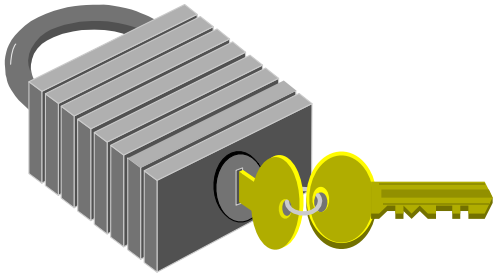
Sicurezza digitale



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

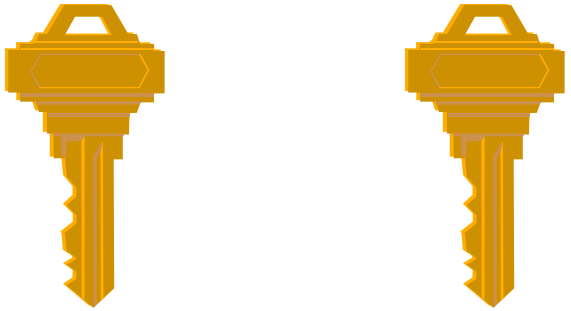
soddisfatti mediante

- **crittografia** = codifica dei dati in forma "illeggibile" per assicurare la riservatezza => autenticazione mittente + integrità messaggio

==> richiede un algoritmo ed una chiave

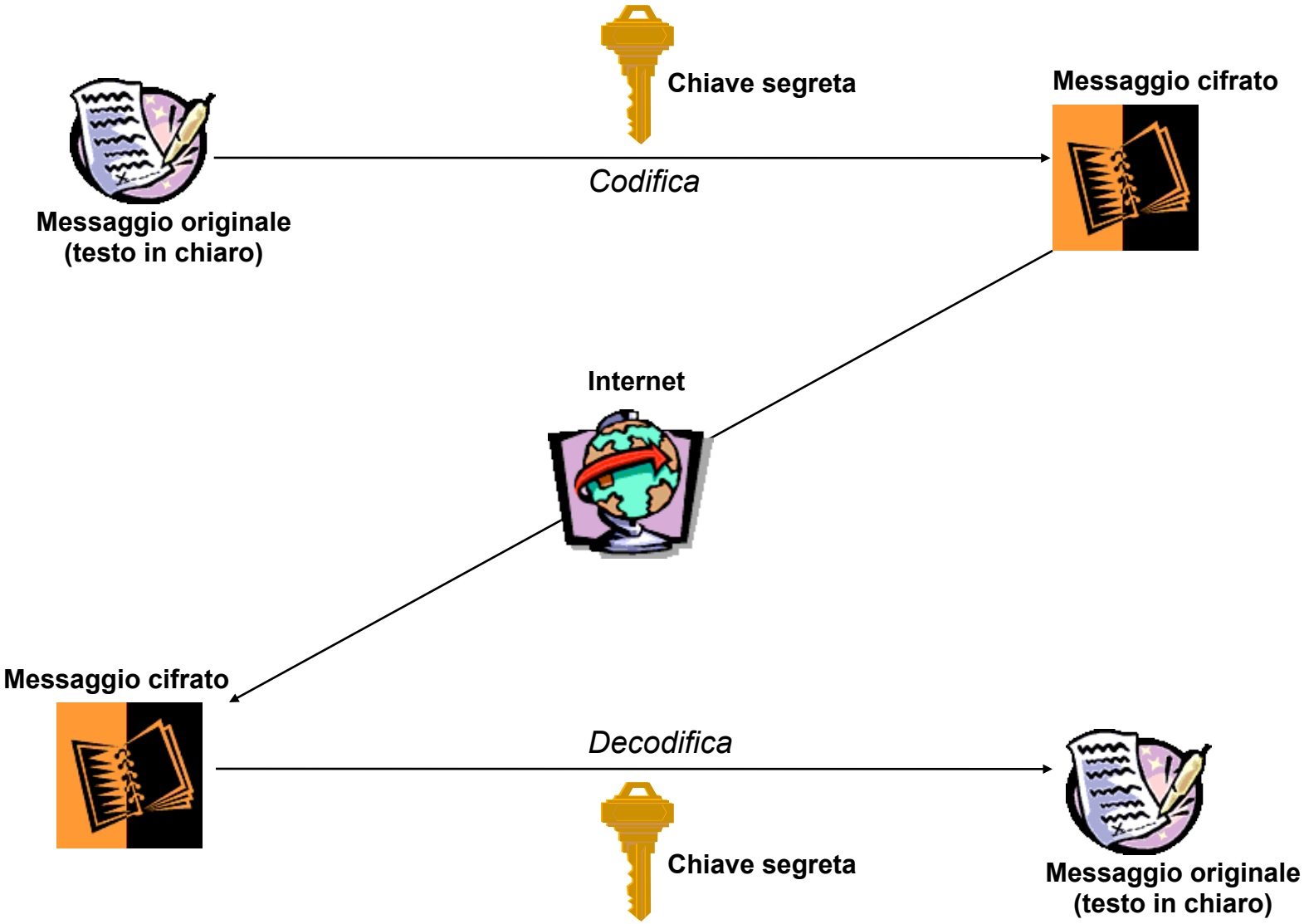
(chiave + lunga = >> sicurezza)

Crittografia simmetrica



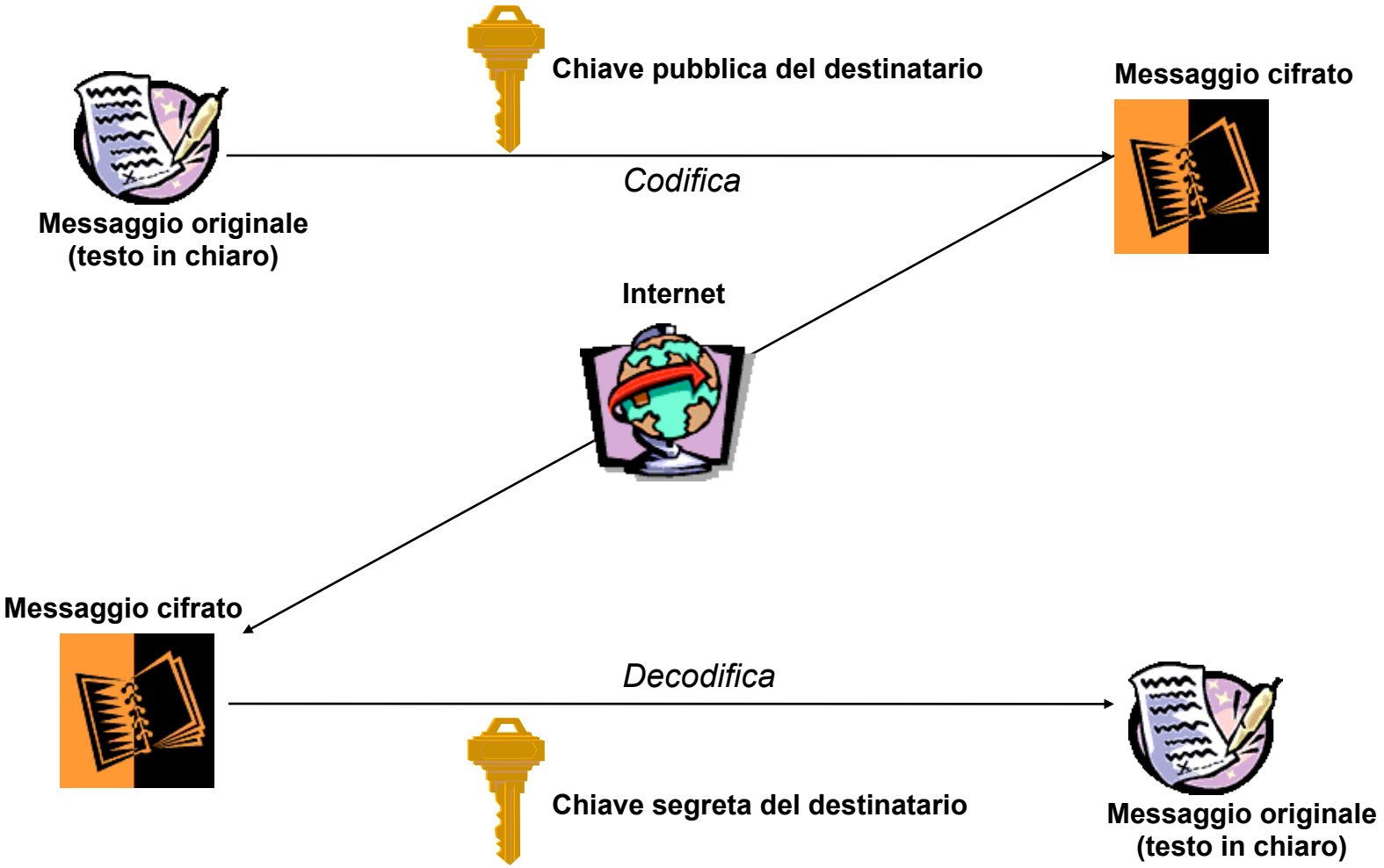
- sia il mittente che il destinatario posseggono la **stessa chiave segreta**
- è necessaria una **diversa chiave segreta** per ogni destinatario
- **non vi è garanzia** di autenticità ed univocità del mittente

Crittografia a chiave simmetrica



Crittografia asimmetrica

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



Crittografia asimmetrica

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

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

Chiave pubblica di Anna

Messaggio originale inviato da Carlo

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

Crittografia asimmetrica

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)*

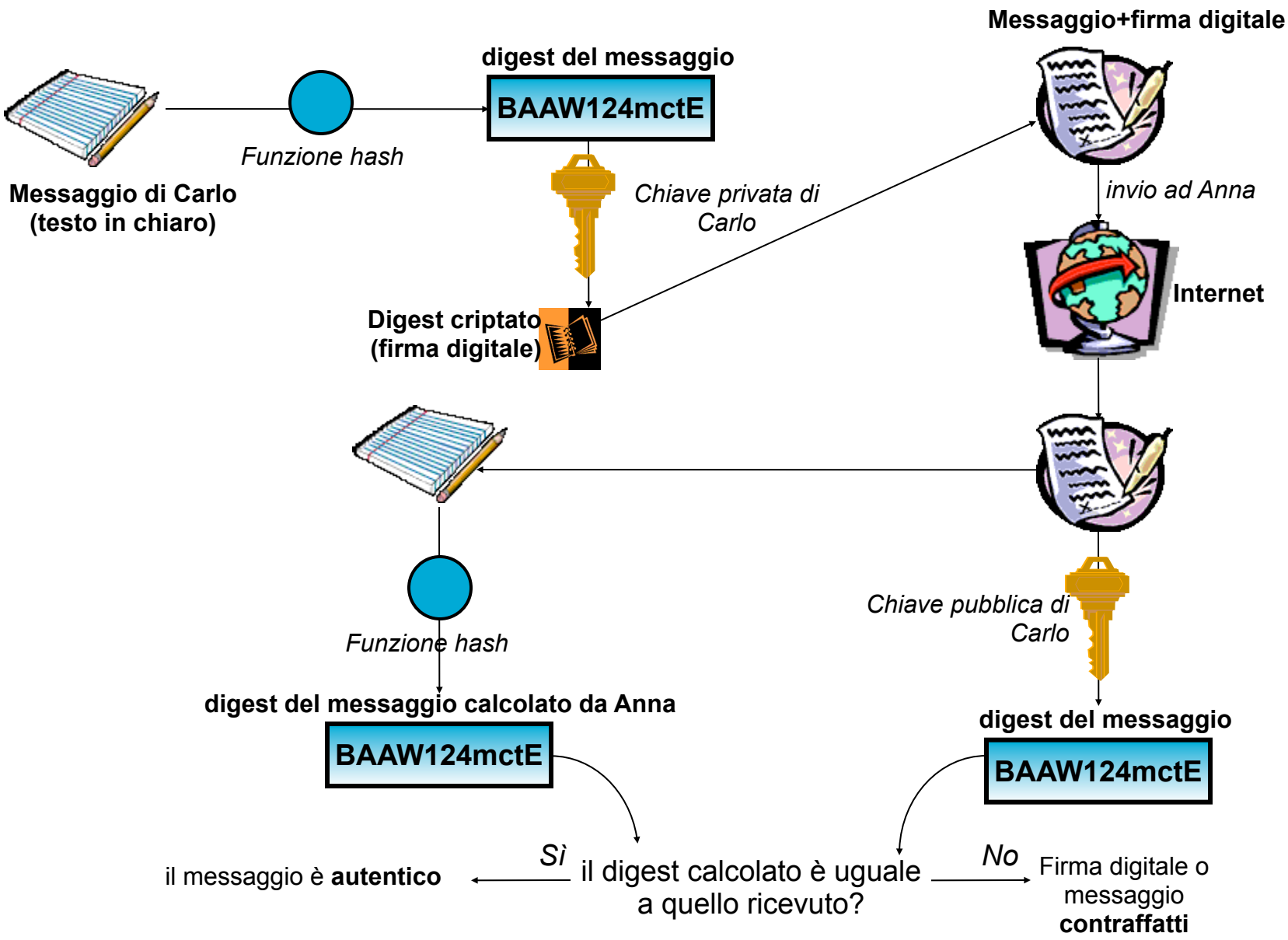
MA chiunque, con la chiave pubblica, può intercettare e decodificare e/o alterare il messaggio originario

Firma digitale

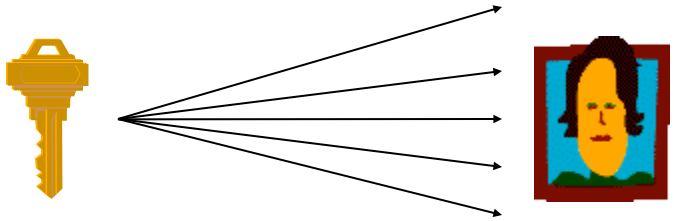
- processo di codifica lento => "message digest" (breve stringa derivata dal messaggio)
- digest codificato con la chiave privata (**firma digitale**)
- digest ricevuto = digest calcolato => messaggio integro

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

Verifica di una firma digitale



Certificato digitale



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

⇓

CERTIFICATE AUTHORITY (18 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, CCIAA, Poste, etc…

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

Sviluppi futuri

- 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