Cenni di Sicurezza di Rete

Reti di Calcolatori

Federica Paganelli

Obiettivi

Riservatezza/segretezza

Solo mittente e destinatario dovrebbero avere disponibili ed essere in grado di comprendere il contenuto del messaggio trasmesso

Integrità

Il contenuto della comunicazione non deve subire alterazioni durante la trasmissione

Disponibilità/Accessibilità

Deve essere garantita disponibilità/operatività di informazioni e servizi

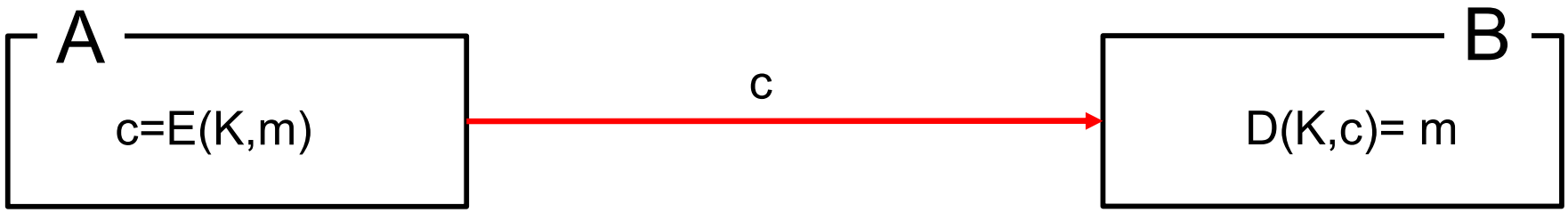
Obiettivi		**Attacchi**
Riservatezza/segretezza	←	Intercettazione intrusione
Integrità	←	spoofing play-back repudiation
Accessibilità	←	DoS DDoS

Sicurezza

- Concetti generali
- Cifratura
  - Cifratura a chiave simmetrica
  - Cifratura a chiave asimmetrica
- Integrità del messaggio, autenticazione
  - Message digest
  - MAC
  - Firma digitale
- Sicurezza a livello rete: IPSec

Cifratura a chiave simmetrica

Idea: stessa chiave (segreta) usata per cifrare e decifrare



m = testo in chiaro
K= chiave condivisa

la chiave può essere utilizzata per la comunicazione bidirezionale.

Cifratura a chiave simmetrica

Cifratura a chiave simmetrica

- Cifrari *monoalfabetici*
  - un carattere(simbolo) nel testo viene sostituito con un altro simbolo
  - *Es. Cifratura di Cesare (k-shift)*
- Cifrari *polialfabetici*

- Cifrari a blocchi:
  - Blocchi di *n* bit cifrati usando chiavi di *k* bit
  - DES: Data Encryption Standard
    - Cifrario a blocchi
    - Chiave di cifratura 56 bit
  - AES: Advanced Encryption Standard
    - 2001 standard, sostituisce DES,
    - Elabora dati in blocchi di 128 bit, chiave di 128, 192, o 256 bit

Cifratura a chiave simmetrica

Problemi

- Come si accordano A e B su chiave da usare?

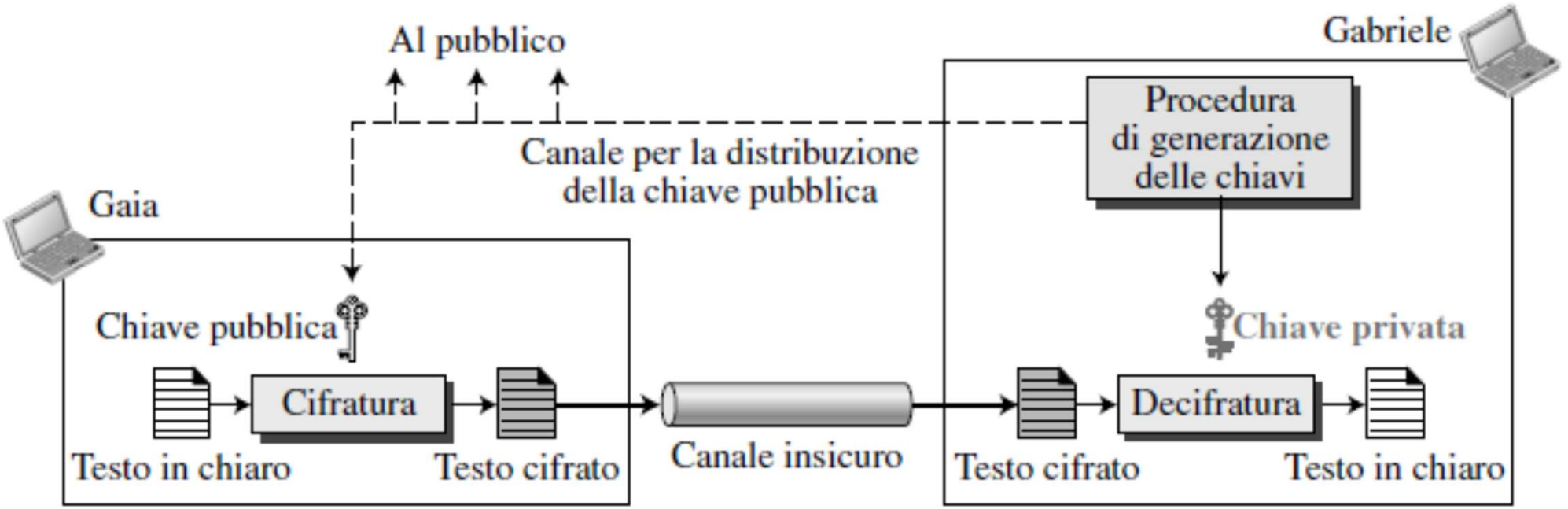
  (soprattutto se non si incontrano mai?)
- Segretezza chiave inversamente proporzionale a quanto viene usata

Cifratura a chiave asimmetrica

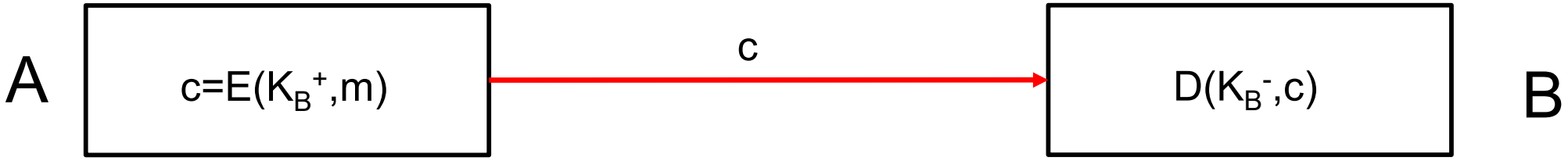
Idea: nessuna chiave segreta condivisa!

Ognuno possiede

- una sua chiave *pubblica* nota a tutti
- una sua chiave *privata* segreta, nota solo a lui



Cifratura a chiave asimmetrica



Cifratura e decifratura: funzioni matematiche su numeri che rappresentano il testo in chiaro e cifrato

K_B^+ chiave pubblica
K_B^- chiave privata

Requisiti

- K_B^+ e K_B^- tali che: $D(K_B^-,E(K_B^+,m)) = m$
- Non deve essere possibile determinare K_B^- a partire da K_B^+

N.B.: $D(K_B^-,E(K_B^+,m)) = D(K_B^+,E(K_B^-,m))$

Problema: efficienza

Esempio: RSA

Esempio: usare la crittografia asimmetrica per inviare chiavi di sessione (simmetriche)

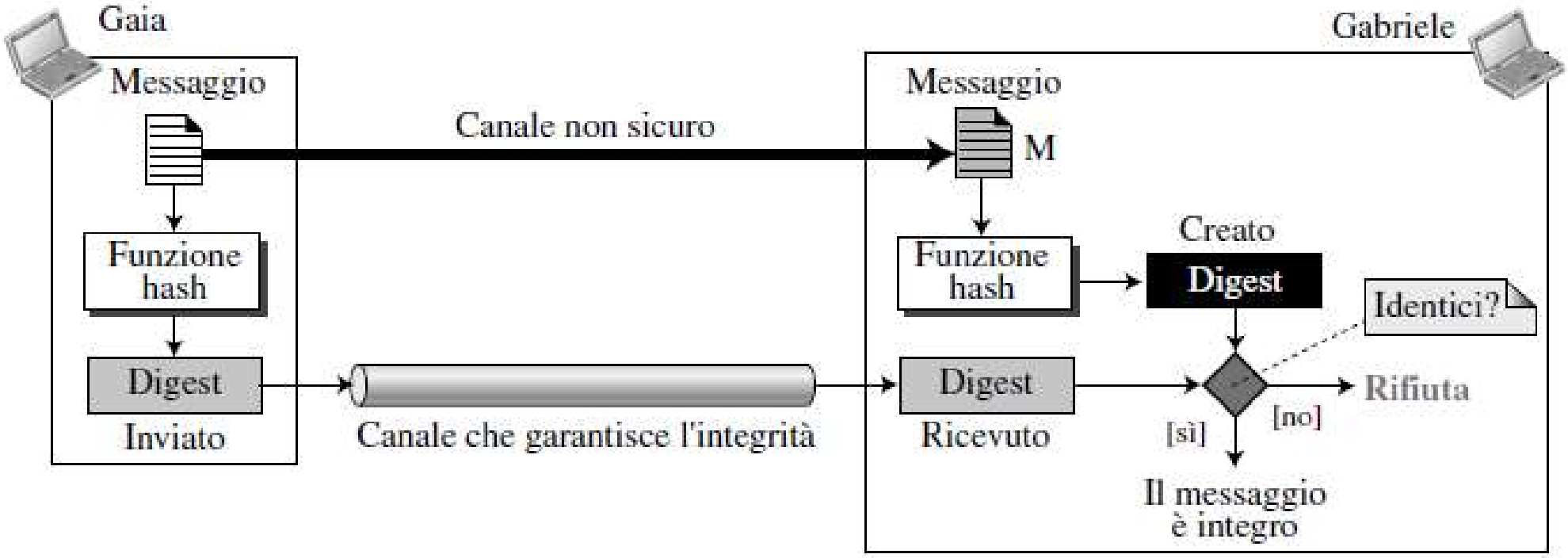
Message digest

- Vi sono casi in cui pur non essendo richiesta la riservatezza, risulta di fondamentale importanza l'integrità: il messaggio originale non deve poter essere modificato.

- Gaia potrebbe per esempio scrivere un documento che non necessita di segretezza (dunque non deve essere cifrato), ma che deve rimanere integro, ovvero il suo contenuto non può essere modificato.

- Funzione hash: Riceve un messaggio di lunghezza arbitraria e produce un digest di lunghezza fissa
  - Esempi MD4 MD5 SHA

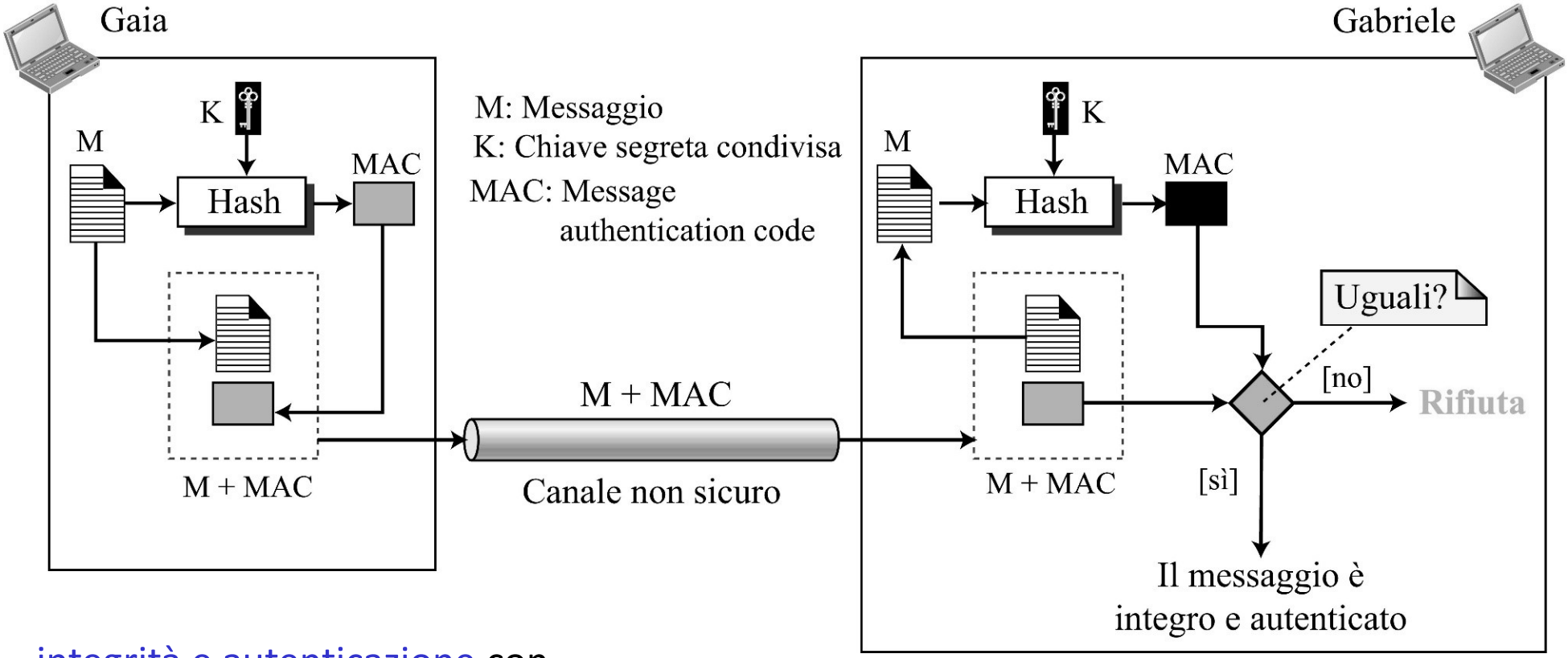
Figura 9.16: Messaggio e relativo digest



Il digest può essere usato per verificare l'integrità di un messaggio

Problema: autenticazione del messaggio

Message Authentication Code (MAC)



integrità e autenticazione con funzione hash e chiave segreta

Gaia e Gabriele condividono la chiave segreta K

Mittente

1. MAC prodotto dalla funzione hash H(M+K)
2. Invia M e MAC su canale non sicuro

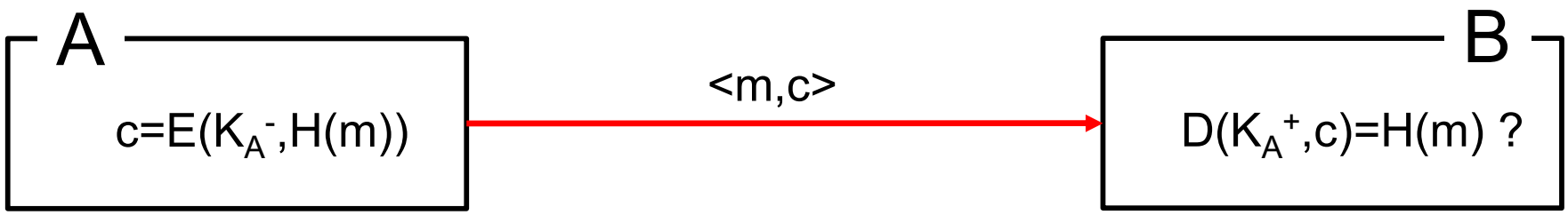
Destinatario

1. Ricalcola H(M+K)
2. Confronta MAC calcolato e ricevuto

Problema: ripudiabilità

Firma digitale

Idea: utilizzare chiave privata per firmare *digest*



A cifra hash di m con la sua chiave privata

Problema: ...ripudiabilità
(A potrebbe cambiare chiavi)

B usa la chiave pubblica di A e verifica se il risultato è uguale all'hash del messaggio ricevuto

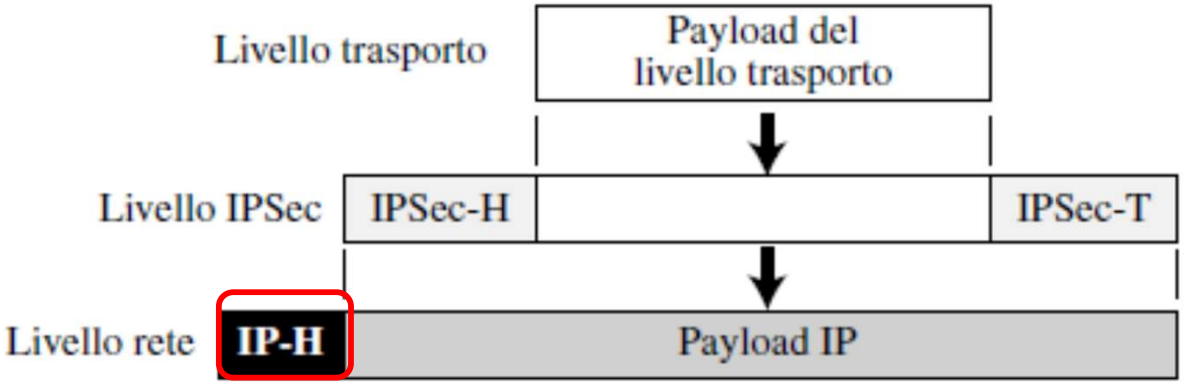
Utilizzo di terze parti fidate come intermediari della comunicazione

IPSec

- Insieme di protocolli per fornire sicurezza a livello rete
- Autenticazione e confidenzialità dei pacchetti IP
  - Modalità trasporto
  - Modalità tunnel

IPsec

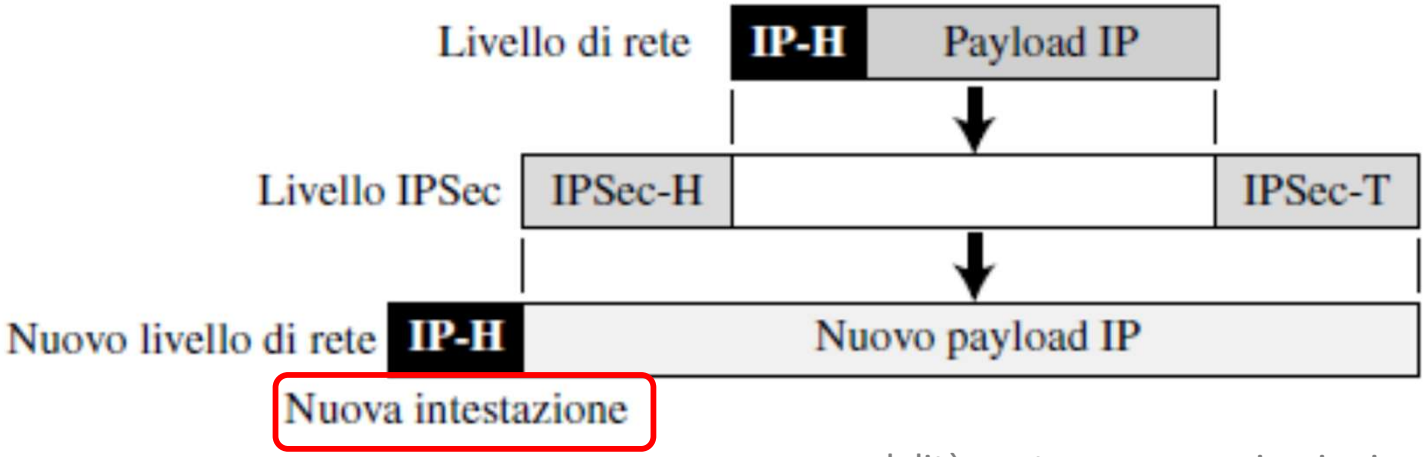
Modalità ***trasporto***: protegge dati passati da liv. trasporto a liv. rete



intestazione IP non protetta

modalità usata per comunicazioni end-to-end

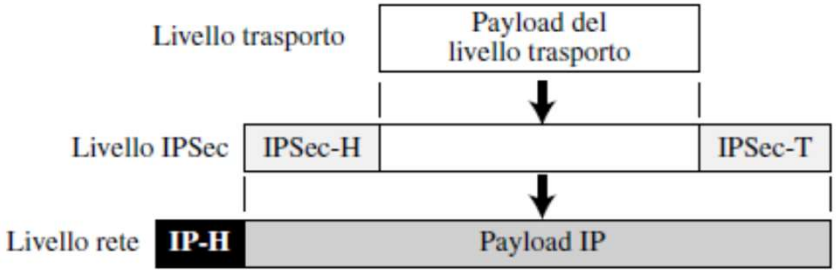
Modalità ***tunnel***: protegge l'intero pacchetto IP

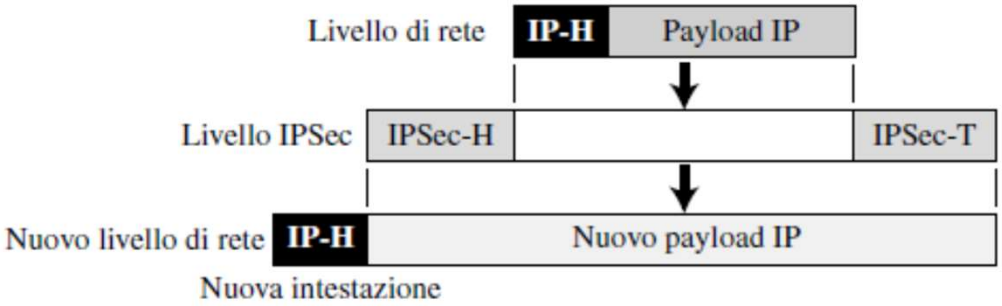


intero datagram protetto

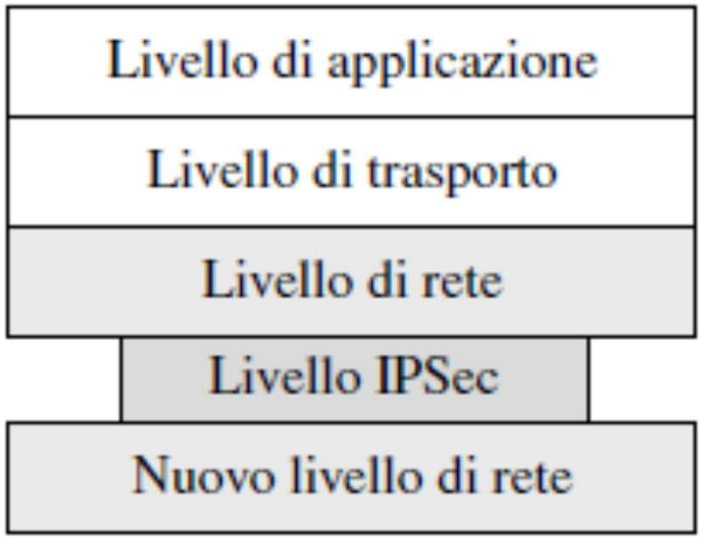
modalità usata per comunicazioni router-to-router o host-router

IPsec





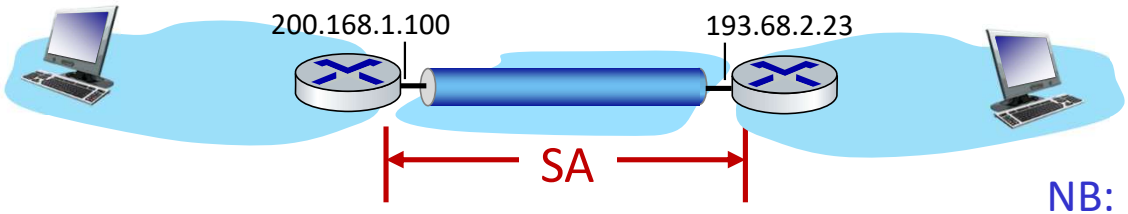
Modalità di trasporto



Modalità tunnel

Security associations (SAs)

- Prima dell'invio dei dati, una Security Association (SA) viene stabilita tra l'entità di invio a quella di ricezione (uni-direzionale)
- Ogni volta che il router R1 deve costruire un datagramma IPsec da inoltrare su questa SA, accede alle informazioni di stato della SA per determinare come autenticare e decifrare il datagramma.
- Il router R2 conserverà le stesse informazioni di stato per questa SA e le utilizzerà per autenticare e decrittografare qualsiasi datagramma IPsec in arrivo dal router R1



SA:

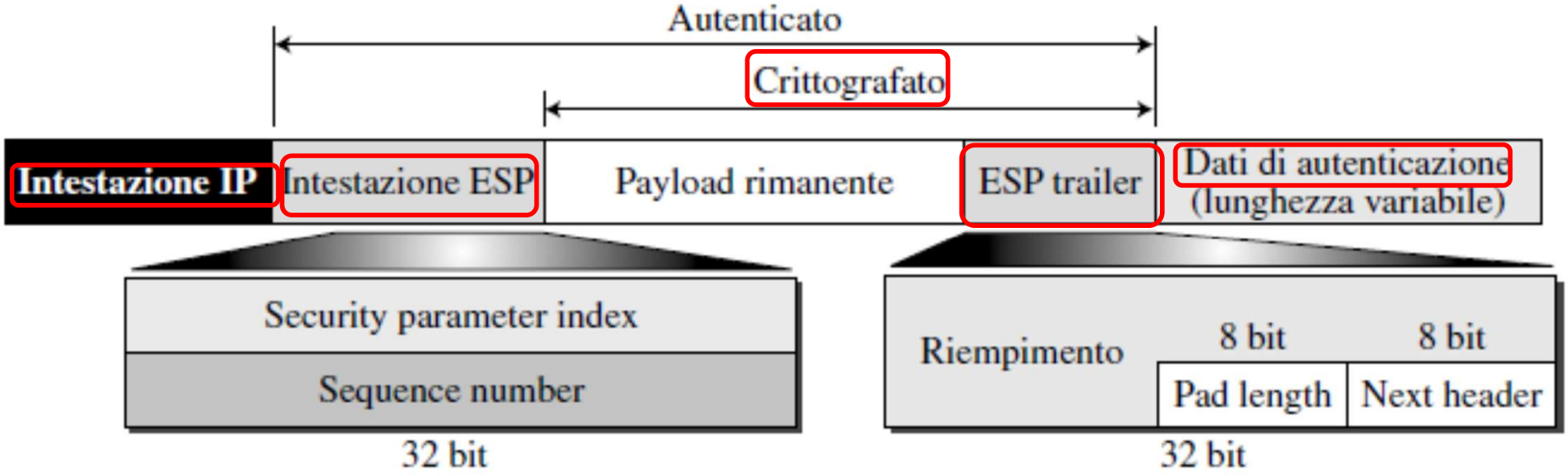
- 32-bit identifier: *Security Parameter Index (SPI)*
- origin SA interface (200.168.1.100)
- destination SA interface (193.68.2.23)
- type of encryption used
- encryption key
- type of integrity check used
- authentication key

NB: IP è senza connessione;
IPsec è orientato alla connessione!

IPsec: protocollo ESP (Encapsulating Security Payload)

Obiettivi: Autenticazione sorgente, Integrità, Riservatezza

1. Viene aggiunto trailer ESP
2. Payload e trailer ESP vengono crittografati
3. Viene aggiunta intestazione ESP
4. Intestazione ESP, payload e trailer ESP vengono usati per generare dati autenticazione (che vengono aggiunti dopo trailer ESP)
5. Viene aggiunta intestazione IP (impostando campo protocollo a 50)



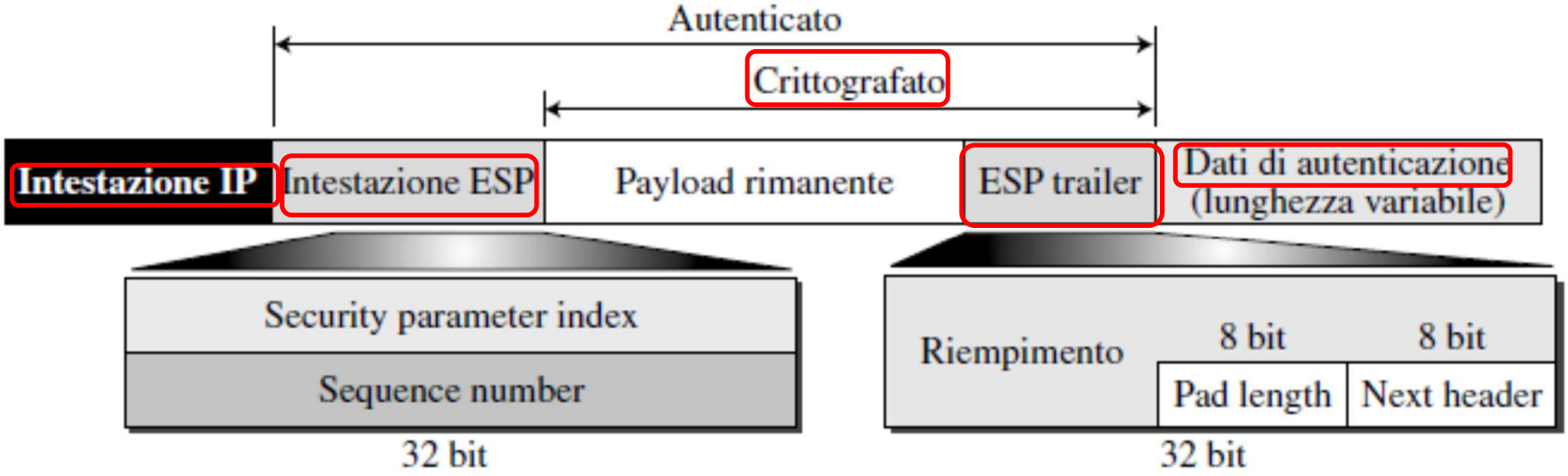
IPsec: protocollo ESP (Encapsulating Security Payload)

ESP Trailer

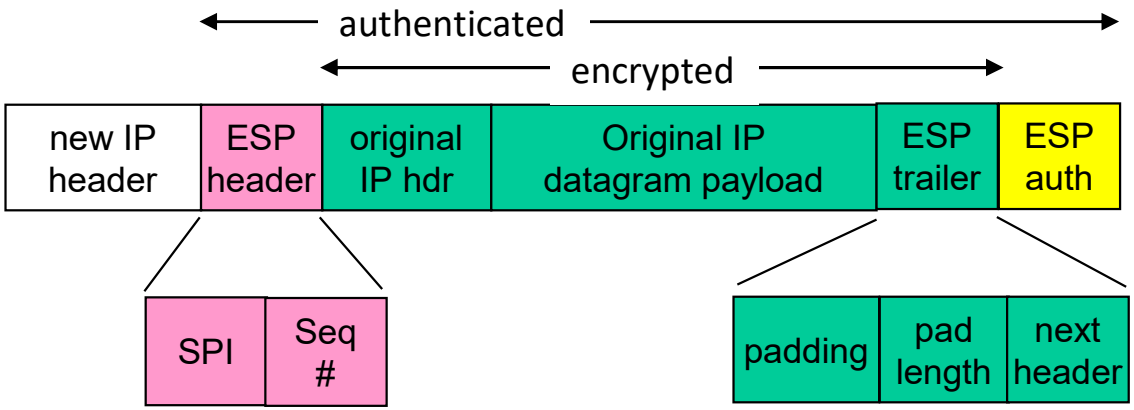
- Padding: valori 0 di riempimento
- Pad length: quanti byte aggiuntivi di padding sono stati inseriti
- Next header: tipo di payload contenuto nel datagramma IP (es. TCP,UDP, ICMP o OSPF)

Intestazione ESP:

- SPI: identificatore della SA
- Sequence number: per prevenire gli attacchi a ripetizione di pacchetto



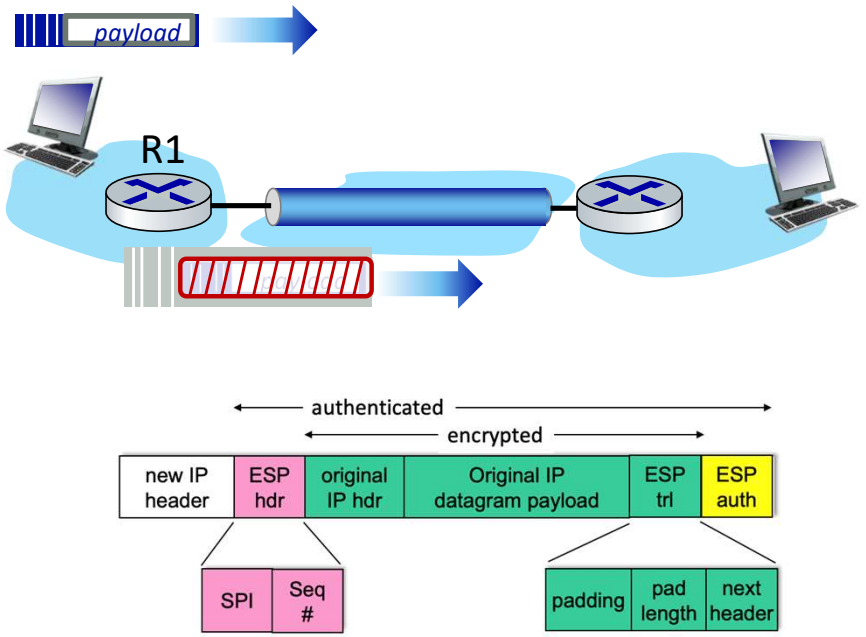
IPsec datagram



tunnel mode ESP

ESP tunnel mode: actions

- R1:
  - aggiunge il trailer ESP al datagramma originale (che include i campi dell'intestazione originale)
  - cripta il risultato utilizzando l'algoritmo e la chiave specificati da SA
  - aggiunge l'intestazione ESP alla parte anteriore di questa quantità criptata
  - crea il MAC di autenticazione utilizzando l'algoritmo e la chiave specificati nella SA
  - aggiunge il MAC al payload
  - crea una nuova intestazione IP, nuovi campi dell'intestazione IP, indirizzi verso l'endpoint del tunnel



Virtual Private Network

- Applicazione di IPSec
  - Rete privata sulla Internet pubblica