UNITELMA SAPIENZA

SAPIENZA
UNIVERSITÀ DI ROMA
DIPARTIMENTO DI INFORMATICA

Sicurezza della comunicazione tra due entità

Prof.ssa Gaia Maselli
maselli@di.uniroma1.it

La sicurezza nelle reti

Principi di crittografia

Integrità dei messaggi

Autenticazione end-to-end

Sicurezza nella comunicazione

Riservatezza o confidenzialità: solo mittente e destinatario devono comprendere il contenuto del messaggio

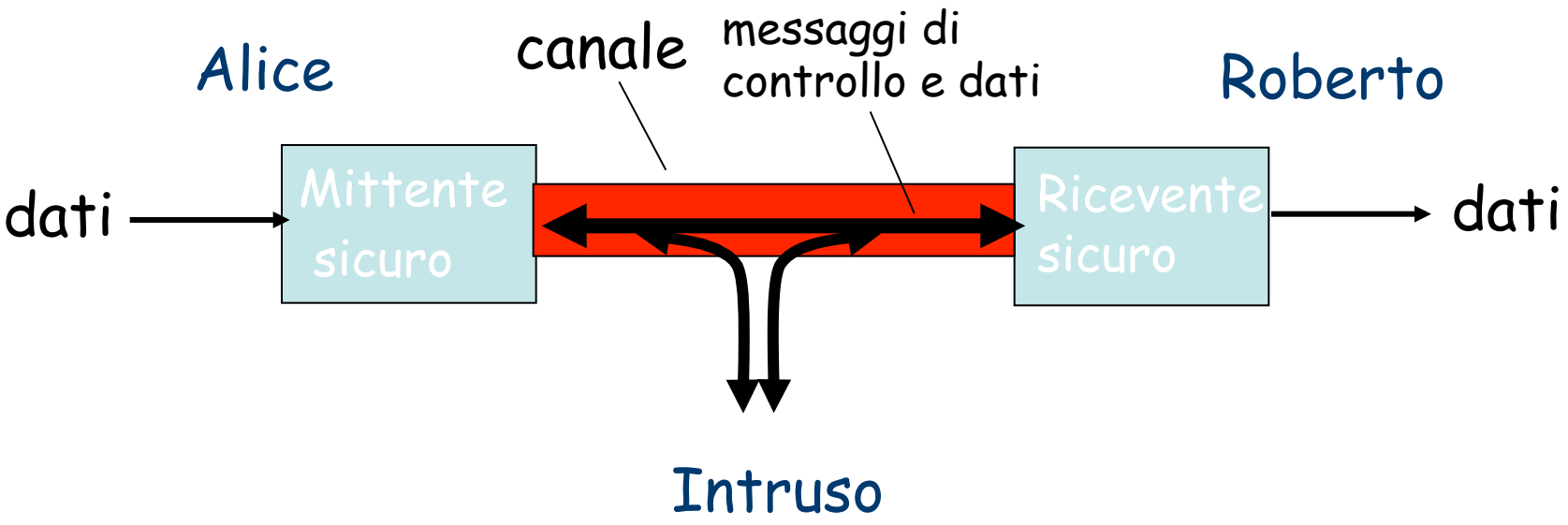
Autenticazione: mittente e destinatario devono essere sicuri della loro identità

Integrità del messaggio: mittente e destinatario devono essere sicuri che il contenuto non subisca alterazioni durante la trasmissione (per cause fortuite o per manipolazioni)

Disponibilità e controllo dell'accesso: un servizio deve essere accessibile a chi è legittimamente autorizzato.

Mittente, ricevente e intruso: Alice, Roberto e l'intruso

- Scenario ben noto nel mondo della sicurezza di rete
- Roberto e Alice vogliono comunicare in modo sicuro
- Un intruso può intercettare, rimuovere, aggiungere messaggi o modificare il loro contenuto



Chi sono Alice e Roberto?

Nella vita reale Alice e Roberto possono essere:

- browser/server Web durante una transazione elettronica (es. un acquisto on-line)
- client/server di banche on-line
- server DNS
- sistemi che si scambiano tabelle d'instradamento
- altro

Possibili attacchi

D: Cosa può fare un nemico?

R: Molto!

- *spiare:* intercettare i messaggi
- *aggiungere* messaggi e sovraccaricare il sistema
- *impersonare* un altro soggetto
- *dirottare* una sessione in corso e sostituirsi al mittente o al destinatario
- *negare il servizio*

E molto altro ancora! .....

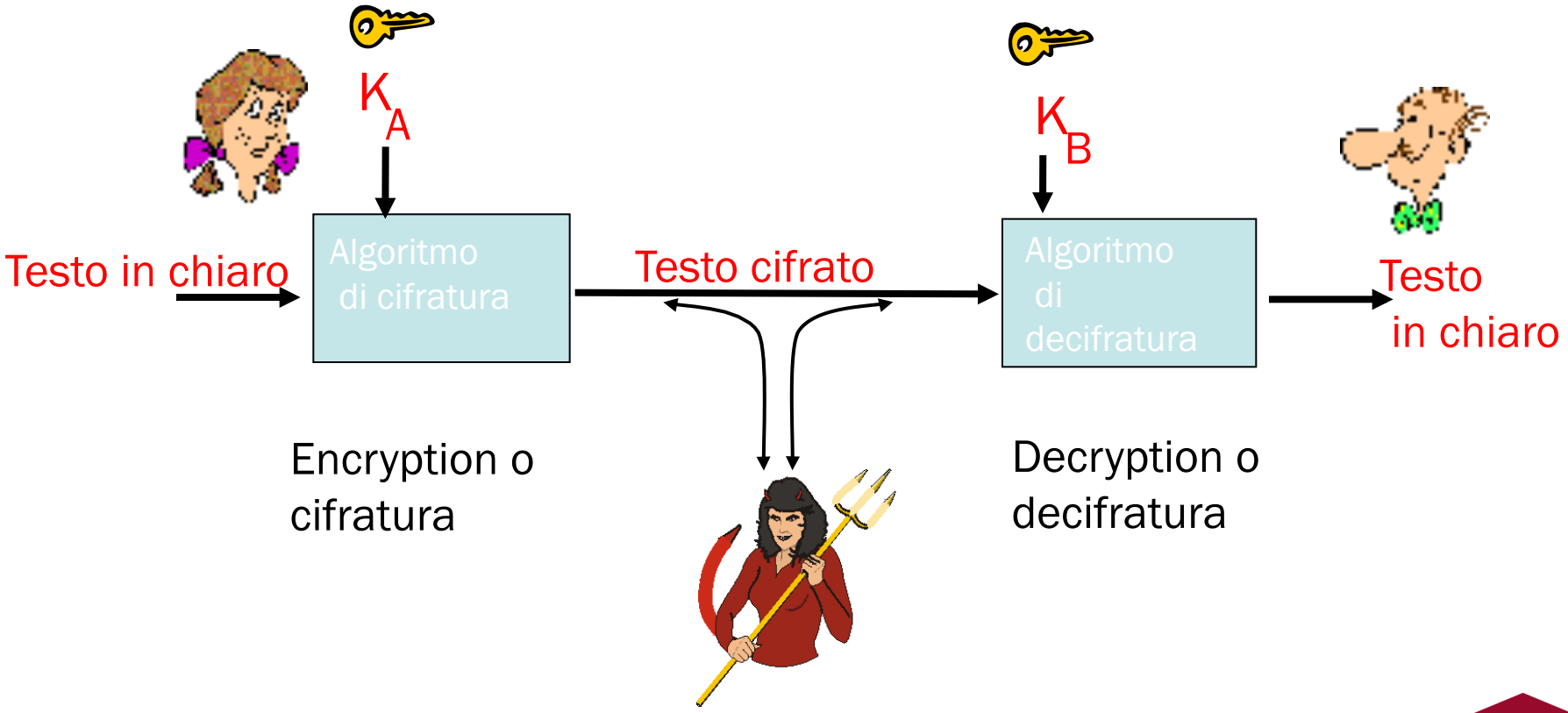
Principi di crittografia

Integrità dei messaggi

Autenticazione end-to-end

Principi di crittografia

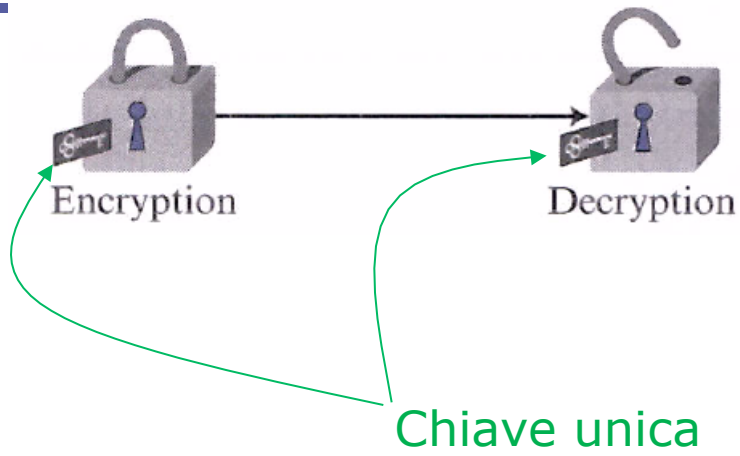
Crittografia: trasformazione dei messaggi per renderli sicuri e immuni agli attacchi – garantisce confidenzialità (riservatezza)



Metodi

Sistemi a chiave simmetrica:

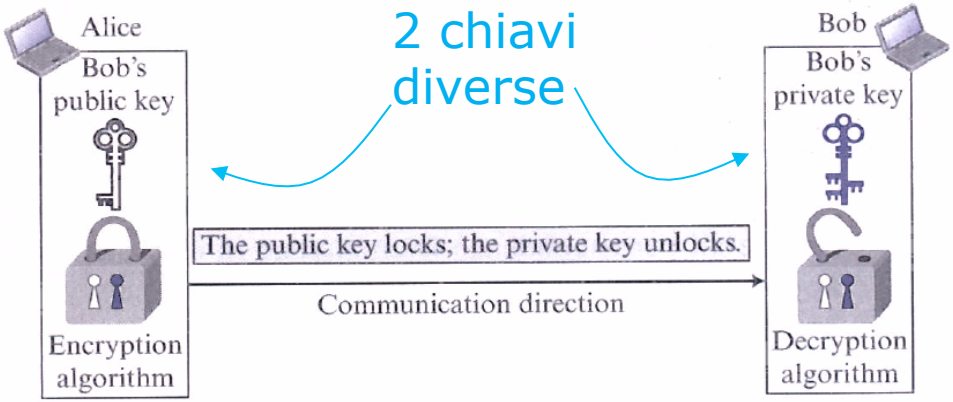
la chiave per la cifratura e decifratura è la stessa e può essere usata per comunicazione bidirezionale (da cui il termine simmetrica)



Sistemi a chiave asimmetrica:

si usa una coppia di chiavi associate al destinatario:

- la chiave di cifratura è **pubblica**
- la chiave di decifratura è **privata**
- Comunicazione unidirezionale con una coppia di chiavi



Crittografia a chiave simmetrica

Per **cifrare** il messaggio è necessario:

- Algoritmo di cifratura
- Chiave simmetrica condivisa

Per **decifrare** il messaggio è necessario:

- Algoritmo di decifratura
- Chiave simmetrica condivisa

N.B. La chiave simmetrica condivisa è segreta e deve essere scambiata a priori

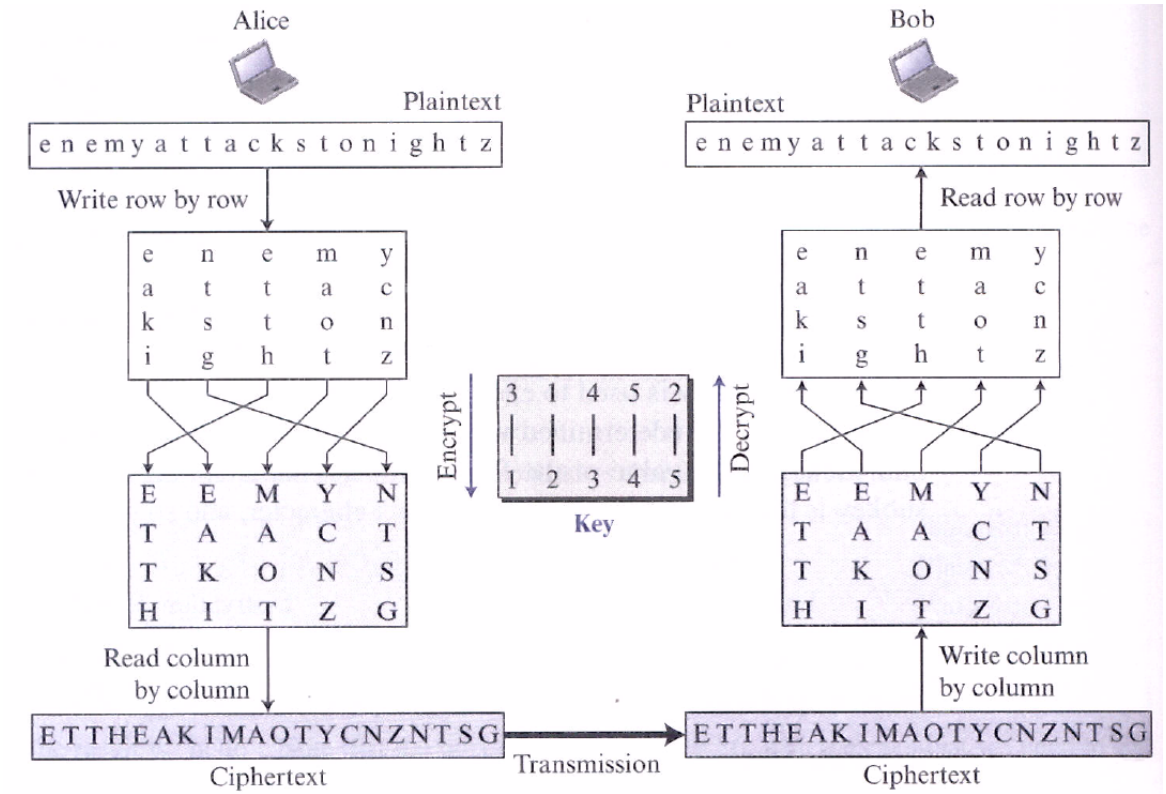
Metodi di cifratura simmetrica

Per sostituzione

- Cifrario monoalfabetico: sostituzione di una lettera con un'altra

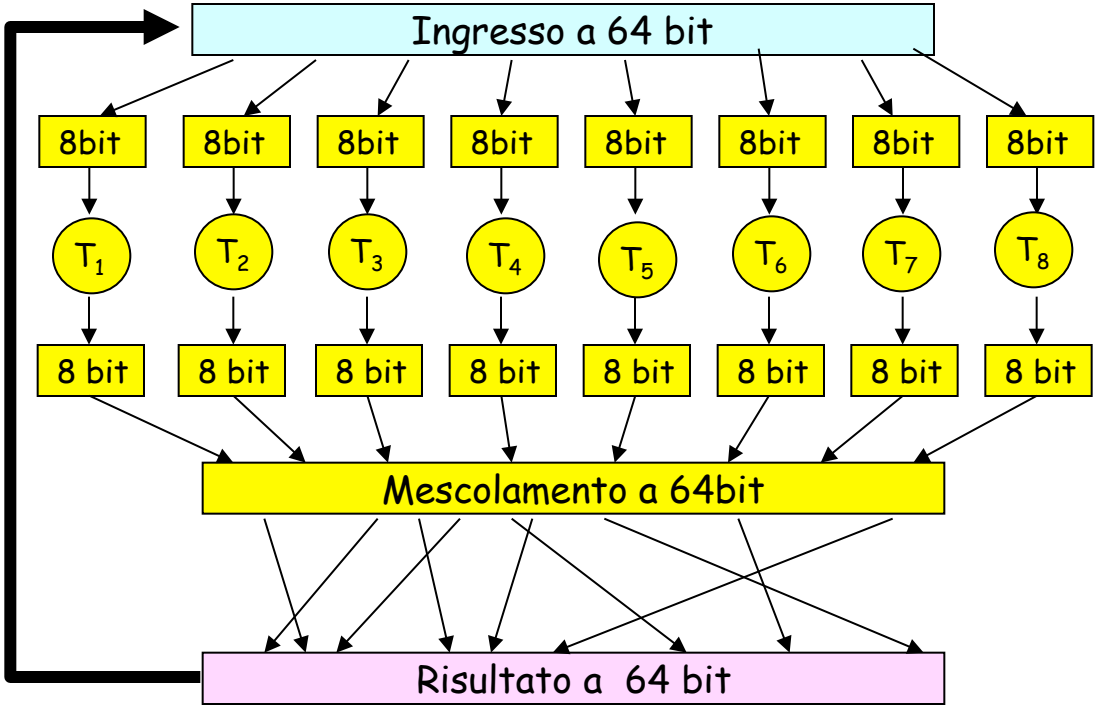
Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	N	O	A	T	R	B	E	C	F	U	X	D	Q	G	Y	L	K	H	V	I	J	M	P	Z	S	W

Per trasposizione



Cifrario a blocchi

ciclo per
n iterazioni



- T_i: tabelle di corrispondenza tra blocco in chiaro e blocco cifrato

- DES (Data Encryption Standard) è un esempio di cifrario a blocchi moderno

Crittografia a chiave asimmetrica (o pubblica)

UNITELMA SAPIENZA

SAPIENZA
UNIVERSITÀ DI ROMA
DIPARTIMENTO DI INFORMATICA

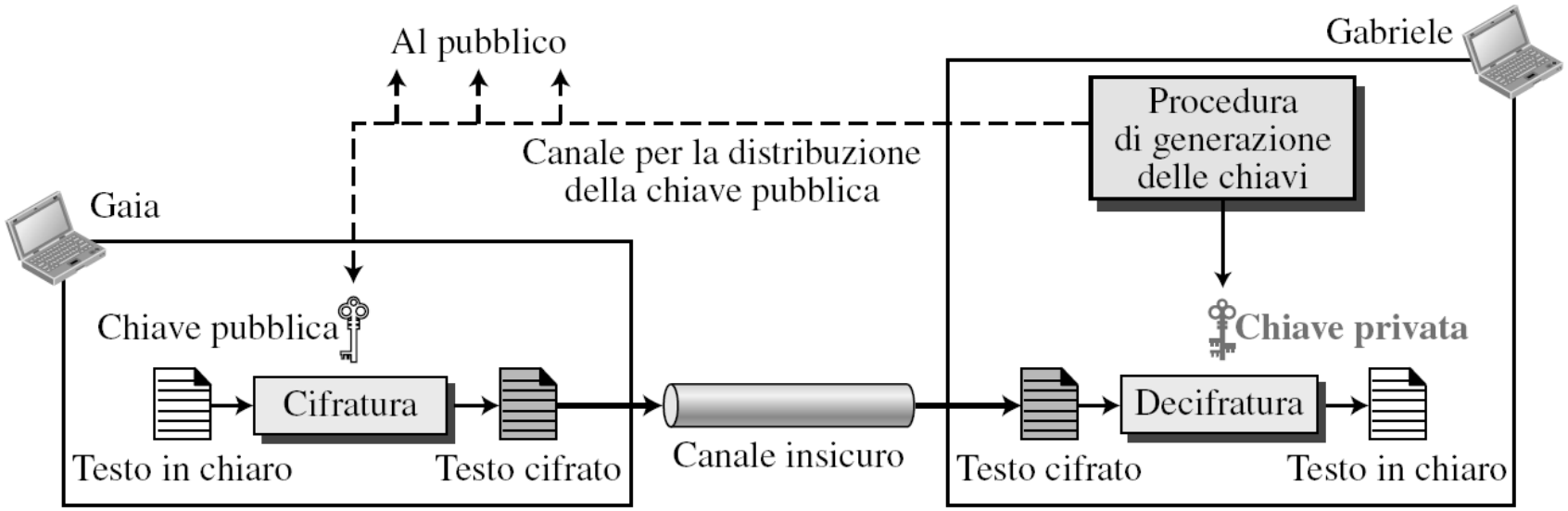
Crittografia a chiave simmetrica

- Richiede che mittente e destinatario condividano una chiave segreta
- D: come si concorda la chiave (specialmente se i due interlocutori non si sono mai "incontrati")?

Crittografia a chiave asimmetrica o pubblica

- approccio radicalmente diverso [Diffie-Hellman, RSA]
- mittente e destinatario *non* condividono una chiave segreta
- la chiave di cifratura *pubblica* è nota *a tutti*
- la chiave di decifratura *privata* è nota solo al destinatario

Crittografia a chiave pubblica



- Una coppia di chiavi può essere usata solo per comunicare in una direzione (il destinatario è il possessore delle chiavi)
- La coppia di chiavi è unica per tutti i mittenti

Algoritmi di cifratura a chiave pubblica

- La crittografia asimmetrica è solitamente impiegata per cifrare/decifare quantità limitate di informazioni (es. la chiave di un cifrario simmetrico)
- Il testo in chiaro e il testo cifrato sono considerati numeri interi
- La cifratura e la decifratura sono funzioni matematiche
- Il testo cifrato può essere inteso come $C = f(K_{pubb}, P)$
- Il testo in chiaro può essere inteso come $P = g(K_{priv}, C)$
- RSA (Rivest, Shamir, Adleman): Algoritmo a chiave asimmetrica largamente diffuso

RSA: scelta delle chiavi

1. Scegliere due numeri primi di valore elevato: *p, q.*
   (es.: 1024 bit ciascuno)

2. Calcolare $n = pq$, $z = (p-1)(q-1)$

3. Scegliere e (con $e < n$) tale che non abbia fattori in comune con z. (*e, z* sono "relativamente primi").

4. Scegliere d tale che $ed-1$ sia esattamente divisibile per z.
   (in altre parole: $ed \bmod z = 1$).

5. La chiave *pubblica* è (n,e), quella *privata* è (n,d).

K_{pubb} K_{priv}

RSA: cifratura, decifratura

0. Dati (n,e) e (n,d) calcolati come abbiamo appena visto,

1. Per la codifica di m si calcola

$$c = m^{e} \bmod n$$

2. Per decifrare il messaggio ricevuto, c, si calcola

$$m = c^{d} \bmod n$$

Incredibile! $m = (\underbrace{m^{e} \bmod n}_{c})^{d} \bmod n$

Un esempio di RSA:

Roberto sceglie $p=5$, $q=7$. Poi $n=35$, $z=24$.

$e=5$ (così e, z sono relativamente primi).

$d=29$ (così $ed-1$ è esattam. divisibile per z).

cifratura:

lettera	m	m^e	$c = m^e \bmod n$
l	12	1524832	17

decifratura:

c	c^d	$m = c^d \bmod n$	lettera
17	481968572106750915091411825223071697	12	l

RSA: un'importante proprietà

La seguente proprietà sarà *molto* utile più avanti:

$$K_{priv}(K_{pubb}(m)) = m = K_{pubb}(K_{priv}(m))$$

Si usa prima la chiave pubblica, e poi quella privata

Si usa prima la chiave privata, e poi quella pubblica

Il risultato non cambia!

La sicurezza nelle reti

- Principi di crittografia → confidenzialità
- Integrità dei messaggi
- Autenticazione end-to-end

Integrità del messaggio

Gabriele riceve un messaggio da Gaia, e vuole essere sicuro che:

- il messaggio provenga effettivamente da Gaia
- il messaggio non sia stato alterato lungo il cammino

Funzioni hash crittografiche

- prende in input m, produce un valore a lunghezza fissa, H(m)
- Deve essere computazionalmente impossibile trovare due messaggi x e y tali che H(x) = H(y)
  - o anche: dato m = H(x), (con x sconosciuta), è impossibile determinare x.

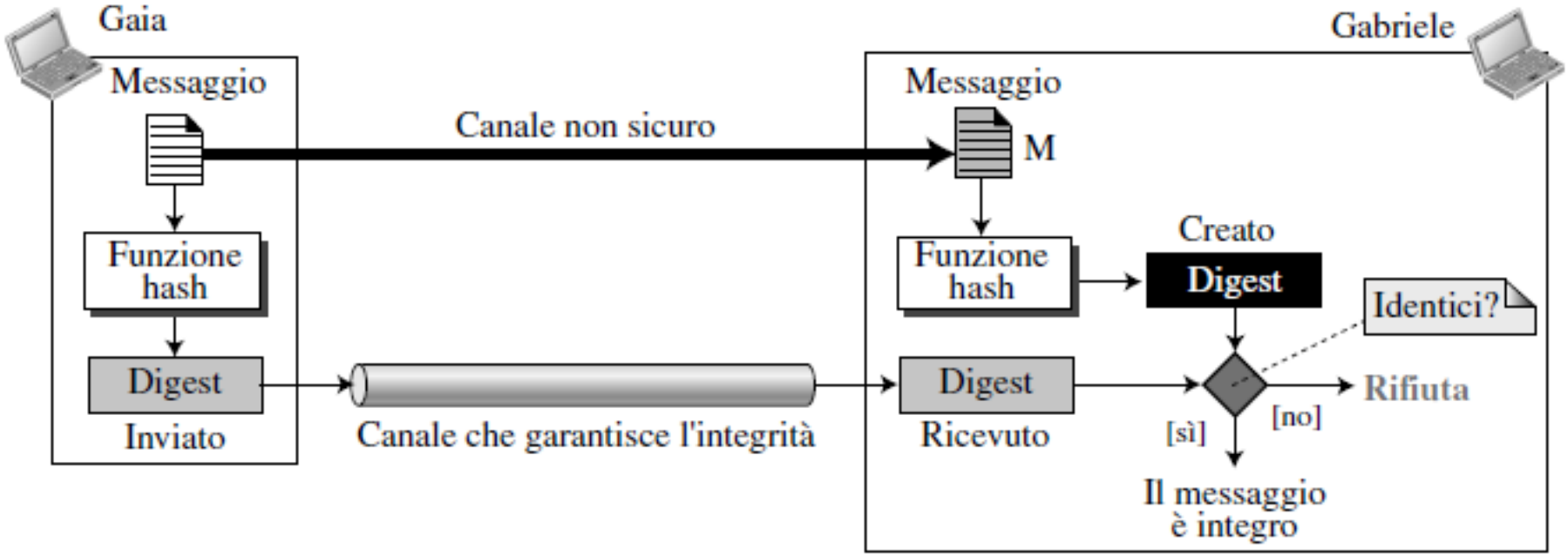
Funzione hash crittografica

Garantisce integrità (il messaggio non è stato cambiato)

Funzione hash che produce *digest* (immagine compressa del messaggio)

Viene inviato sia il messaggio, sia il digest

N.B. il messaggio viaggia in chiaro!!!



Funzioni hash

- MD5 è molto usato per l'hash dei messaggi (RFC 1321)
  - MD sta per Message Digest
  - Calcola una hash di 128 bit con un processo a 4 fasi
  - Con una stringa x di 128 bit arbitrari, appare difficile costruire un messaggio m il cui hash MD5 sia uguale a x
- È molto usato anche Secure Hash Algorithm (SHA)
  - Standard statunitense [NIST, FIPS PUB 180-1]
  - Produce una sintesi del messaggio di 160 bit

Autenticazione dei messaggi

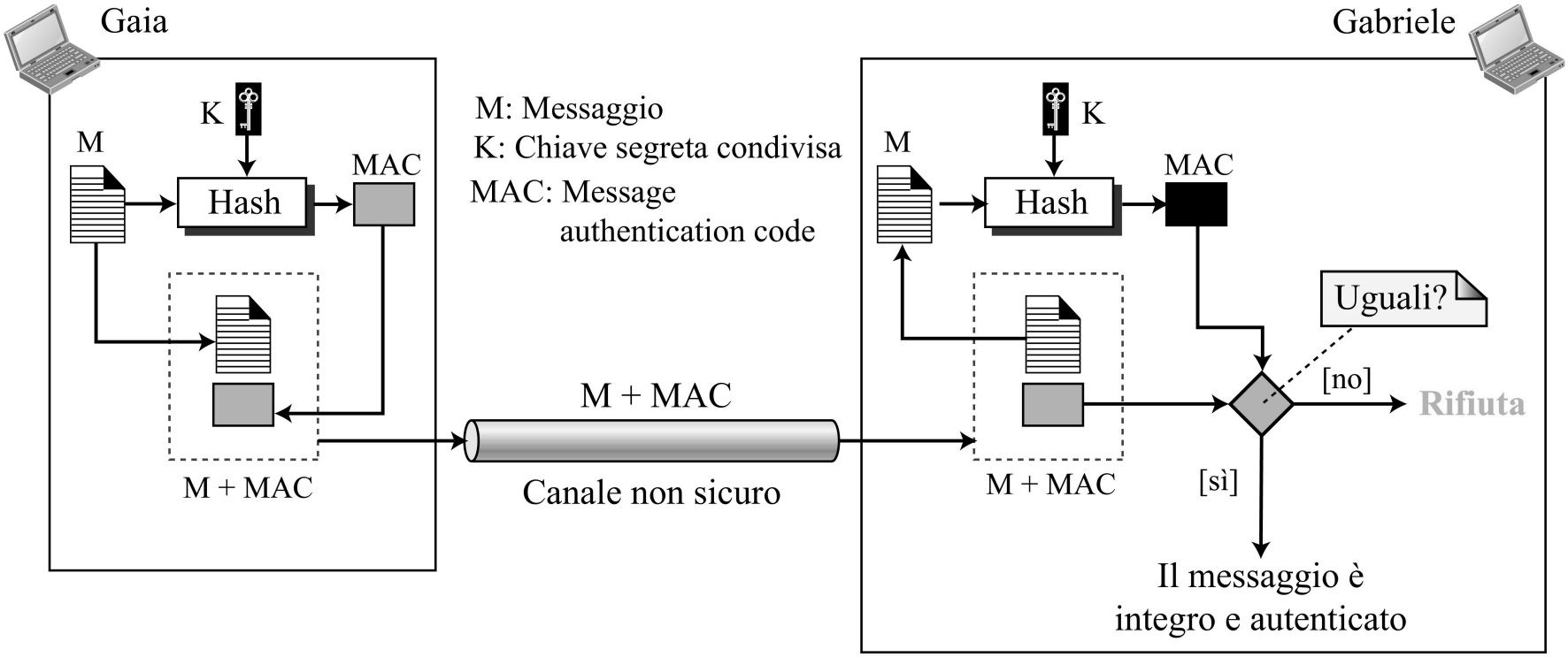
Per autenticare l'origine del messaggio (Il messaggio è stato scritto da Gaia) viene inserito un codice segreto condiviso tra Gaia e Gabriele

Si usa insieme alla hash crittografica per creare un

Message Authentication code (MAC)

MAC

- Integrità + autenticazione
- Funzione hash + codice segreto condiviso



Firma digitale

Tecnica crittografica analoga all'invio di una tradizionale "firma scritta"

- Altro modo di garantire integrità e autenticazione di un messaggio
- Il mittente firma digitalmente un documento, stabilendo che lui è l'unico proprietario/creatore del messaggio.
- Verificabile e non falsificabile: il destinatario può dimostrare che il mittente e nessun altro può aver firmato il documento.
- Avviene mediante l'uso di una coppia di chiave pubblica e privata di chi firma

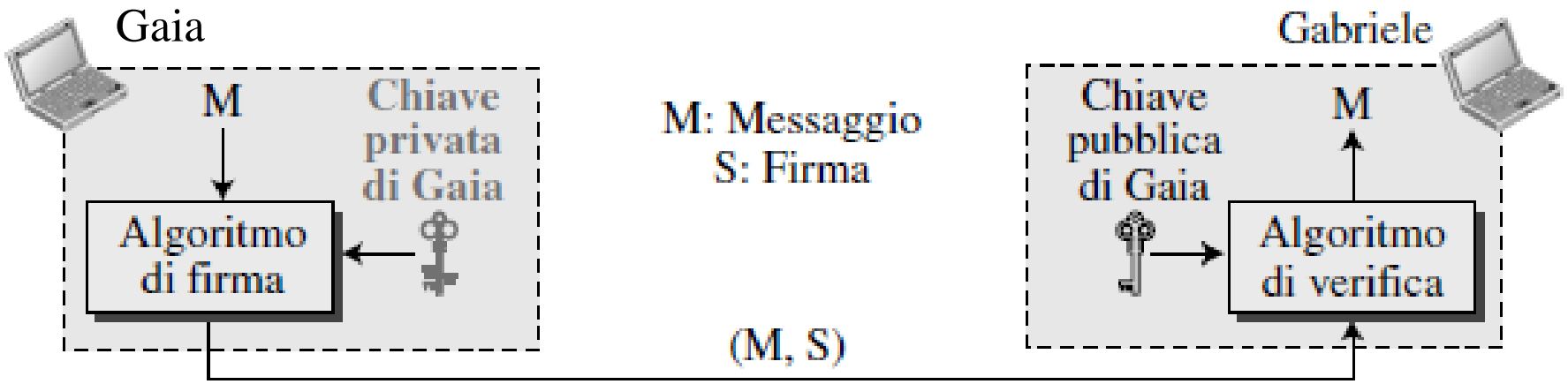
Firma digitale

Creazione della firma digitale di un messaggio M:

Gaia firma un messaggio M, cifrandolo con la sua chiave privata, creando così un messaggio "firmato"

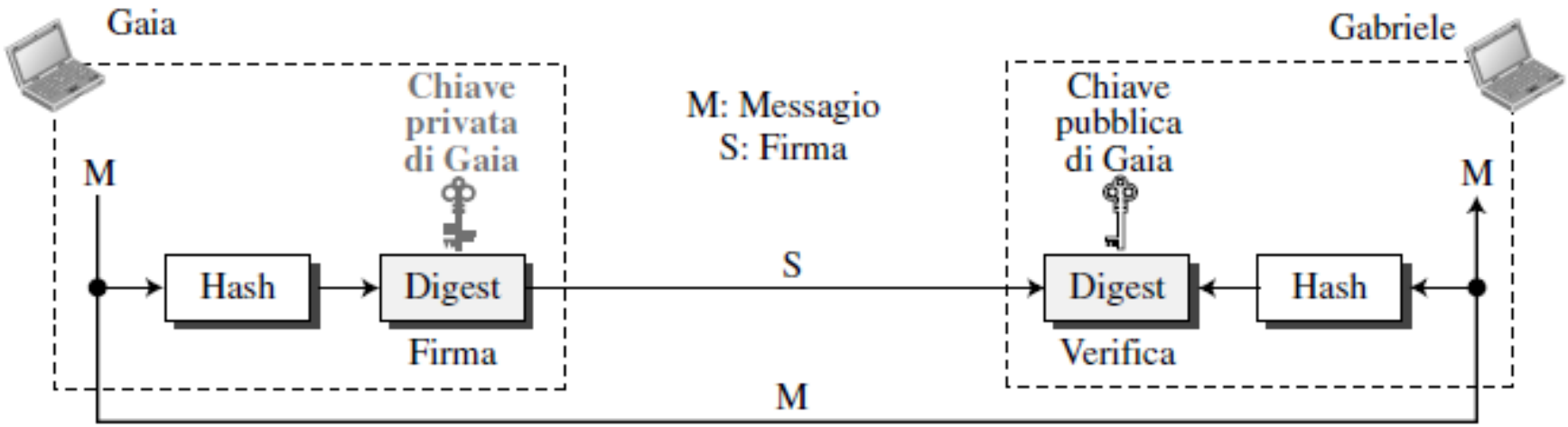
Gabriele decifra il messaggio applicando la chiave pubblica di Gaia

N.B. è il meccanismo di crittografia asimmetrica applicata in modo inverso



Firma digitale (messaggi digest firmati)

- Impossibile firmare un messaggio di un'altra persona a meno che non si conosca la sua chiave segreta
- La firma digitale garantisce la proprietà di non ripudio: Gaia non può negare di aver firmato il documento e Gabriele può verificare che
  - ✓ Gaia ha firmato M
  - ✓ Nessun altro ha firmato M
  - ✓ Gaia ha firmato M e non M'.
- Poiché la crittografia asimmetrica è inefficiente su messaggi lunghi, in genere si applica la firma digitale a un MESSAGE DIGEST



Certificazione della chiave pubblica

Problema per la crittografia a chiave pubblica:

- Quando Gaia riceve la chiave pubblica di Gabriele (attraverso un dischetto, il sito web o via e-mail), come fa a sapere che è veramente la chiave pubblica di Gabriele e non quella di qualcun altro?

Soluzione:

- Autorità di certificazione (CA, *certification authority*)

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")