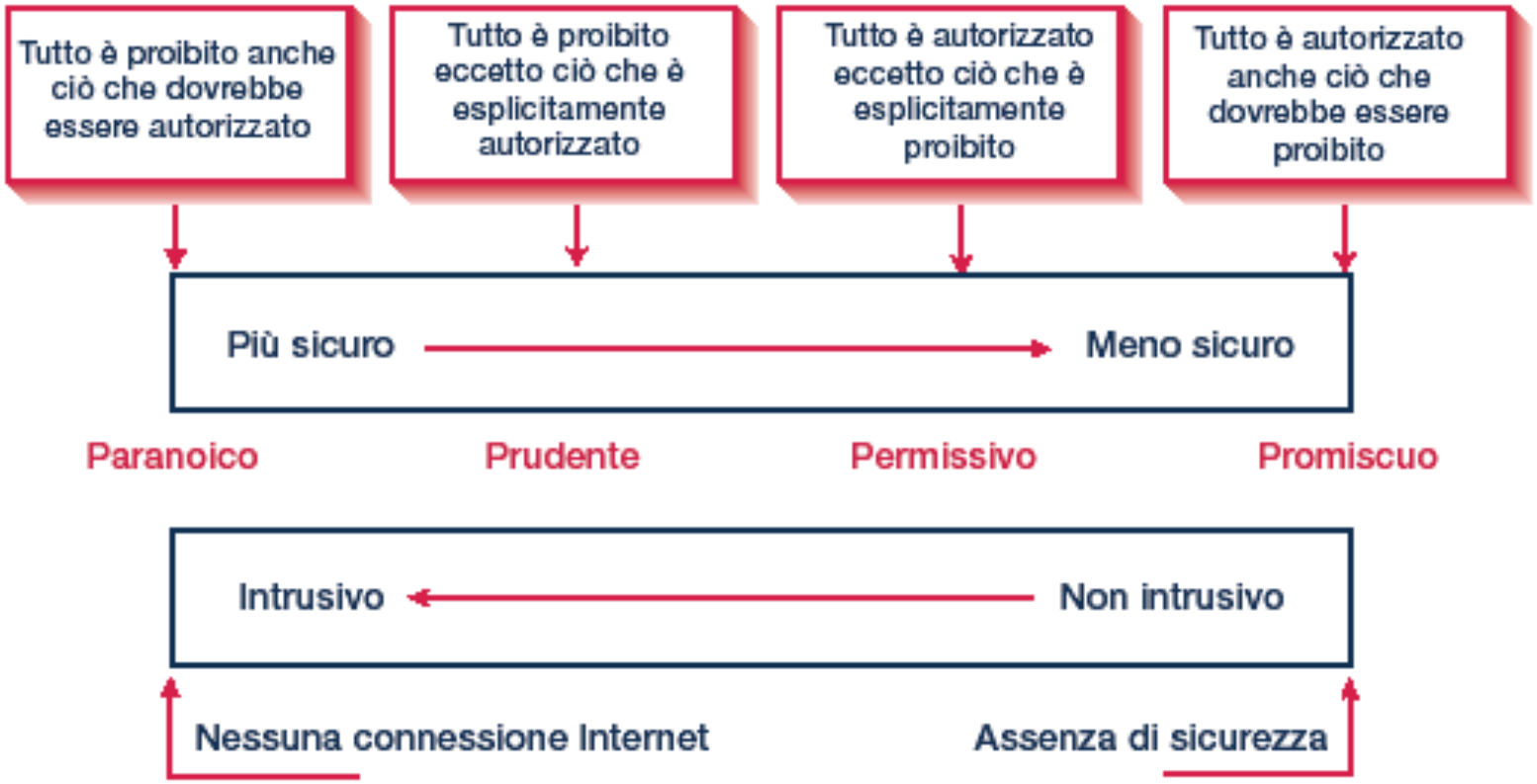
Approcci al problema della sicurezza



Aspetti della sicurezza e tecnologie correlate

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

Requisiti per la sicurezza:

1. qualcosa che "sai" (username/password)
2. qualcosa che "hai" (cellulare, token, smart-card, …)
3. qualcosa che "sei" (impronte digitali, iride, tratti del volto, …)

La sicurezza digitale

Requisiti principali:

1. **riservatezza**
2. **autenticazione** (del soggetto estensore del documento)
3. **integrità** (del documento)

Soddisfatti mediante la **crittografia** = *codifica dei dati in forma "illeggibile"*.

Richiede un algoritmo ed una chiave (chiave più lunga $\Longrightarrow$ maggiore sicurezza).

Crittografia

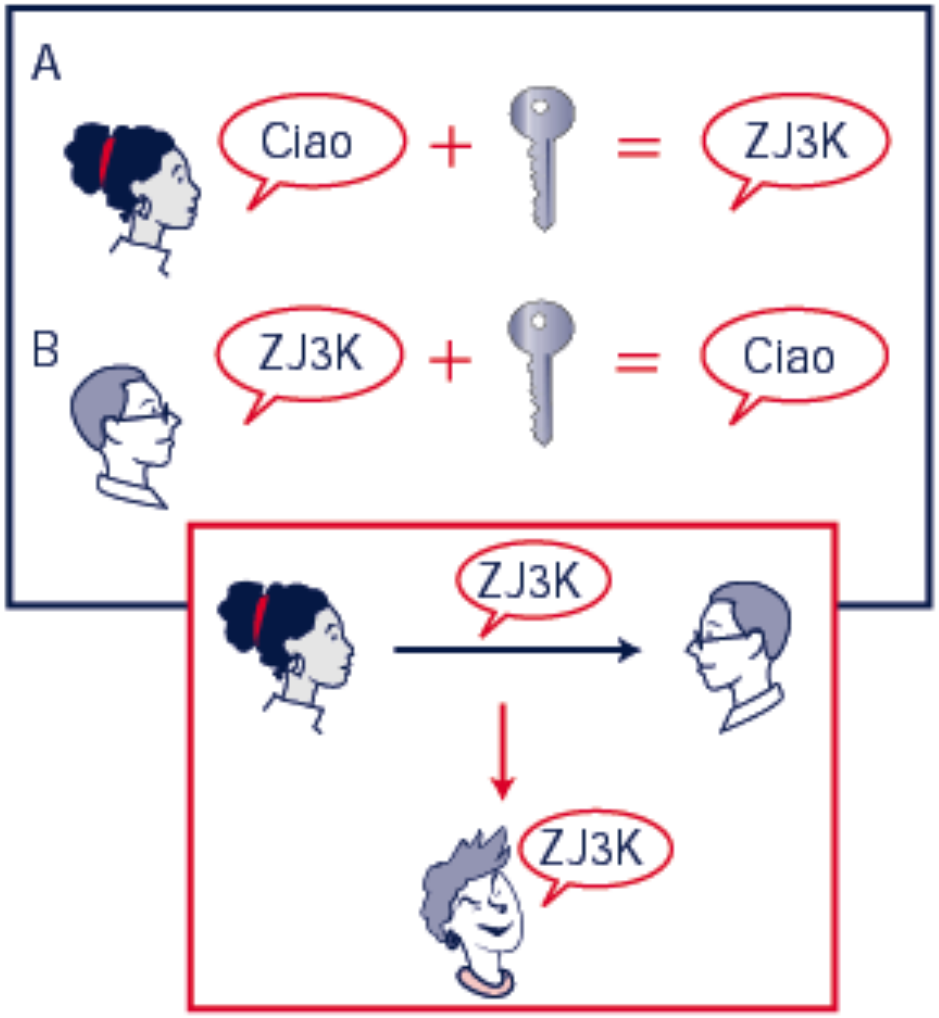
Processo di trasformazione dei dati attraverso algoritmi matematici che rende i dati illeggibili a chi non disponga di una chiave di decifratura.

Testo in chiaro Algoritmo 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.

Sistemi a chiave privata (o simmetrica)

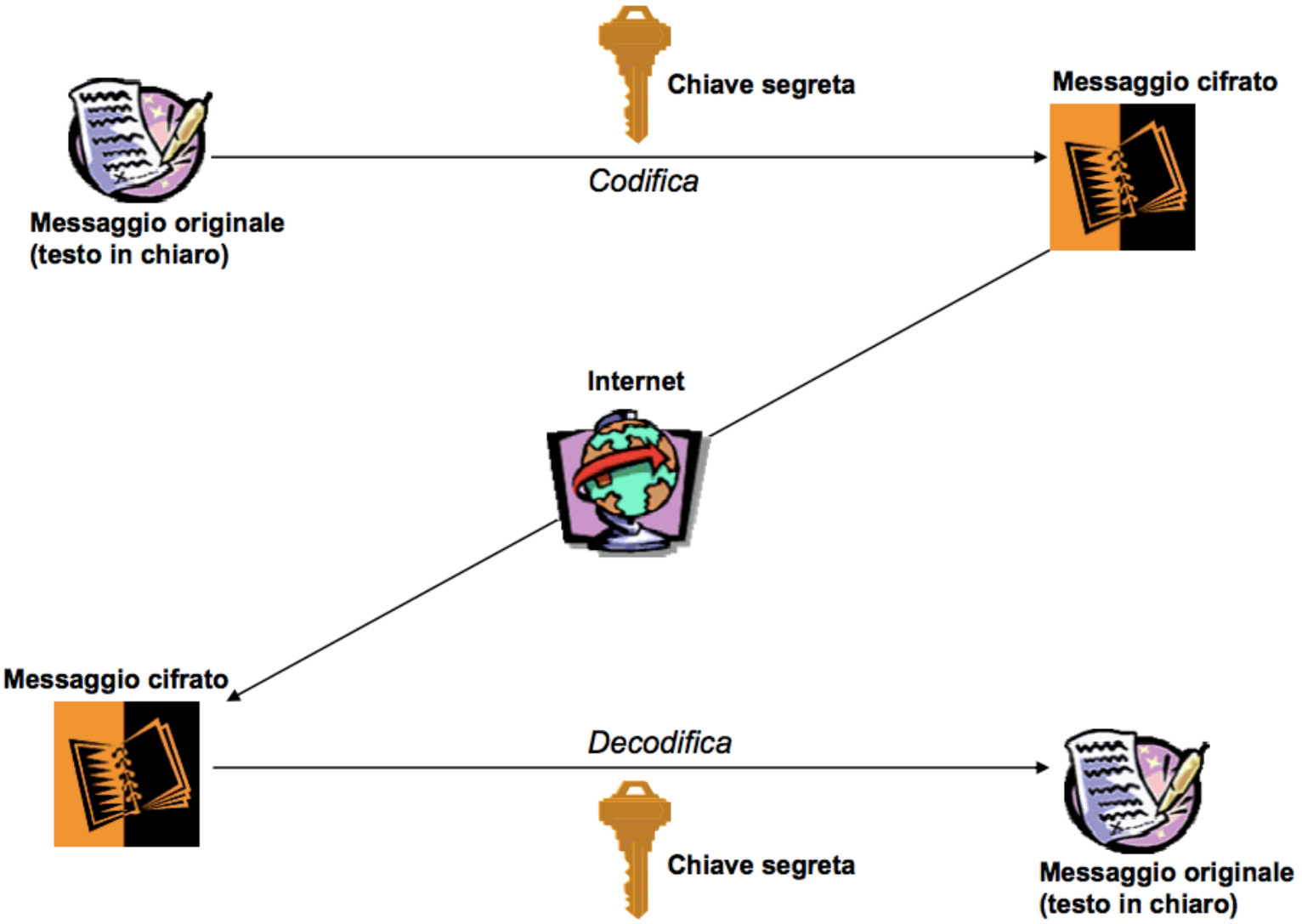


- In tali sistemi è prevista un'unica chiave, condivisa da mittente e ricevente.
- È necessaria una chiave diversa per ciascun destinatario.
- Non vi è garanzia di univocità del mittente e quindi di autenticità del messaggio.

Esempio di crittografia tradizionale (cifrario di Cesare)

Algoritmo = "scalare di x posizioni"

Crittografia a chiave simmetrica



Numero di chiavi necessarie nel sistema di crittografia simmetrica

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

Crittografia a chiave simmetrica

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

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

Sistema di crittografia asimmetrica (a doppia chiave pubblica/privata)

- utilizza una **coppia di chiavi**: una pubblica (che può essere distribuita ed è pubblicamente disponibile) ed una privata (che deve essere detenuta esclusivamente dal titolare);
- i messaggi codificati con una possono essere decodificati solo con l'altra;
- PKI = Public Key Infrastructure.

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 asimmetrica (a doppia chiave pubblica/privata)

Requisito della **riservatezza**

Il mittente (A) vuole essere sicuro che solo il destinatario (B) possa leggere il contenuto di un documento/ messaggio inviato.

In tal caso (A), dopo aver scritto il testo del messaggio, preleva dall'apposito registro la chiave pubblica di B che utilizzerà per cifrare il testo, ossia trasformarlo in modo tale che il suo contenuto divenga incomprensibile.

Sistema di crittografia asimmetrica (a doppia chiave pubblica/privata)

Requisito della **riservatezza**

Infine, il destinatario (B) decodifica il documento/messaggio con la propria chiave privata.

In caso di esito positivo, è disponibile il documento/messaggio nella sua originaria forma leggibile.

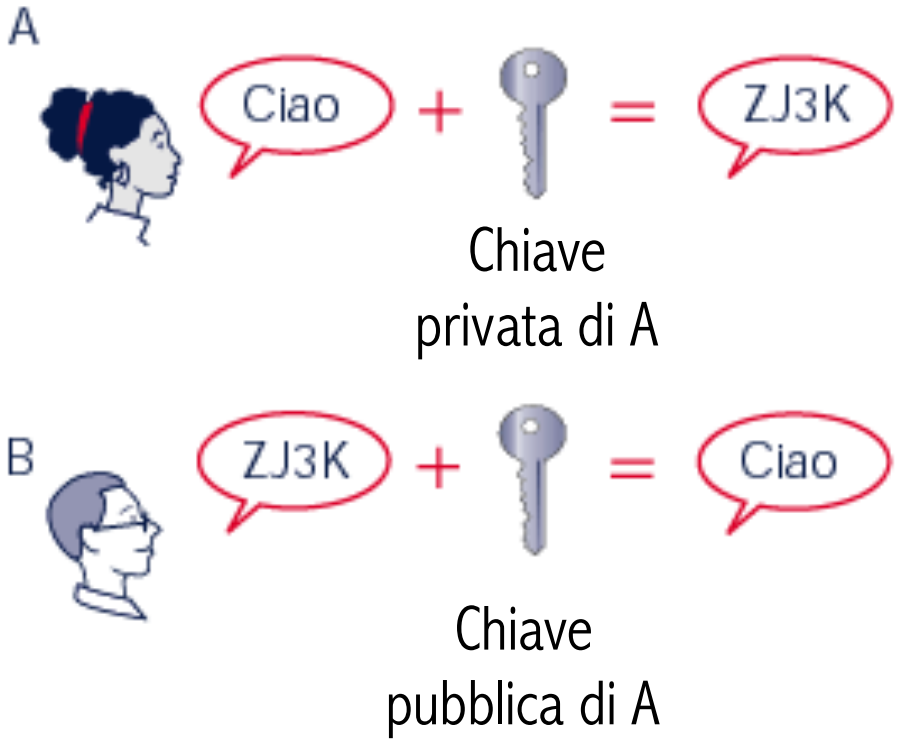
Sistema di crittografia asimmetrica (a doppia chiave pubblica/privata)

*Attraverso il sistema a chiave pubblica non è solo possibile mantenere la riservatezza, ma anche verificare l'**autenticità** e l'**integrità** di un messaggio.*

*Quest'ultima attraverso la cosiddetta **firma digitale**.*

Sistema di crittografia asimmetrica (a doppia chiave pubblica/privata)

Requisito della **autenticità**



Il mittente (A) vuole essere sicuro che il destinatario (B) possa riconoscere l'autenticità (dell'estensore) del documento/messaggio.

In tal caso, (A) dopo aver prodotto il documento/messaggio, lo cifra con la propria chiave privata.

Il destinatario (B) lo decifra con la chiave pubblica del mittente: in caso di esito positivo, è dimostrata l'autenticità del documento.

Sistema di crittografia asimmetrica (a doppia chiave pubblica/privata)

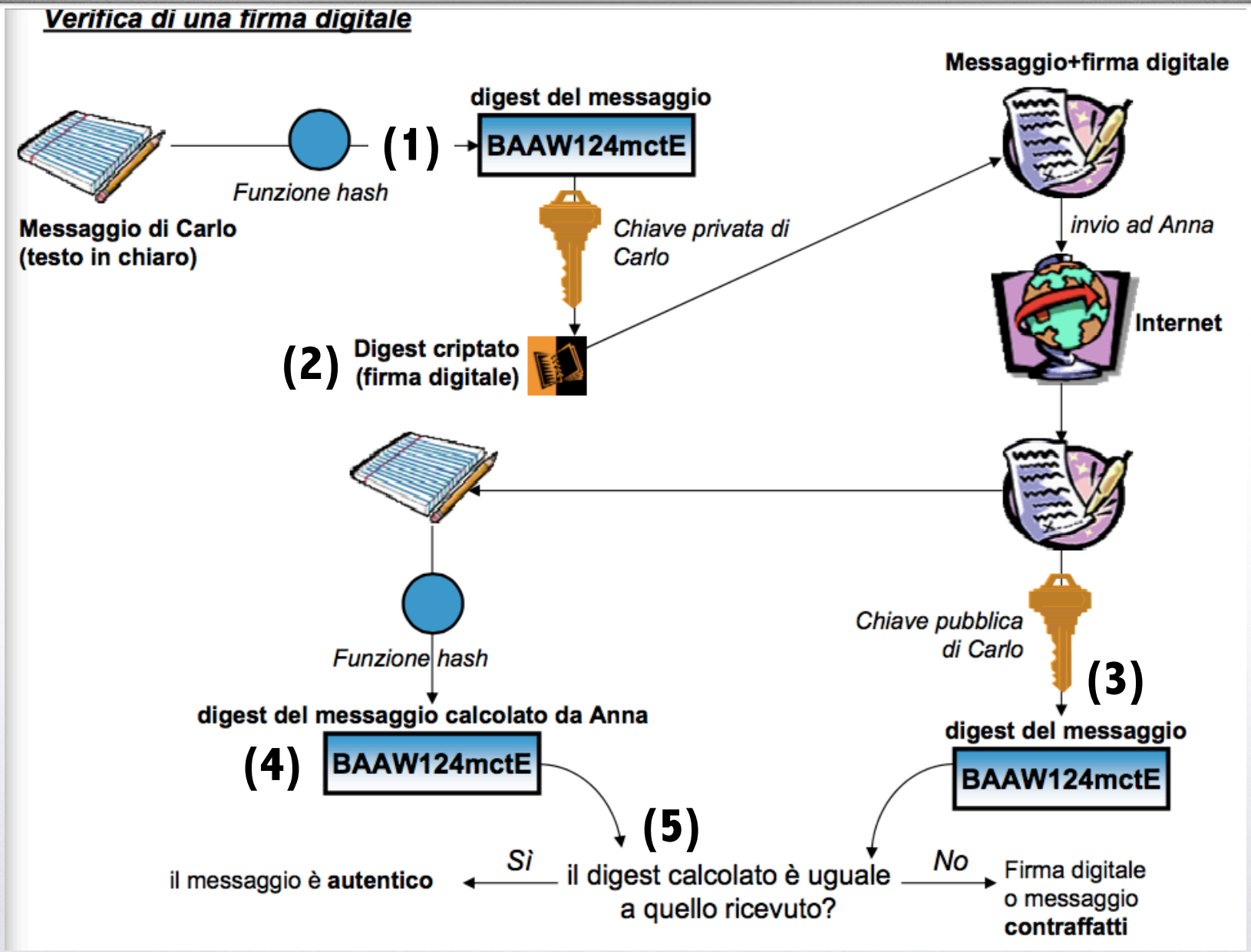
Requisiti di **riservatezza** + **autenticità**

La firma digitale

Si tratta di un processo di codifica così articolato:

1. dal messaggio viene derivata (tramite tecniche "hash") una breve stringa, detta **digest** o "impronta";
2. il digest codificato con la chiave privata del mittente produce la **firma digitale**;
3. la firma digitale viene decodificata con la chiave pubblica del mittente (se OK il messaggio è autentico), riottenendo il digest di partenza;
4. dal messaggio ricevuto viene ricalcolato il digest;
5. se digest ricevuto = digest calcolato $\Longrightarrow$ messaggio integro

(se è richiesta la riservatezza basta utilizzare una chiave simmetrica oppure la chiave pubblica del destinatario)

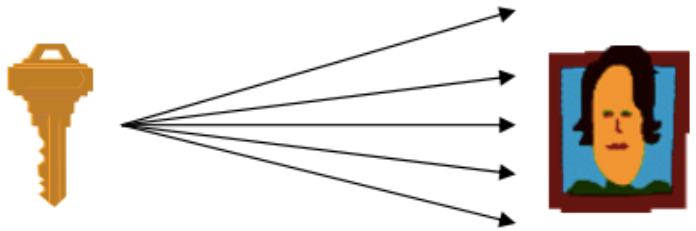

Verifica di una firma digitale
Messaggio+firma digitale
digest del messaggio
BAAW124mctE
(1)
Funzione hash
Messaggio di Carlo
(testo in chiaro)
Chiave privata di
Carlo
invio ad Anna
Internet
(2)
Digest criptato
(firma digitale)
Funzione hash
Chiave pubblica
di Carlo
(3)
digest del messaggio calcolato da Anna
(4)
BAAW124mctE
digest del messaggio
BAAW124mctE
(5)
il messaggio è autentico
Sì
il digest calcolato è uguale
a quello ricevuto?
No
Firma digitale
o messaggio
contraffatti

La firma digitale

Caratteristiche della funzione matematica "**hash**" (come disciplinato dall'art. 1 lett. c) dell'Allegato tecnico al D.P.C.M. 08/02/1999):

1. l'impronta ottenuta è di lunghezza fissa, a prescindere dal documento/messaggio di partenza;
2. si tratta di un processo non reversibile (dall'impronta non si può risalire al documento/messaggio);
3. a documenti/messaggi differenti (anche per un solo carattere) corrispondono impronte differenti.

CERTIFICATI DIGITALI



- come distribuire la propria chiave pubblica?
- pericolo falsificazione "personalità"

⇓

CERTIFICATE AUTHORITY

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

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