Cifrari Asimmetrici

Prof. Francesco Bergadano

Dipartimento di Informatica

Università di Torino

Copyright Notice

Prof. Francesco Bergadano

Dipartimento di Informatica

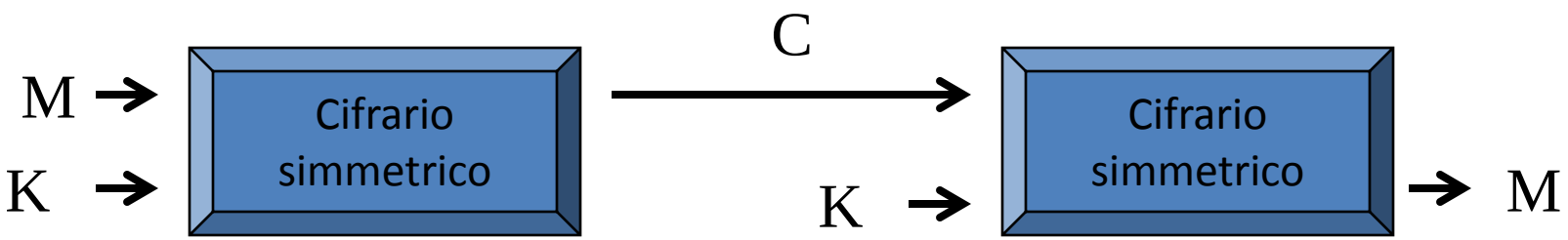
Università di Torino

Cifrari Asimmetrici

“Per cifrare e decifrare si usano chiavi diverse”

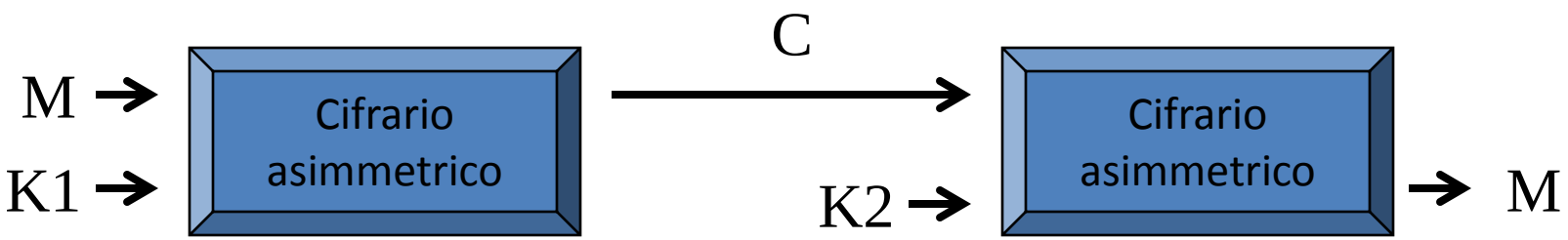
Cifrari Simmetrici

- “Per cifrare e decifrare si
- usa la stessa chiave”



Cifrari Asimmetrici

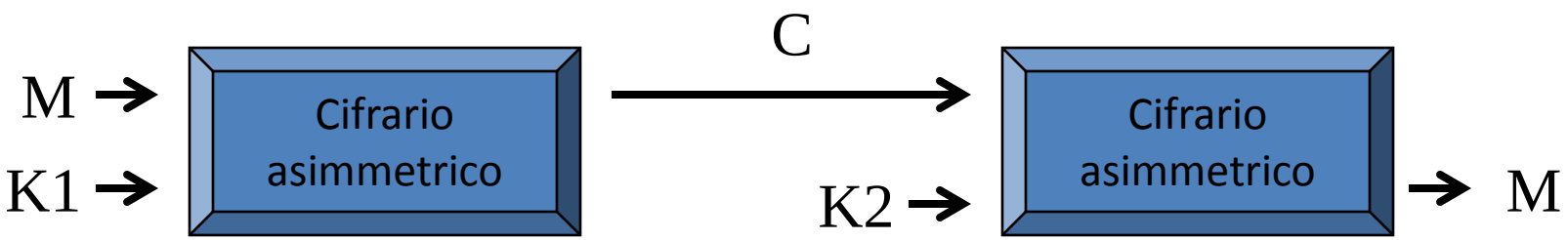
“Per cifrare e decifrare si usano chiavi diverse”



Cifrari asimmetrici

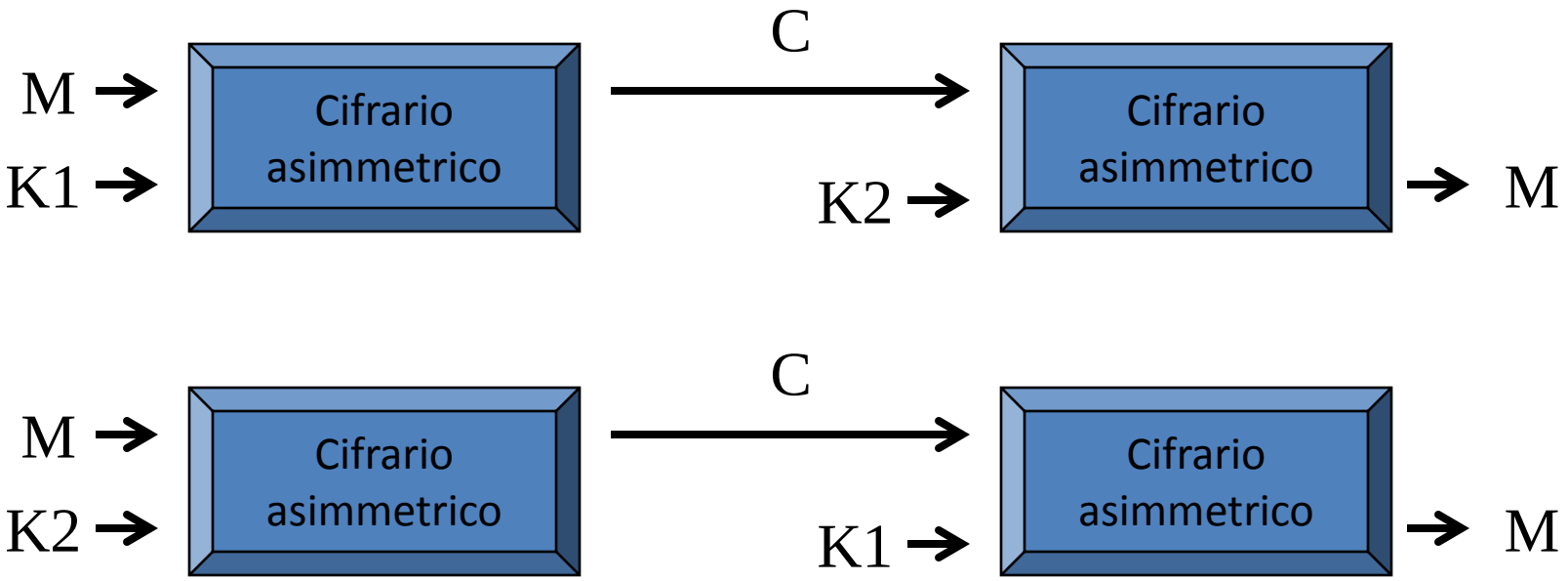
1. Non è possibile ottenere K2 da K1, e viceversa
2. Non è possibile decifrare, anche se si conosce K1

   K1,K2 generate insieme da apposita procedura



Se 1 e' falsa, allora anche 2 e' falsa, quindi se 2 e' vera, anche 1 e' vera

Cifrari asimmetrici - è possibile cifrare con entrambe le chiavi



Cifrari asimmetrici

- Basati su principi completamente diversi da quelli della crittografia convenzionale:
  - nei cifrari convenzionali la difficoltà della lettura di un messaggio cifrato consiste nel fatto che la trasformazione realizzata dal cifrario non è conosciuta
  - nei cifrari asimmetrici la trasformazione è conosciuta, ma è troppo difficile da calcolare se non si conosce l'informazione segreta (trapdoor) utilizzata per generare le chiavi e/o per decifrare.

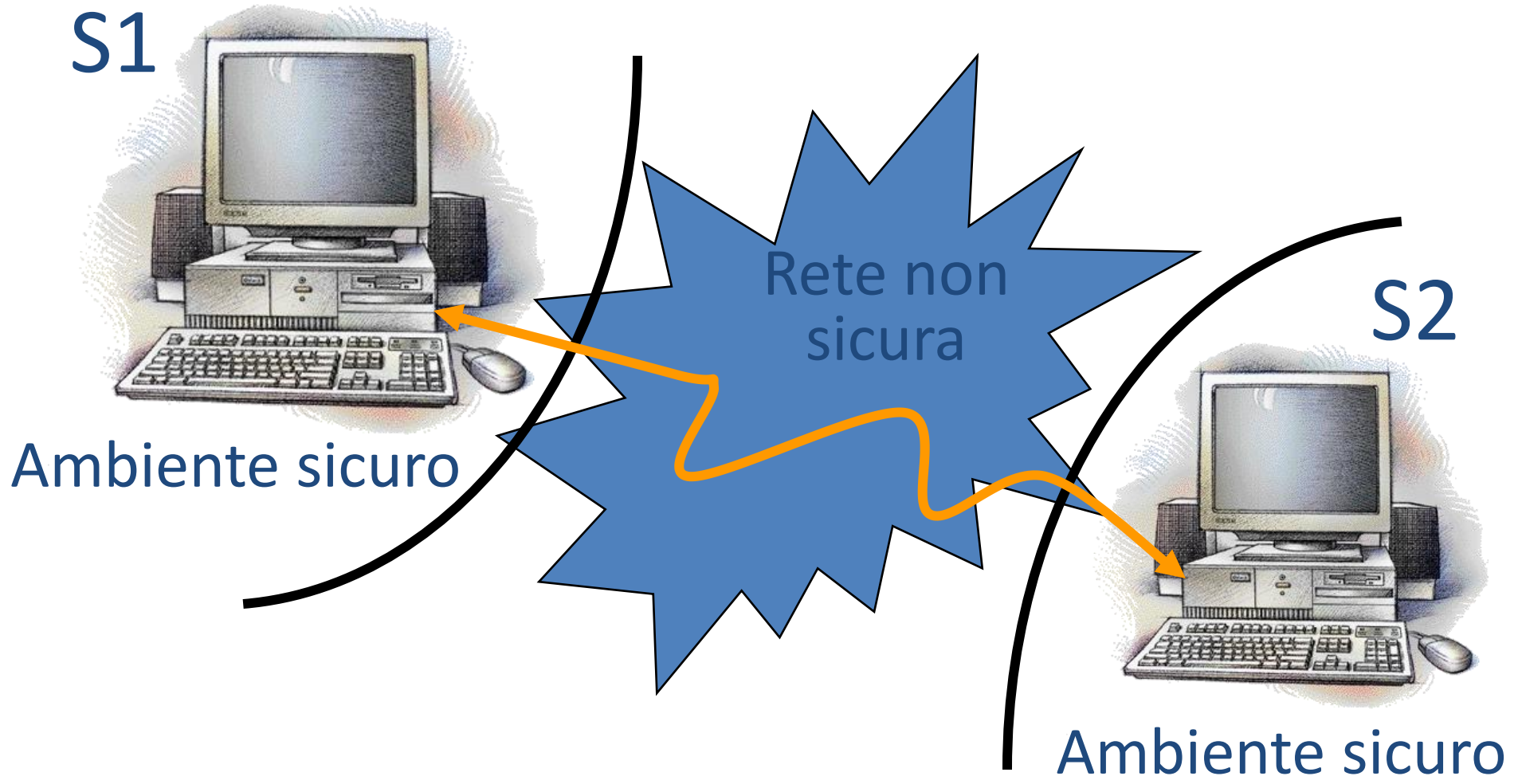
Cifrari asimmetrici

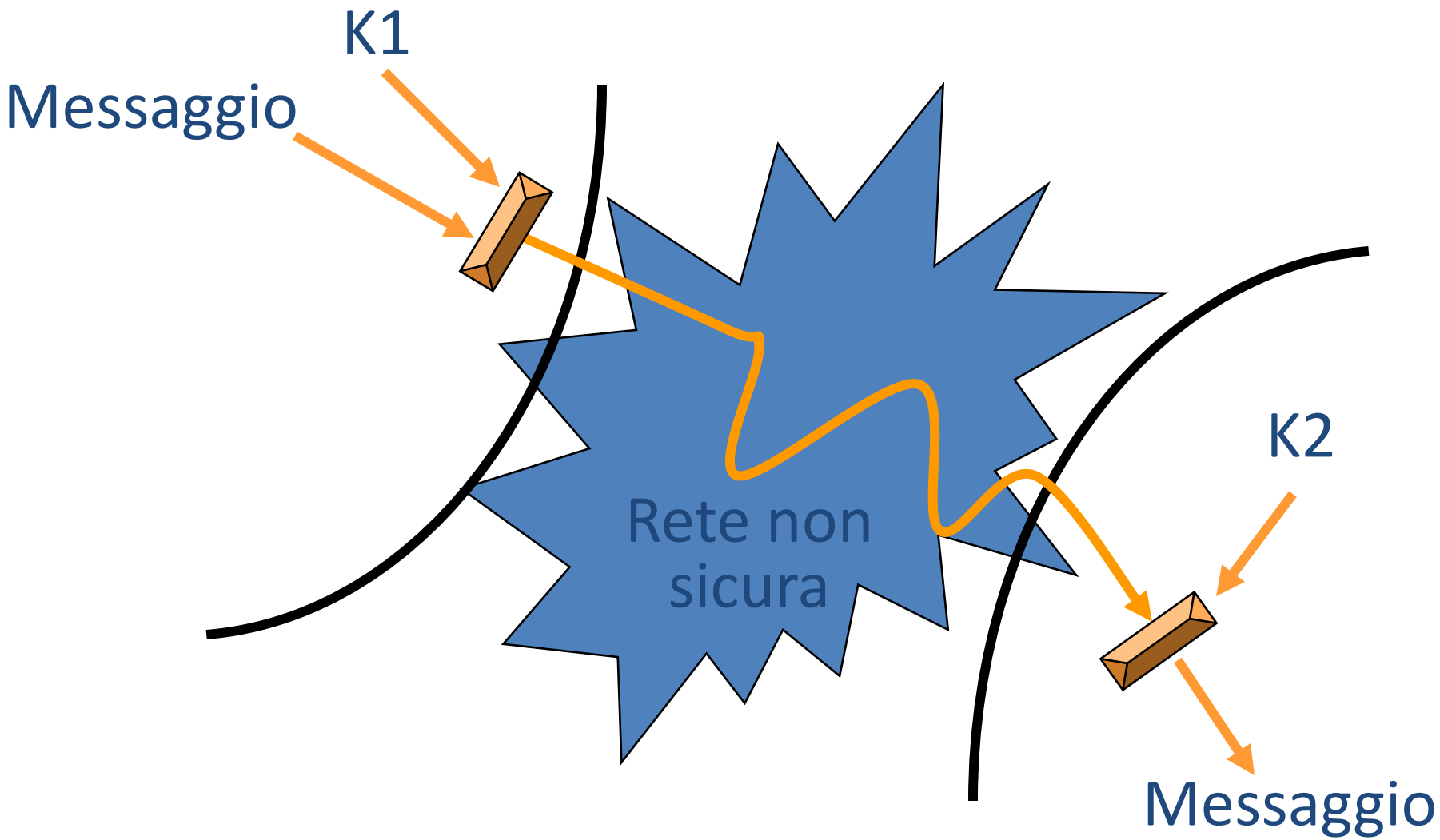
- Compaiono pubblicamente solo a partire dalla fine degli anni 1970, mentre i primi cifrari convenzionali sono antichissimi.
- Richiedono più risorse computazionali sia per cifrare e decifrare, sia per generare le chiavi. Pertanto i cifrari asimmetrici non sostituiscono le tecniche convenzionali, ma generalmente si affiancano ad esse per particolari applicazioni.

Perché i cifrari asimmetrici rappresentano una importante novità, con notevoli conseguenze applicative?

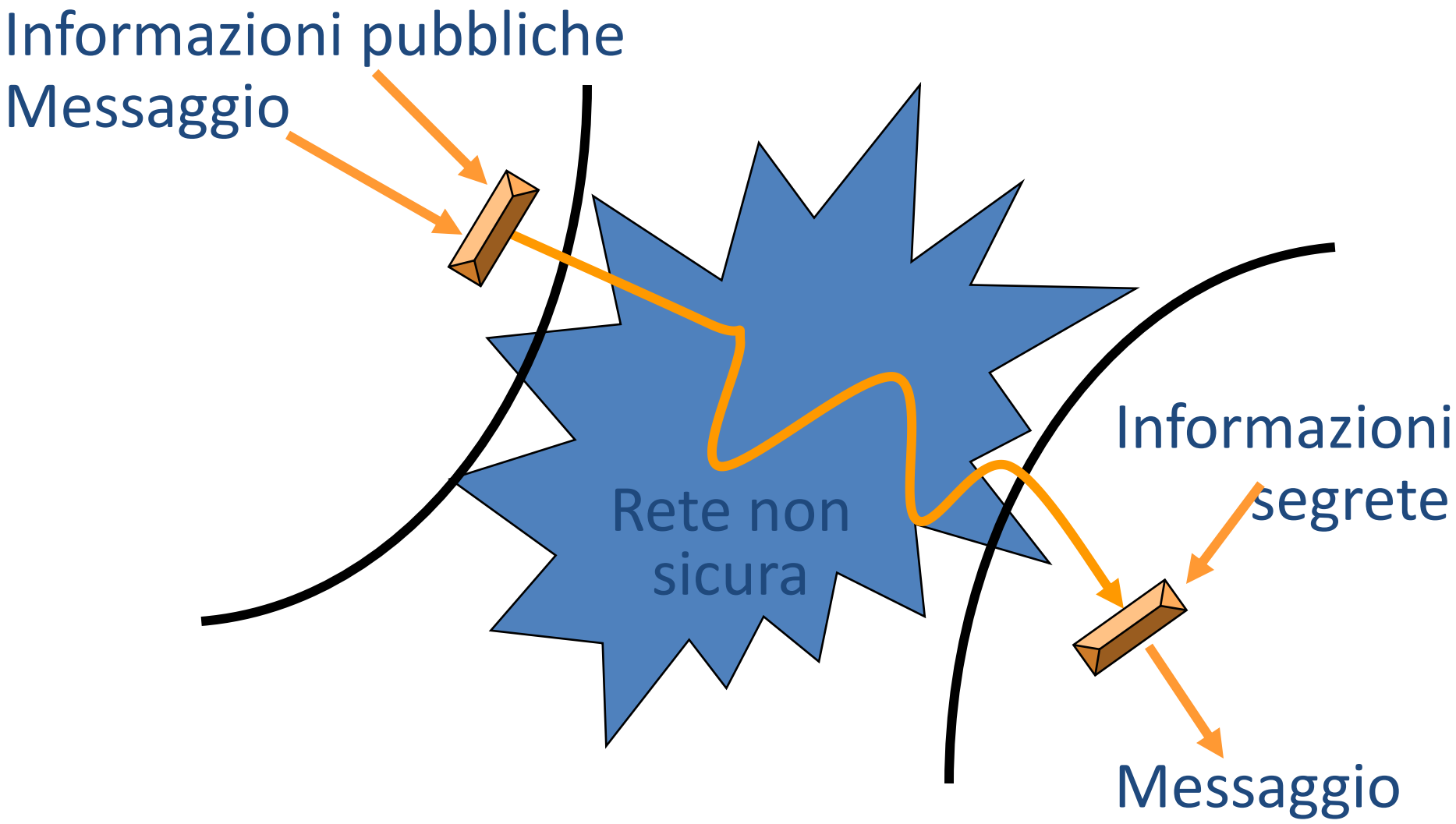
- **Perché diventa possibile cifrare un messaggio senza condividere un segreto con il destinatario → maggiore facilità nella distribuzione delle chiavi**

- **Perché solo chi detiene la chiave di cifratura è in grado di produrre un dato messaggio cifrato → possibilità di effettuare operazioni non disconoscibili (non repudiation)**

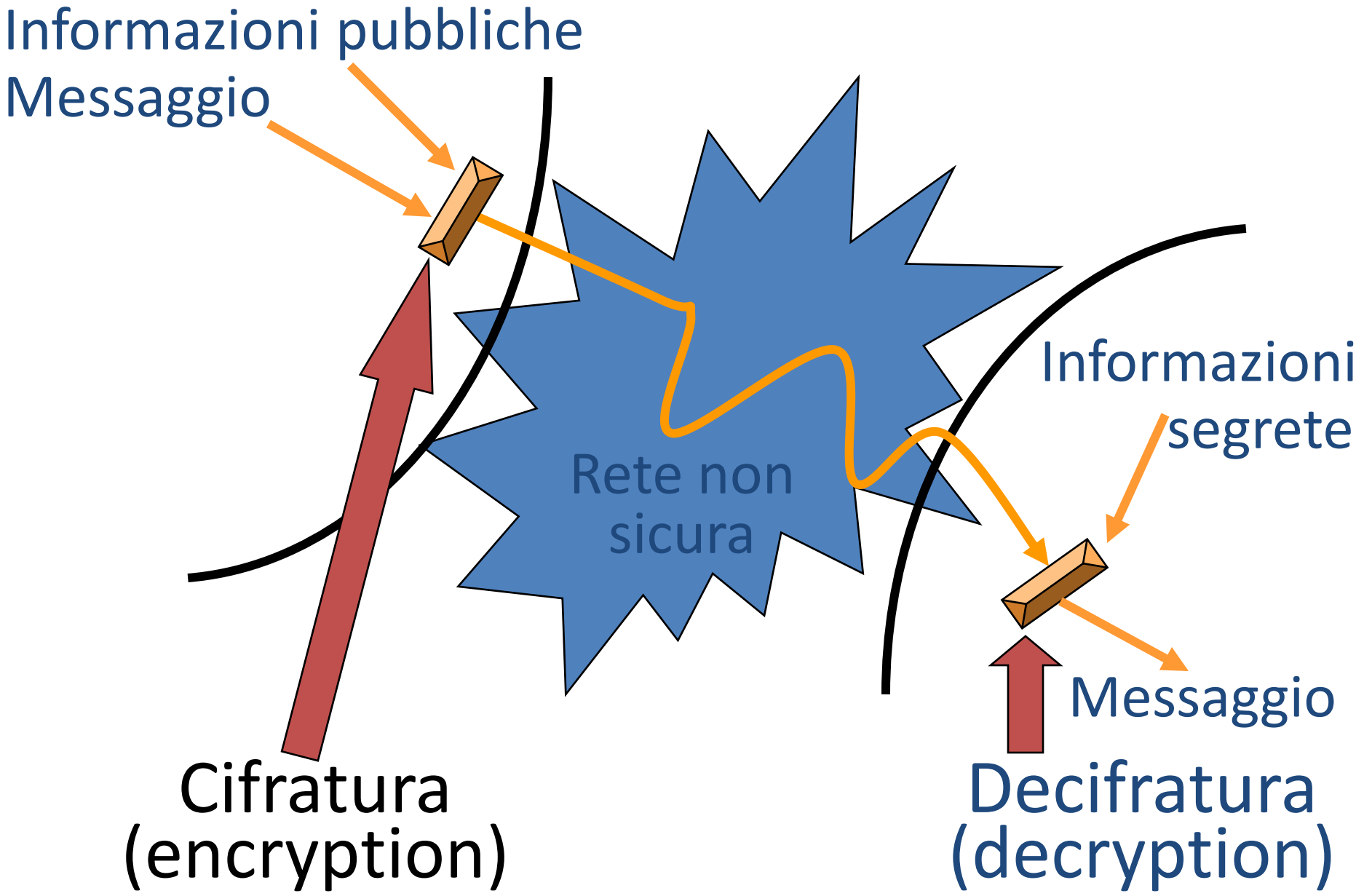

S1
Rete non sicura
S2
Ambiente sicuro
Ambiente sicuro

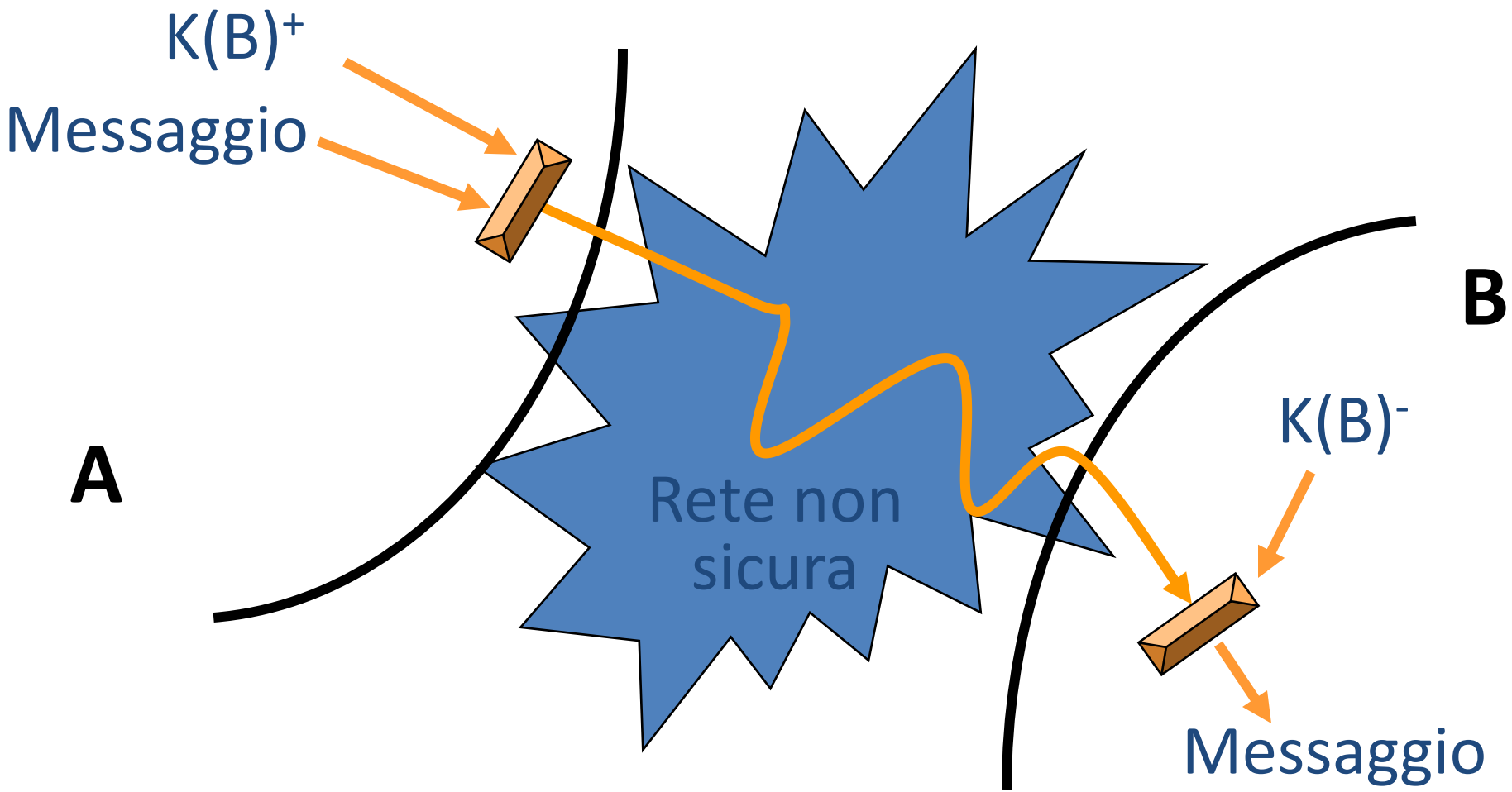


Cifratura asimmetrica



Cifratura asimmetrica


Informazioni pubbliche
Messaggio
Rete non sicura
Informazioni segrete
Messaggio
Cifratura (encryption)
Decifratura (decryption)



Cifratura asimmetrica

Termini equivalenti

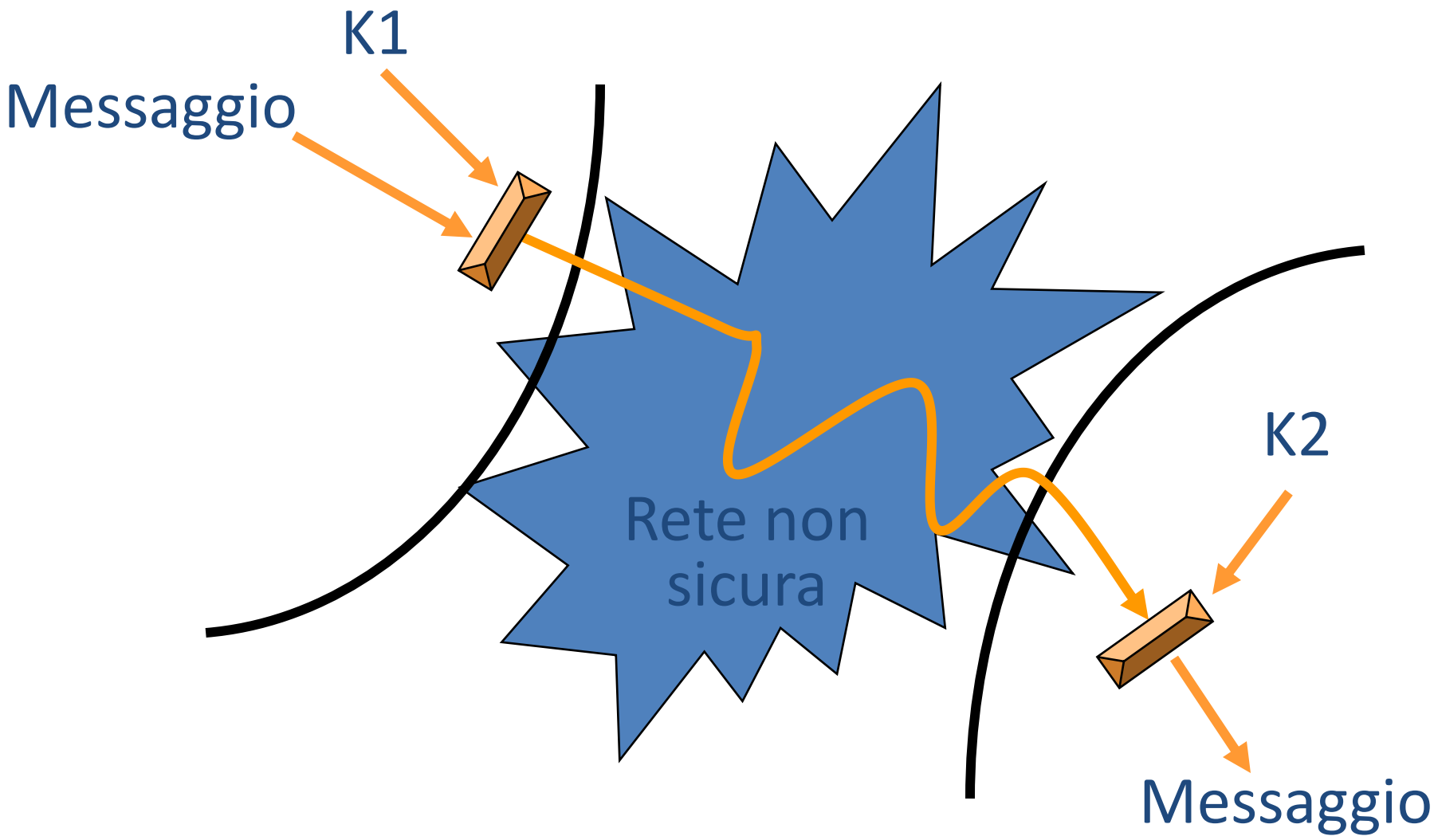
Cifrari asimmetrici

=

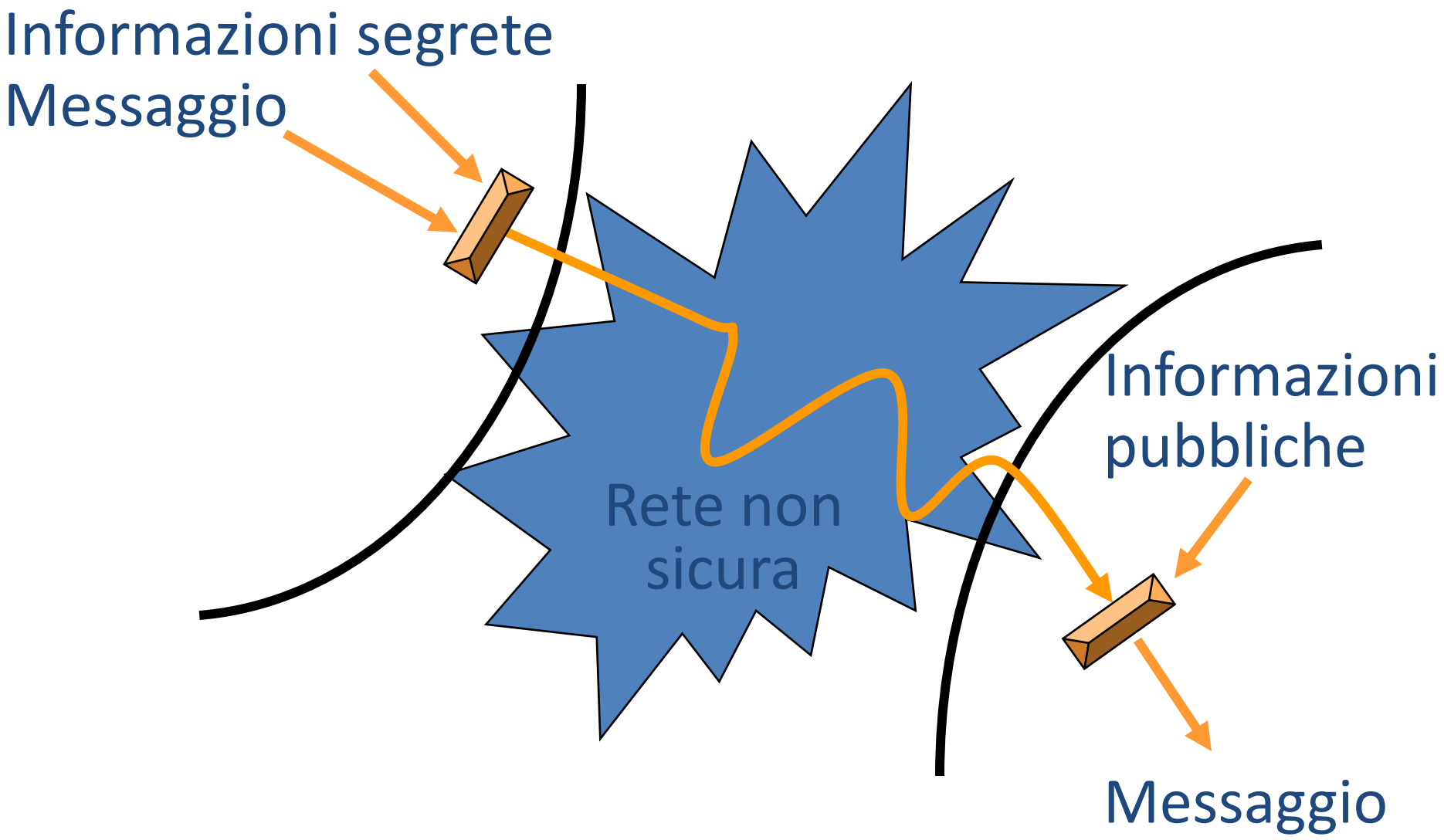
Cifrari a chiave pubblica

- **Perché diventa possibile cifrare un messaggio senza condividere un segreto con il destinatario → maggiore facilità nella distribuzione delle chiavi**

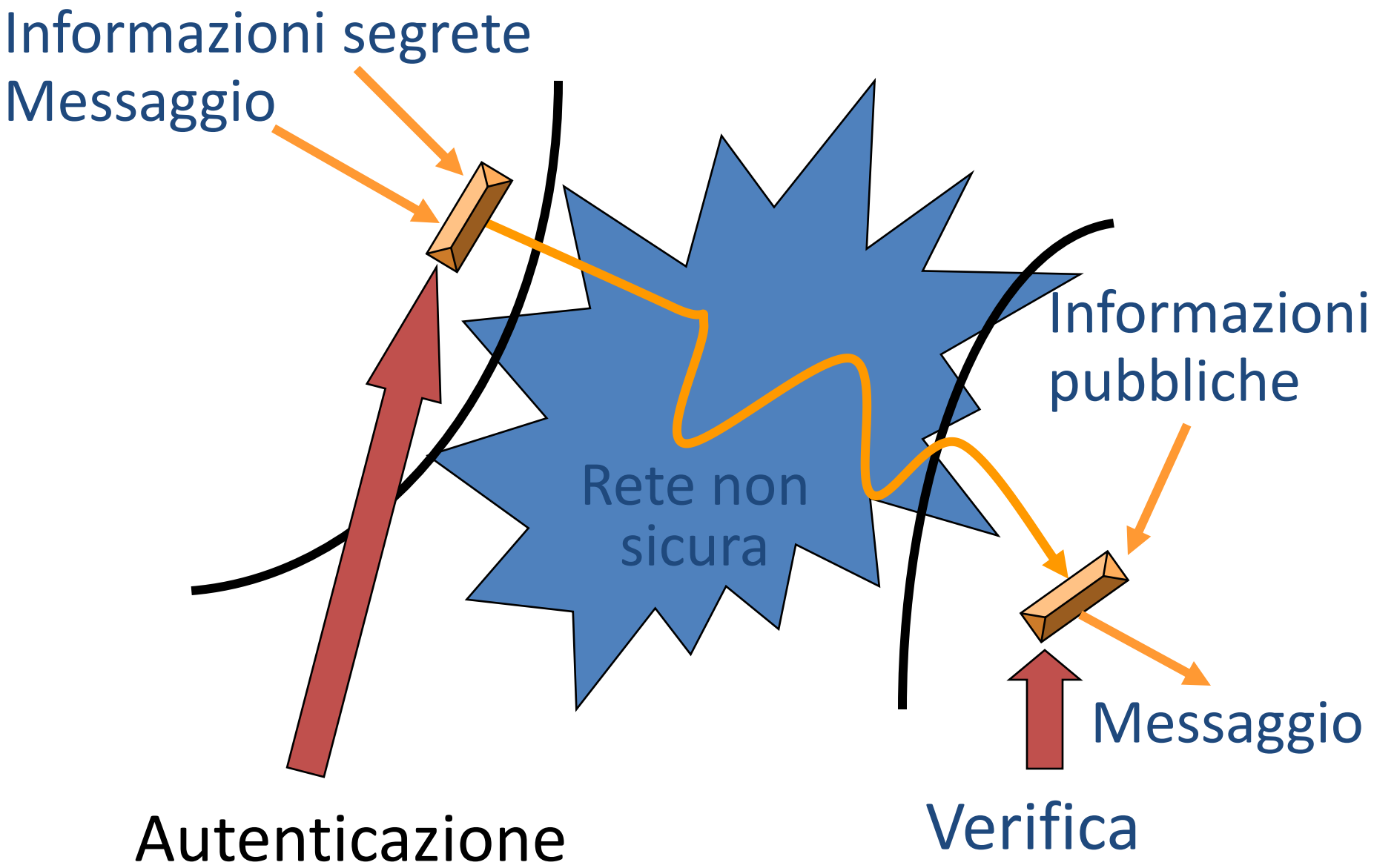
- **Perché solo chi detiene la chiave di cifratura è in grado di produrre un dato messaggio cifrato → possibilità di effettuare operazioni non disconoscibili (non repudiation)**

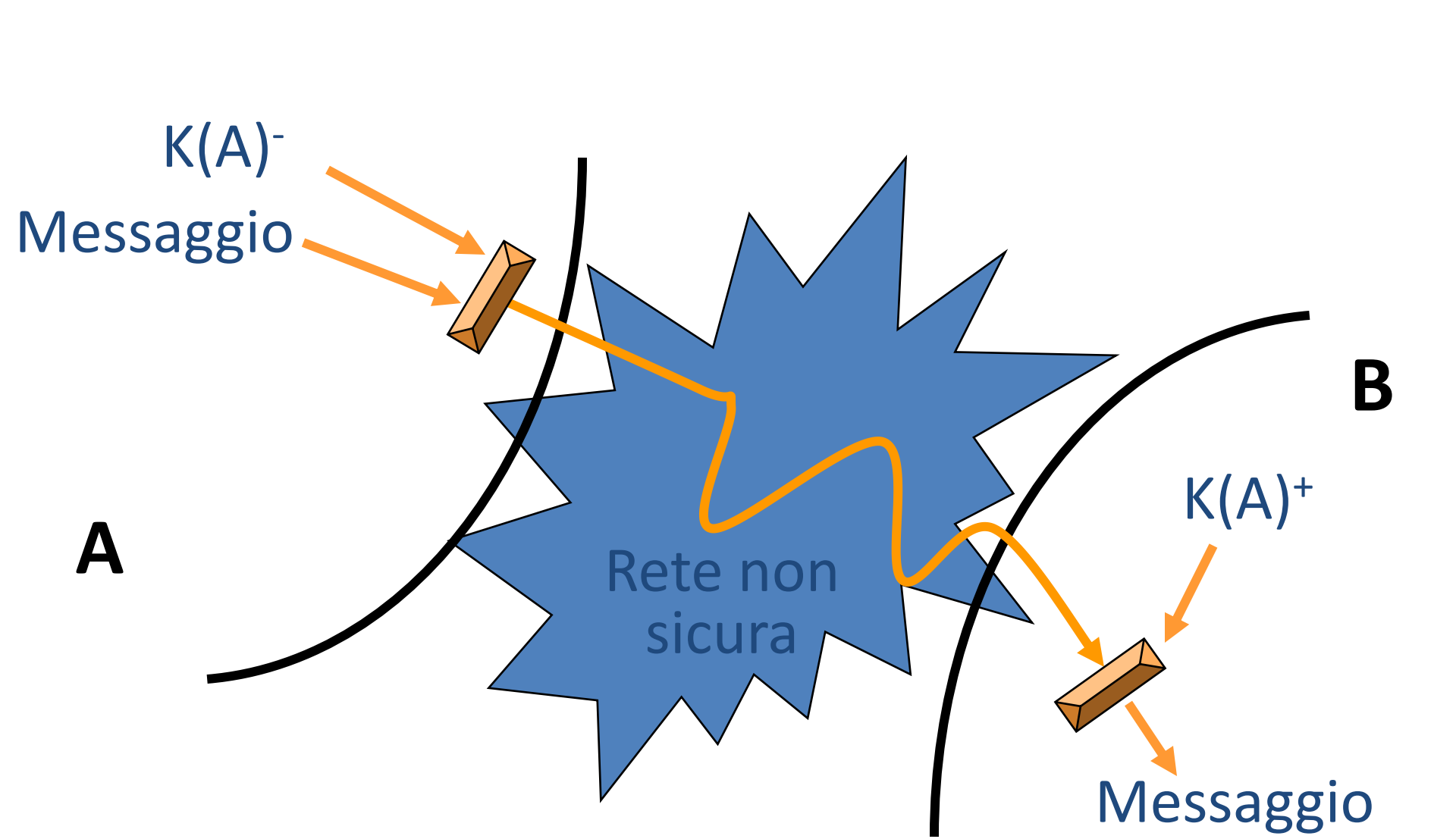


Semplice forma di autenticazione



Semplice forma di autenticazione


Informazioni segrete
Messaggio
Rete non sicura
Informazioni pubbliche
Messaggio
Autenticazione
Verifica



Semplice forma di autenticazione

Cifrari asimmetrici

- Questa semplice forma di autenticazione asimmetrica non garantisce in generale l'effettiva provenienza del messaggio dal mittente dichiarato
- Una tecnica più complessa, ma basata sugli stessi principi, porta invece ad un forma di autenticazione sicura e non disconoscibile (firma elettronica)

Caratteristiche dei cifrari asimmetrici

- Mittente e ricevente non condividono chiavi
- Per cifrare e decifrare si usano chiavi diverse
- Cifratura e decifratura sono relativamente inefficienti
- E’ difficile o praticamente impossibile decifrare senza conoscere la chiave, perché questo richiede eccessive risorse computazionali

Esistono cifrari asimmetrici sicuri e utilizzabili in pratica?

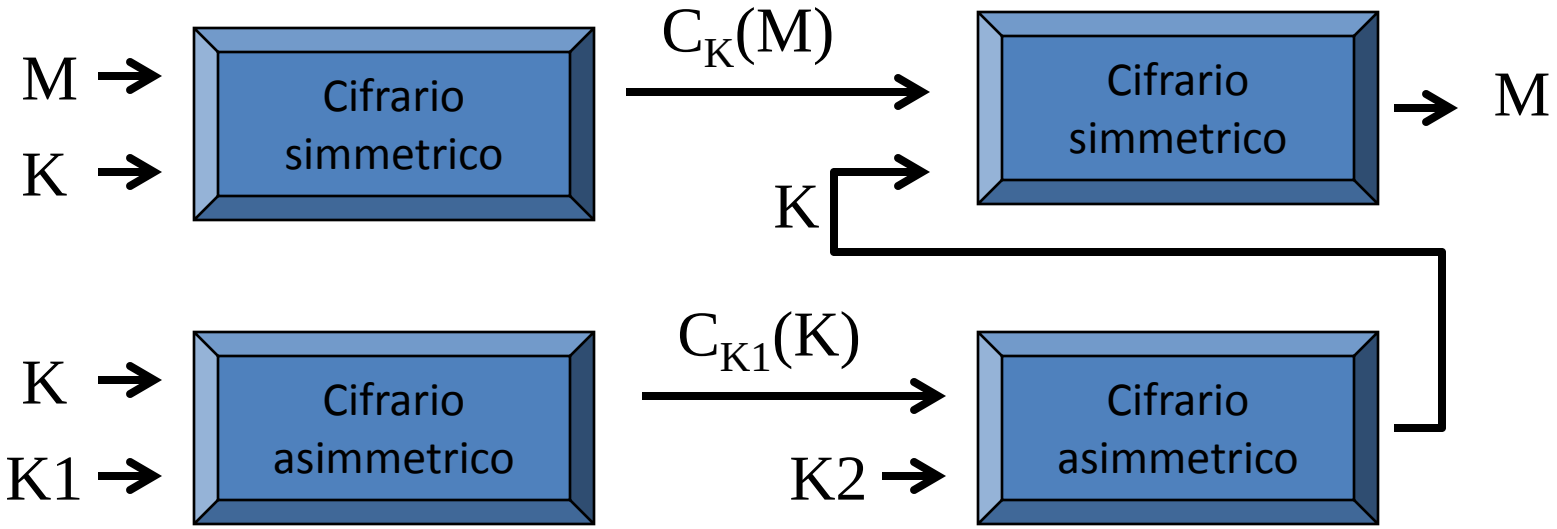
Si ritiene che vari cifrari a chiave pubbica presentati nella letteratura siano sicuri anche rispetto ad attacchi molto sofisticati. Il cifrario più utilizzato e conosciuto è RSA.

I cifrari asimmetrici conosciuti sono tutti abbastanza lenti e devono essere combinati con cifrari simmetrici e con funzioni di hash

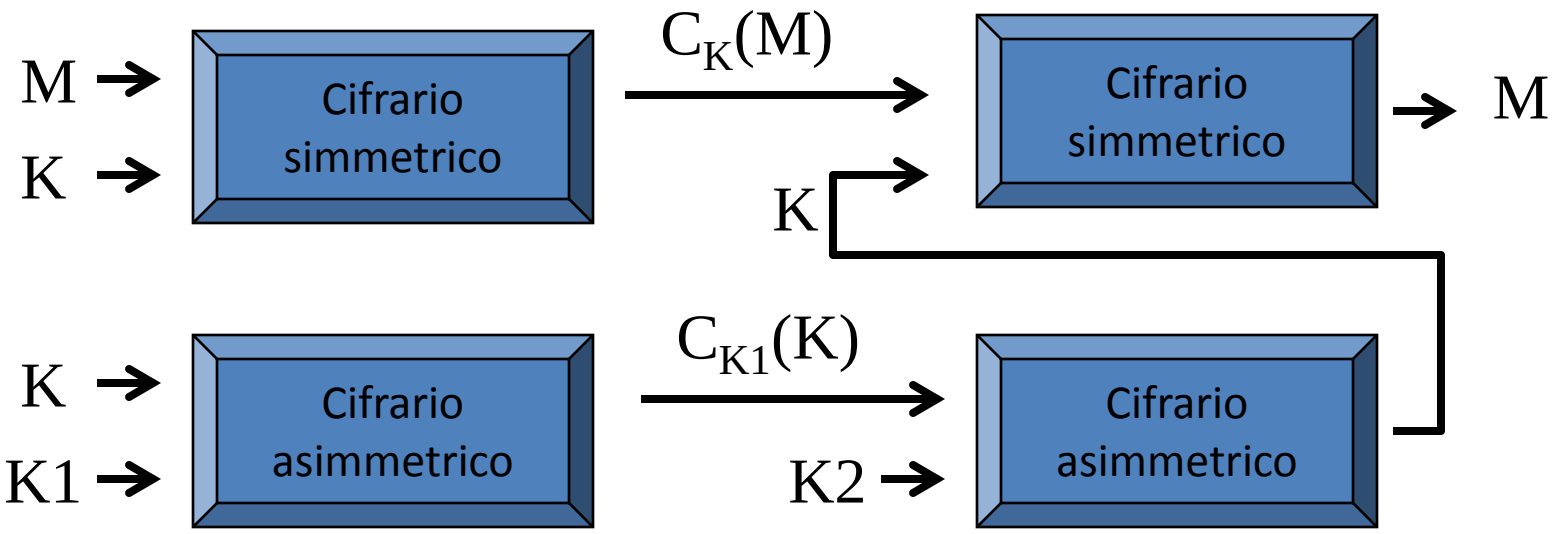
Combinazione di cifrari simmetrici e asimmetrici

Per inviare un messaggio cifrato si prepara un ‘digital envelope’ che consiste nel messaggio cifrato con una chiave simmetrica K, e nella chiave K stessa cifrata mediante un cifrario asimmetrico

Combinazione di cifrari simmetrici e asimmetrici



Digital envelope = < $C_K(M)$, $C_{K1}(K)$>



I protocolli effettivamente usati sono più complessi in modo da identificare il mittente e per evitare forme di attacco (replay) basate sul riutilizzo della chiave K in momenti diversi.