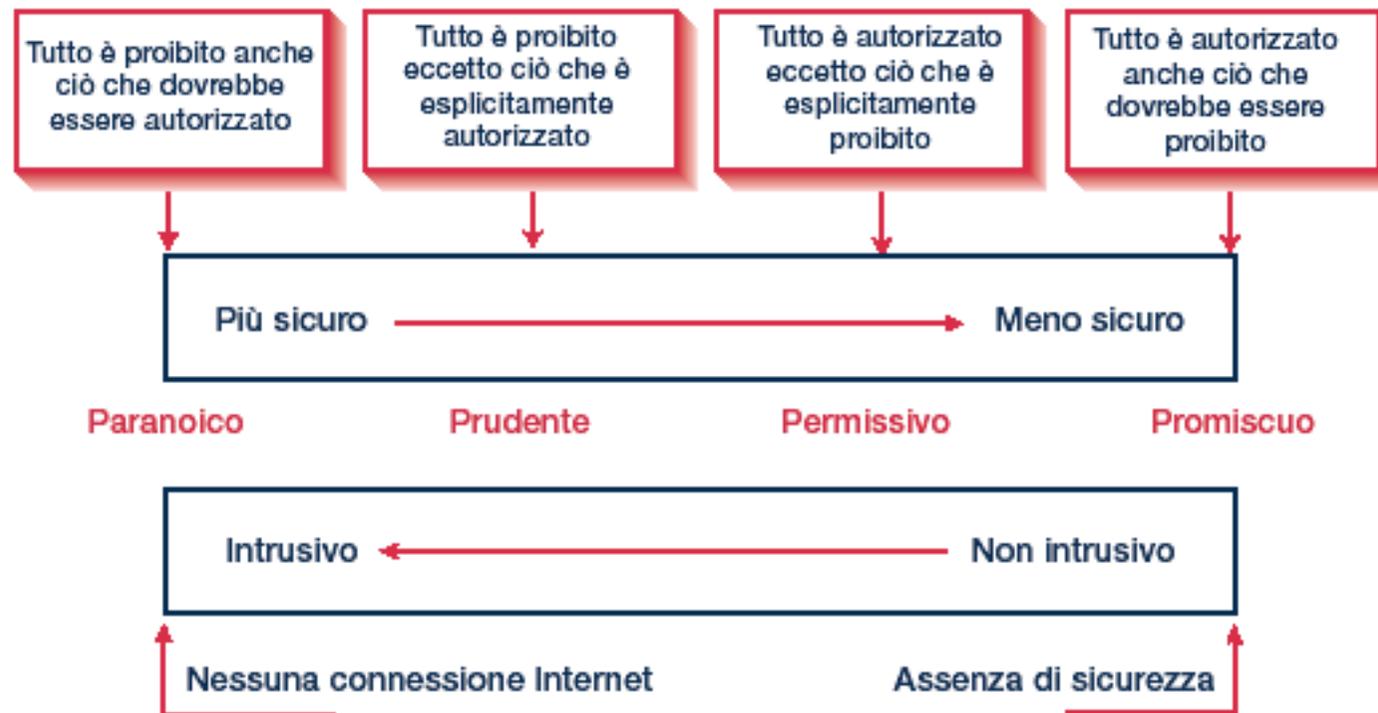


Approcci al problema della sicurezza



Accessi non autorizzati

- ❑ **Hacker:** coloro che si avvalgono delle proprie conoscenze informatiche e di tecnologia delle telecomunicazioni per scoprire e infrangere le regole attraverso cui le tecnologie della sicurezza sono gestite.
- ❑ **Sniffing**
- ❑ **Spoofing**
- ❑ **Firewall**

Accessi non autorizzati

“Fare sniffing” significa registrare, per un determinato periodo, le transazioni da o verso un determinato sistema sino a individuarne un punto debole per attaccarlo.

Effettuare invece lo “spoofing” dei pacchetti IP significa falsificarli, in maniera tale che, ad es., la provenienza dei pacchetti risulti diversa dall’effettiva locazione della macchina da cui provengono.

Accessi non autorizzati

Firewall: un insieme di dispositivi atti a proteggere un'organizzazione connessa ad una rete pubblica.

Il principio alla base dei firewall è il seguente: è *molto più facile proteggere un piccolo numero di sistemi piuttosto che centinaia o migliaia di macchine.*

Aspetti della sicurezza e tecnologie correlate

Obiettivi	Soluzioni
Controllo degli accessi	Password, firewall ecc.
Riservatezza	Crittografia, firma digitale ecc.
Integrità	Software antivirus ecc.

Aspetti della sicurezza e tecnologie correlate

A proposito della sicurezza in Rete, in realtà la maggior parte dei dati circolano anche al di fuori di essa, con modalità di trasmissione molto meno sicure.

Internet non è nata con lo scopo di supportare transazioni commerciali. L'evoluzione tecnologica garantisce livelli di sicurezza relativa sempre più elevati, e gli investimenti necessari per attaccare anche i più comuni sistemi di difesa utilizzati in Rete spesso superano di qualche ordine di grandezza il potenziale "bottino" ottenibile.

Password

- ❑ Metodo di controllo e autenticazione più diffuso ma più vulnerabile
- ❑ Il loro uso corretto può aumentarne il grado di affidabilità:
 - almeno 6 caratteri
 - mix di lettere maiuscole, minuscole caratteri speciali, numeri
 - nessun riferimento a dati personali

Crittografia

- ❑ Processo di trasformazione dei dati attraverso algoritmi matematici che rende i dati illeggibili a chi non disponga di una chiave di decriptazione

Criptazione

Testo in chiaro



Algoritmo

Decriptazione

Testo cifrato

Crittografia

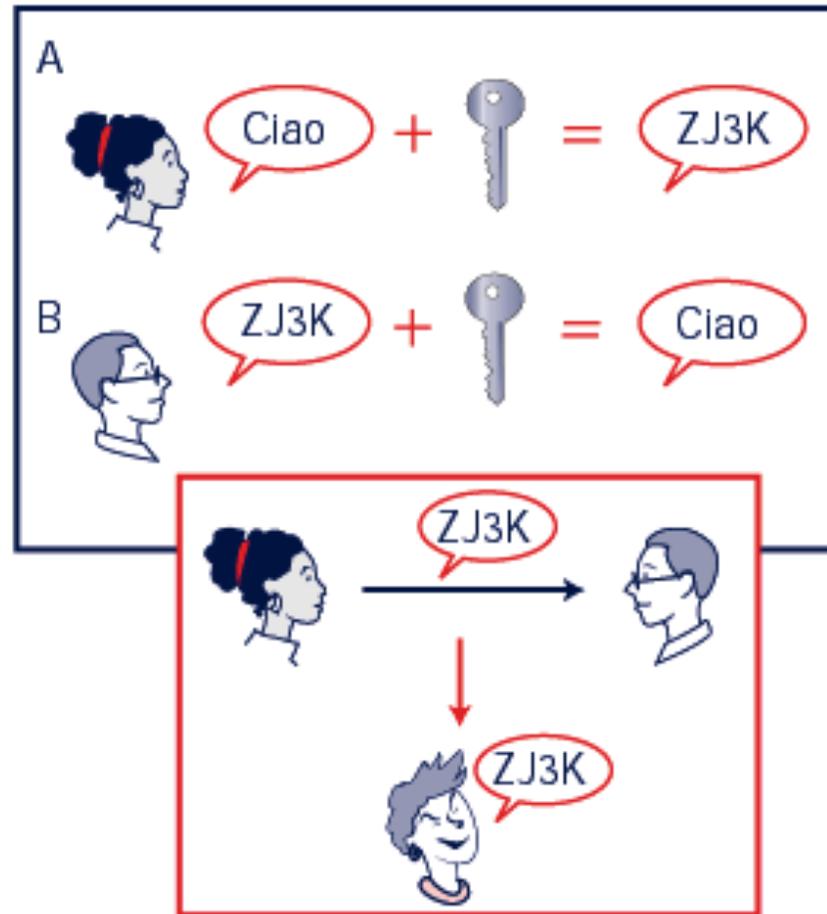
La crittografia è stata implementata a diversi livelli e viene comunemente utilizzata per garantire la **riservatezza** nella trasmissione di numeri di carte di credito o di semplici messaggi di posta elettronica, ma anche nell'ambito dei sistemi di **certificazione** e di **firma digitale**.

Scenari d'attacco a un sistema di crittografia

- ❑ L'agente ostile dispone solo del testo cifrato
- ❑ L'agente ostile dispone del testo in chiaro e del testo cifrato
- ❑ L'agente ostile sceglie il testo in chiaro

In ogni caso è considerato assolutamente insicuro un modello che basi la sua efficacia sull'ipotesi che l'agente ostile non conosca l'algoritmo usato per cifrare.

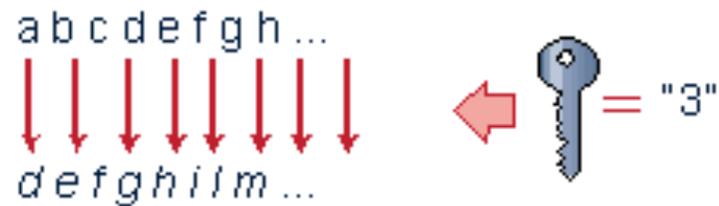
Sistemi a chiave privata



In tali sistemi è prevista un'unica chiave, condivisa da mittente e ricevente.

Esempio di crittografia tradizionale

Algoritmo = "scalare di x posizioni"



Crittografia a chiave privata

I principali problemi generati da un sistema di crittografia a chiave privata sono:

- da un lato, la necessità di scambio preliminare della chiave fra mittente e destinatario attraverso un canale reputato sicuro (se voglio scambiare dati via e-mail devo prima comunicare la chiave al mio interlocutore per telefono o per lettera);
- dall'altro, la necessità di generare un elevato numero di chiavi. Infatti, dato un sistema di n utenti, sono necessarie $n(n-1)/2$ chiavi (distinte) per permettere il dialogo cifrato bidirezionale fra tutti i soggetti del sistema.

Numero di chiavi necessarie nei diversi sistemi di crittografia

Numero di soggetti partecipanti	Chiavi necessarie	
	Sistema a chiave privata	Sistema a chiave pubblica
2	1	4
3	3	6
4	6	8
5	10	10
6	15	12
10	45	20
500	12 4750	1000
10 000	49 995 000	20 000
n	$n(n-1)/2$	$2n$

Sistema di crittografia a chiave pubblica



Dal modello a chiave asimmetrica alla firma digitale



La firma digitale

Attraverso il sistema a chiave pubblica non è solo possibile mantenere la *riservatezza*, ma anche verificare l'*autenticità* (ed *integrità*) di un messaggio attraverso la cosiddetta **firma digitale**.

Supponiamo, prima, che il mittente (A) voglia essere sicuro che solo il destinatario (B) possa leggere il contenuto di un documento inviato. In tal caso, A dopo aver scritto il testo del messaggio, dovrà prelevare dall'apposito registro la chiave pubblica di B, che utilizzerà - assieme alla propria chiave privata - per cifrare il testo, ossia trasformarlo in modo tale che il suo contenuto divenga incomprensibile.

La firma digitale

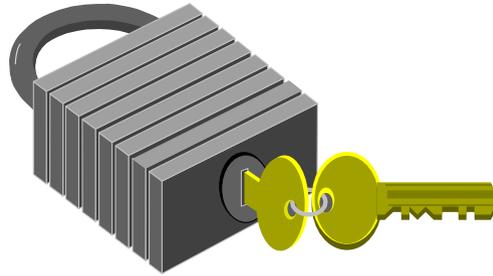
A questo punto, solamente il destinatario B sarà in grado di decifrare il contenuto del documento, utilizzando la propria chiave privata e la chiave pubblica di A, prelevata dallo stesso registro.

Grazie a questo metodo, A ha la certezza che solo B sarà in grado di leggere il contenuto del suo messaggio, mentre B è certo che il mittente può essere solamente A.

Virus

- ❑ Modificano o sostituiscono un programma eseguibile o una sua parte oppure un file di dati che può contenere istruzioni eseguibili (**macrovirus**)
- ❑ È impossibile essere contagiati da un virus semplicemente leggendo un messaggio di posta elettronica o una pagina HTML
- ❑ Alcuni modificano il *boot sector* dei dischi
- ❑ Una volta in memoria, infettano altri file

La SICUREZZA digitale

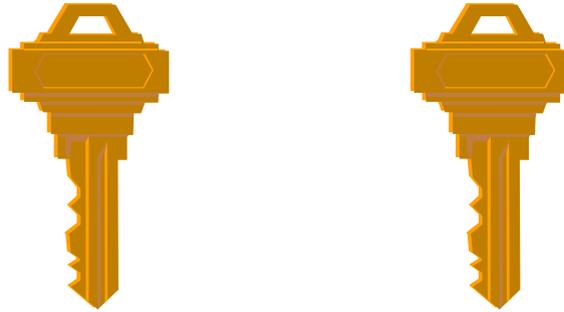


- **requisiti:** confidenzialità, integrità, autenticazione, autorizzazione, assicurazione, riservatezza

soddisfatti mediante

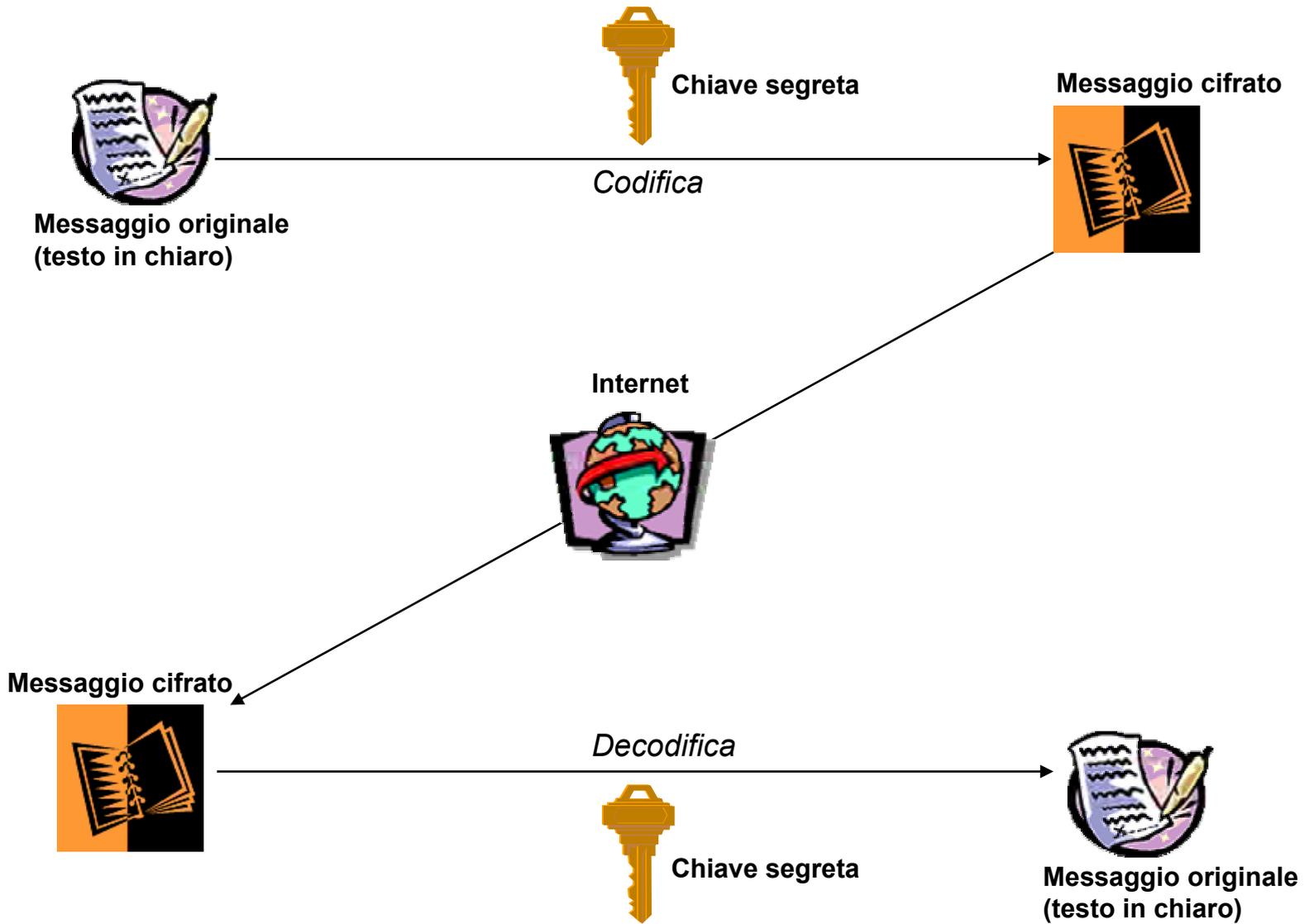
- **crittografia** = codifica dei dati in forma “illeggibile” per assicurare la riservatezza => autenticazione mittente + integrità messaggio
==> richiede un algoritmo ed una chiave
(*chiave + lunga = >> sicurezza*)

Crittografia a chiave simmetrica



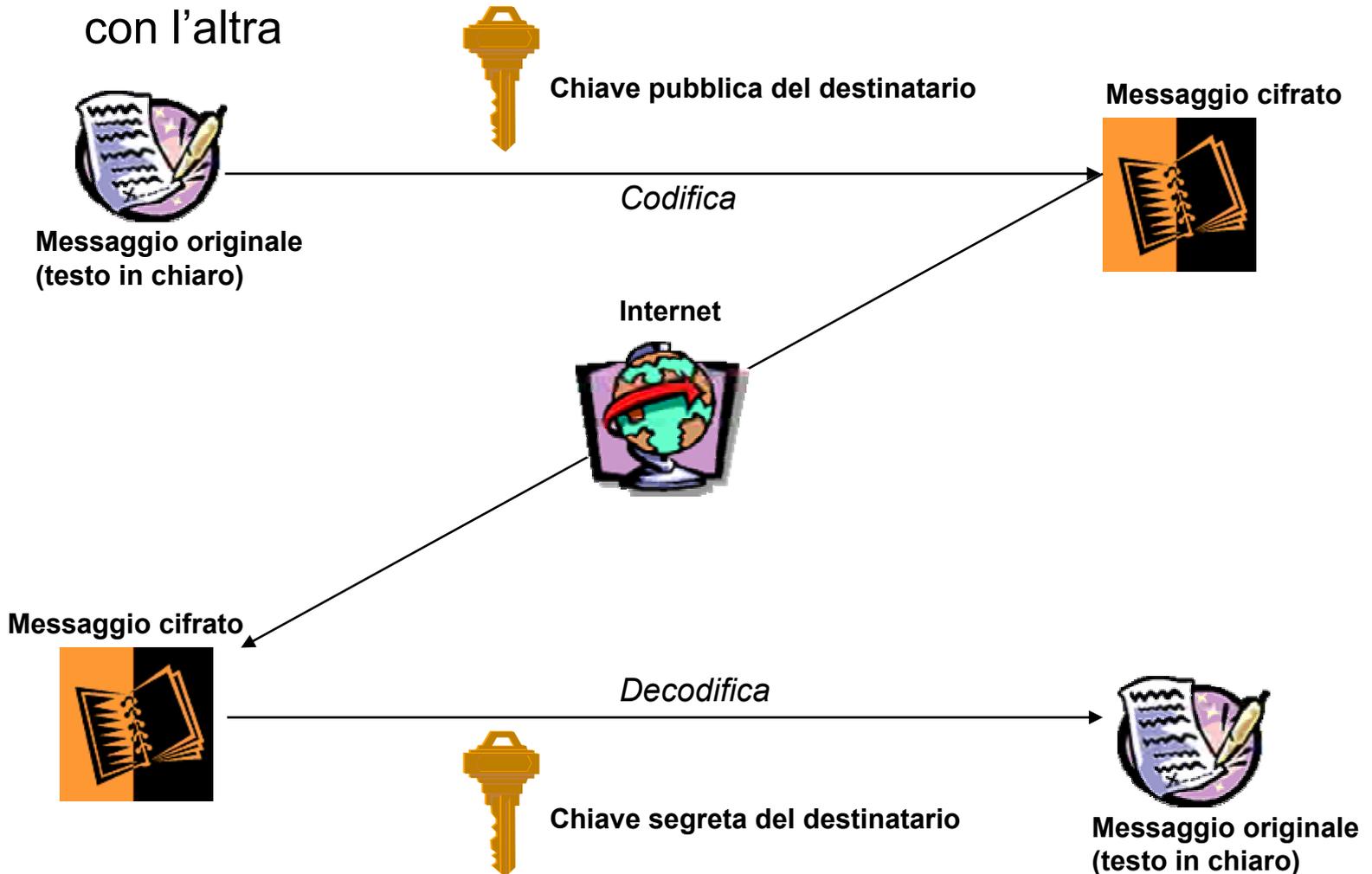
- sia il mittente che il destinatario posseggono la **stessa chiave segreta**
- è necessaria una **diversa chiave segreta** per ogni destinatario
- **non vi è garanzia** di autenticità ed univocità del mittente

Crittografia a chiave simmetrica



Crittografia a chiave pubblica

- utilizza una **coppia di chiavi**: una pubblica ed una privata
- i messaggi codificati con una possono solo essere decodificati con l'altra



Confidenzialità (crittografia chiave pubblica)

- la chiave pubblica del destinatario assicura la **confidenzialità** della comunicazione

Prima di inviare il messaggio ad Anna, Carlo ne acquisisce la chiave pubblica



Messaggio originale inviato da Carlo



Chiave pubblica di Anna

Codifica

Messaggio di Carlo cifrato



Internet



Messaggio di Carlo cifrato



Decodifica

Carlo ha la garanzia che solo Anna con la sua chiave privata possa leggere il messaggio

Chiave segreta di Anna



Messaggio originale inviato da Carlo

Autenticazione (crittografia chiave pubblica)



Chiave privata posseduta solo dal proprietario:

- *il proprietario codifica il messaggio con la sua chiave privata*
- *il destinatario lo decodifica con la chiave pubblica (garanzia della provenienza)*

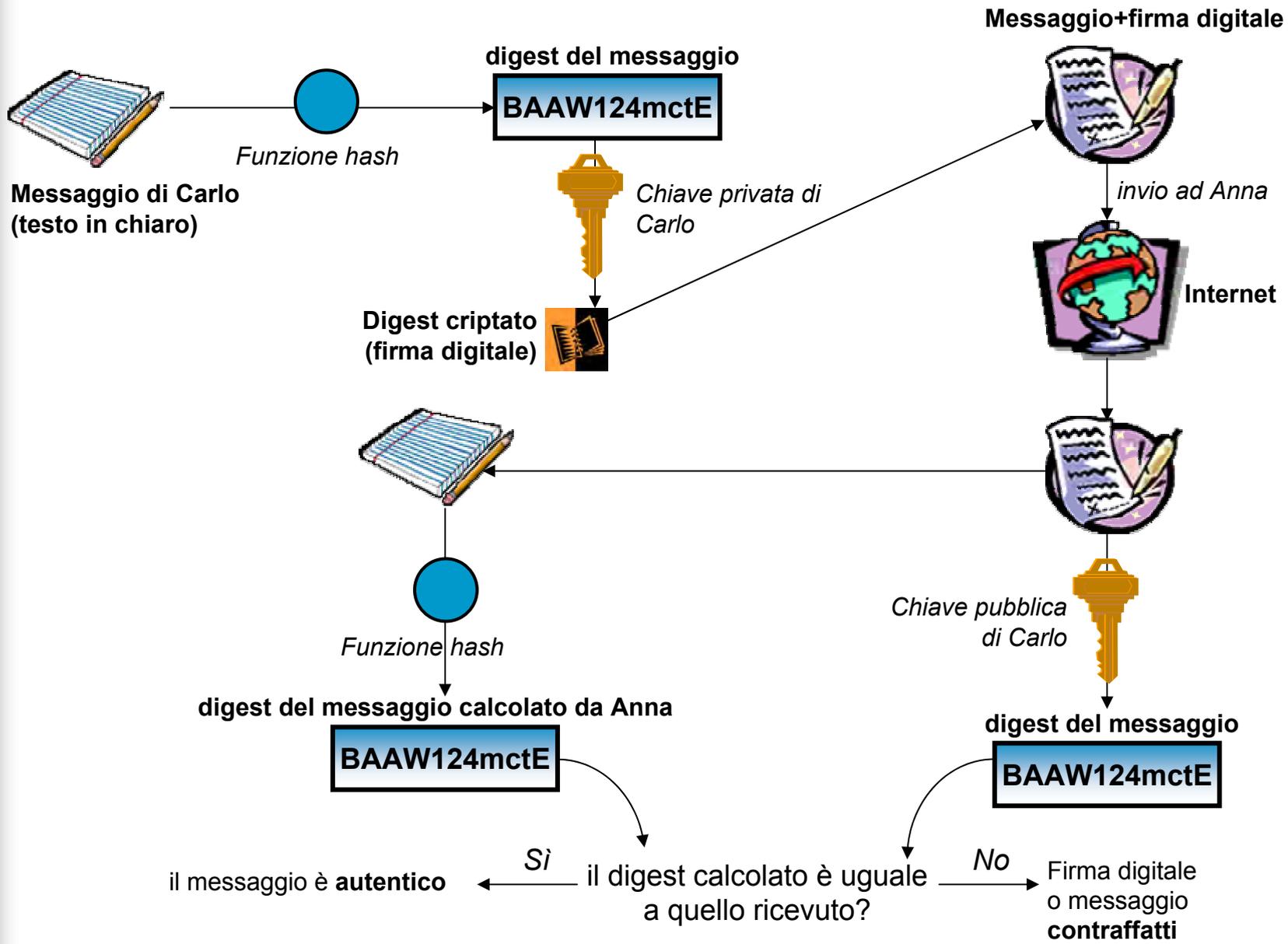
MA chiunque, con la chiave pubblica, può intercettare e decodificare e/o alterare il messaggio originario

FIRMA DIGITALE

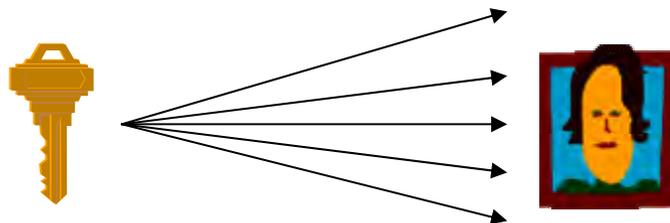
- processo di codifica lento => “message digest” (breve stringa derivata dal messaggio)
- digest codificato con la chiave privata (**firma digitale**)
- digest ricevuto = digest calcolato => messaggio integro

MA nessuna garanzia di riservatezza
(utilizzare in aggiunta la chiave simmetrica)

Verifica di una firma digitale



CERTIFICATI DIGITALI



- come distribuire la propria chiave pubblica?
- pericolo falsificazione “personalità”



CERTIFICATE AUTHORITY (13 in Italia)

- verifica l'identità dell'emittente e ne conserva la chiave pubblica
- distribuisce a terzi chiave pubblica e identità mediante certificati digitali

Verisign, Cybertrust, Nortel, etc...

4 Classi di certificati, data scadenza, gerarchia C.A.

II FUTURO della sicurezza

- stabilizzazione di Internet (ISP)
- *nuovi protocolli per “priorità di traffico” e sicurezza*
- sostituzione reti private con VPN
- *connessione reti Enti Pubblici con Internet*
- sviluppo e proliferazione Certificate Authorities
- *adozione smart-card ed autenticazione biometrica*
- Clipper chip & key escrow => controllo governativo