Programmazione in Rete

a.a. 2005/2006

http://www.di.uniba.it/~lisi/courses/prog-rete/prog-rete0506.htm

dott.ssa Francesca A. Lisi
lisi@di.uniba.it

Orario di ricevimento: mercoledì ore 10-12

dib

Sommario della lezione di oggi: La sicurezza nelle reti (3/3)

Dai fondamenti ...

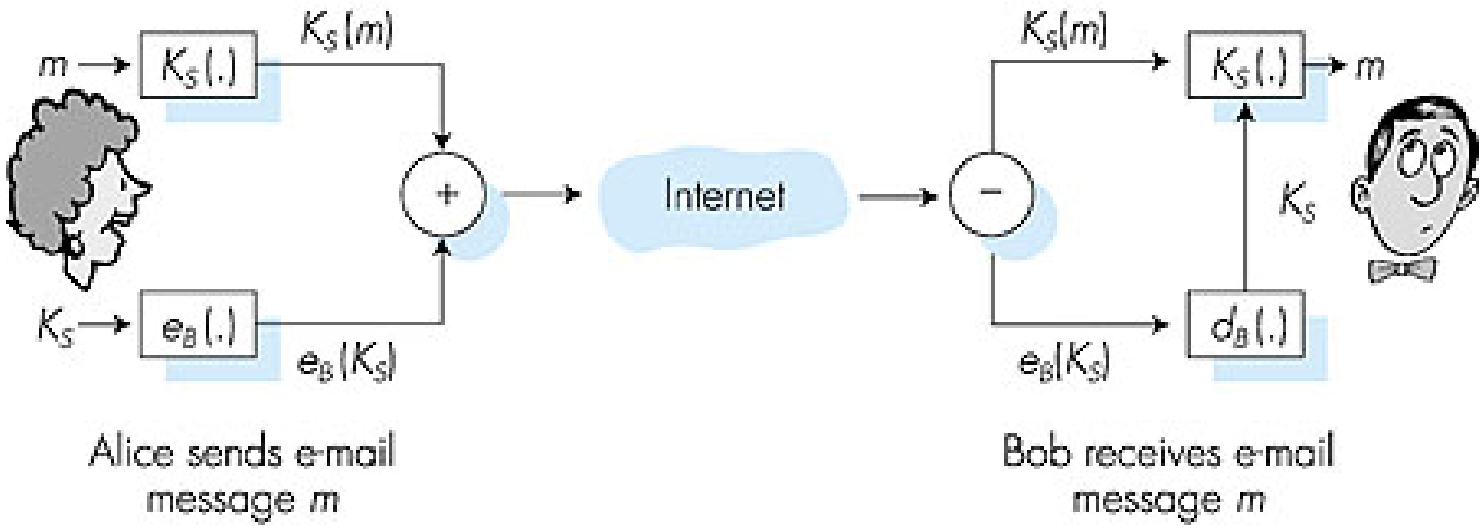
- che cosa è la sicurezza?
- crittografia
- autenticazione
- integrità e non ripudiabilità del messaggio
- distribuzione delle chiavi e certificazione

... in pratica

- a livello di applicazione: e-mail sicura
- a livello di trasporto: commercio Internet, SSL, SET
- a livello di rete: sicurezza IP

Sicurezza a livello di applicazione: posta elettronica sicura

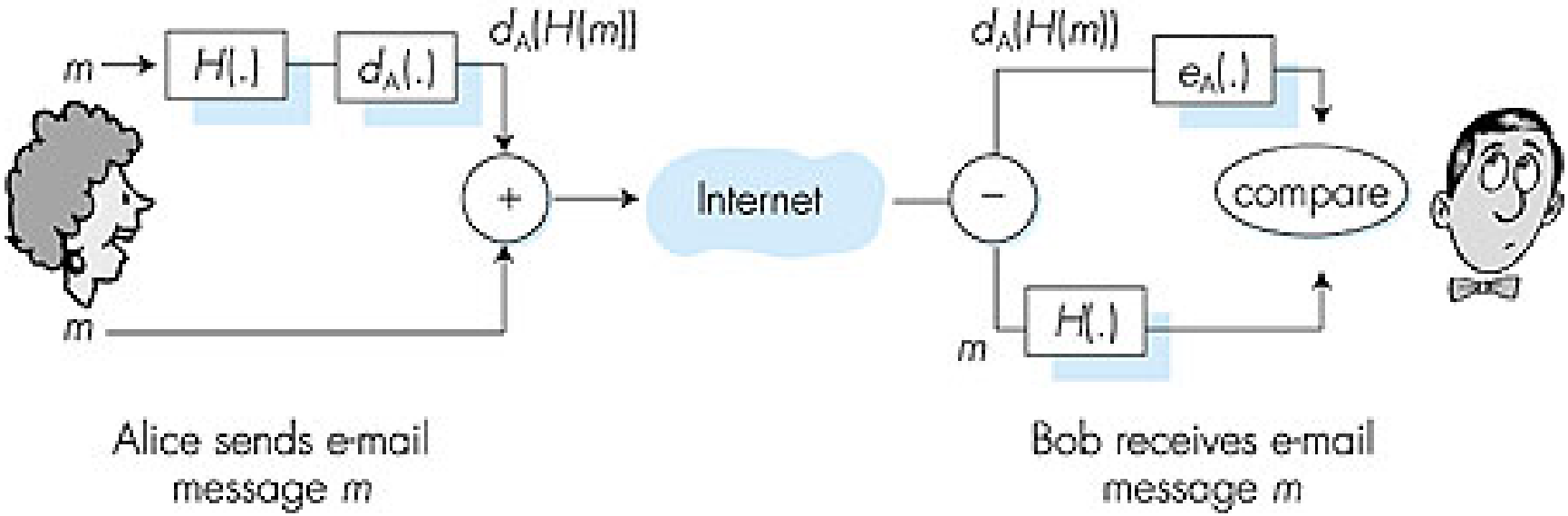
Alice vuole inviare un messaggio e-mail segreto, m, a Bob.



- genera una chiave simmetrica random, K_S.
- codifica il messaggio con K_S
- codifica anche K_S con la chiave pubblica di Bob
- invia sia $K_S(m)$ sia $e_B(K_S)$ a Bob.

Sicurezza a livello di applicazione: posta elettronica sicura (cont.)

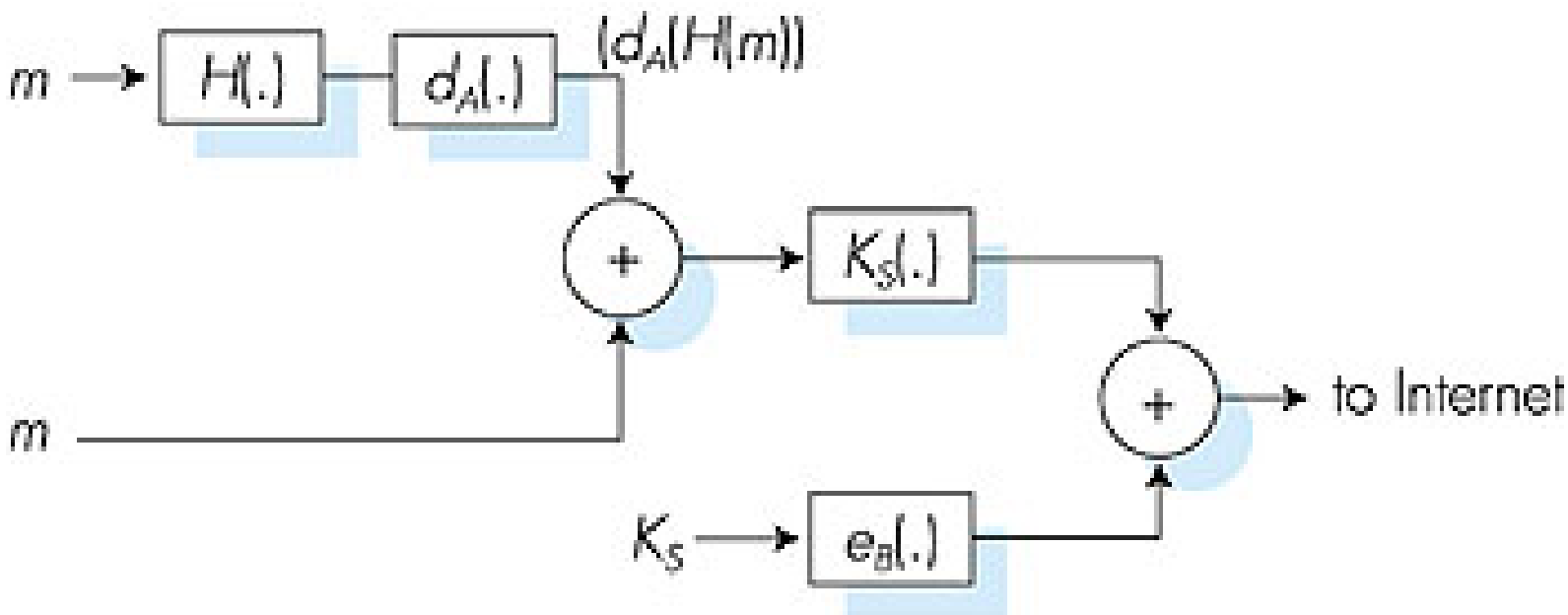
Alice vuole fornire autenticazione del mittente ed integrità del messaggio.



- Alice appone firma digitale al messaggio
- invia sia il messaggio (in chiaro) e firma digitale

Sicurezza a livello di applicazione: posta elettronica sicura (cont.)

Alice vuole fornire segretezza, autenticazione del mittente, ed integrità del messaggio.



Nota: Alice usa sia la propria chiave privata sia la chiave pubblica di Bob.

Sicurezza a livello di applicazione: pretty good privacy (PGP)

- Schema di cifratura della posta elettronica su Internet, uno standard de facto.
- Usa crittografia a chiave simmetrica, crittografia a chiave pubblica, funzione hash, e firma digitale come descritto.
- Fornisce segretezza, autenticazione del mittente, integrità.
- Inventore: Phil Zimmerman, soggetto ad investigazione federale per tre anni.

Un messaggio firmato PGP:

```
---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1

Bob:My husband is out of town
   tonight.Passionately yours,
   Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3mqJ
   hFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

Sicurezza a livello di trasporto: secure sockets layer (SSL)

- SSL fornisce sicurezza a qualsiasi applicazione TCP-based che usa i servizi SSL
  - https viene usato fra browser WWW e server per E-commerce.
- Servizi SSL:
  - autenticazione del server
  - criptaggio dati
  - autenticazione del client (opzionale)
- Autenticazione del server:
  - browser SSL-enabled include chiavi pubbliche per CA di fiducia.
  - Browser richiede al server il certificato, rilasciato da CA di fiducia.
  - Browser usa chiave pubblica di CA per estrarre la chiave pubblica del server dal certificato.
- Visita il menu di sicurezza del tuo browser per vedere i suoi CA di fiducia.

Sicurezza a livello di trasporto: SSL (cont.)

Sessione SSL criptata:

- Browser genera una chiave simmetrica di sessione, la cripta con la chiave pubblica del server, invia la chiave criptata al server.
- Usando la sua chiave privata, il server decifra la chiave di sessione.
- Browser e server concordano che tutti i dati inviati nel socket TCP sono criptati con chiave di sessione.
- SSL: alla base di IETF Transport Layer Security (TLS).
- SSL può essere usato per applicazioni non-Web, p.e. IMAP.
- Autenticazione del client può essere fatta con i certificati del client.

Sicurezza a livello di trasporto: Secure electronic transactions (SET)

- Progettato per transazioni di carta di pagamento su Internet.
- Fornisce sicurezza fra 3 entità in gioco, tutti muniti di certificati:
  - cliente
  - venditore
  - banca del venditore
- SET specifica significati legali dei certificati.
  - Distribuzione di responsabilità per le transazioni
- Numero di carta del cliente viene passato alla banca del venditore senza che quest'ultimo veda mai il numero in chiaro.
  - Previene i venditori dal rubare o far trapelare i numeri di carta di pagamento.
- Tre componenti sw:
  - il portafogli del browser
  - il server del venditore
  - il gateway dell'acquirente

Sicurezza a livello di rete: IPsec

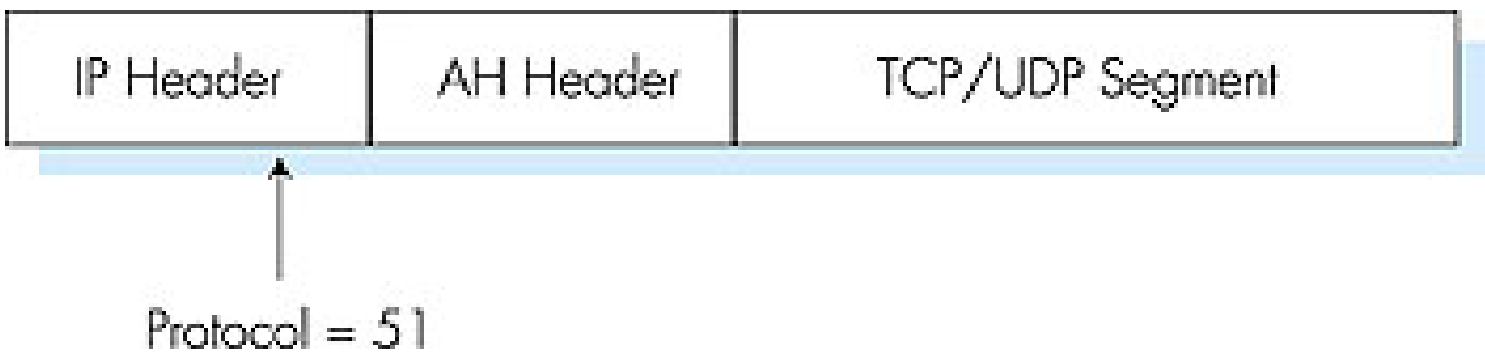
- Segretezza:
  - host mittente cripta i dati in IP datagram
  - segmenti TCP e UDP; messaggi ICMP e SNMP.
- Autenticazione
  - host destinatario può autenticare indirizzo IP del sorgente
- Due protocolli principali:
  - Authentication Header (AH) protocol
  - Encapsulation Security Payload (ESP) protocol
- Per entrambi AH e ESP, handshake fra sorgente e destinazione:
  - crea canale logico a livello di rete detto *Security Association* (SA)
- Ogni SA è unidirezionale.
- Unicamente determinato da:
  - protocollo di sicurezza (AH o ESP)
  - indirizzo IP del sorgente
  - ID di connessione a 32 bit

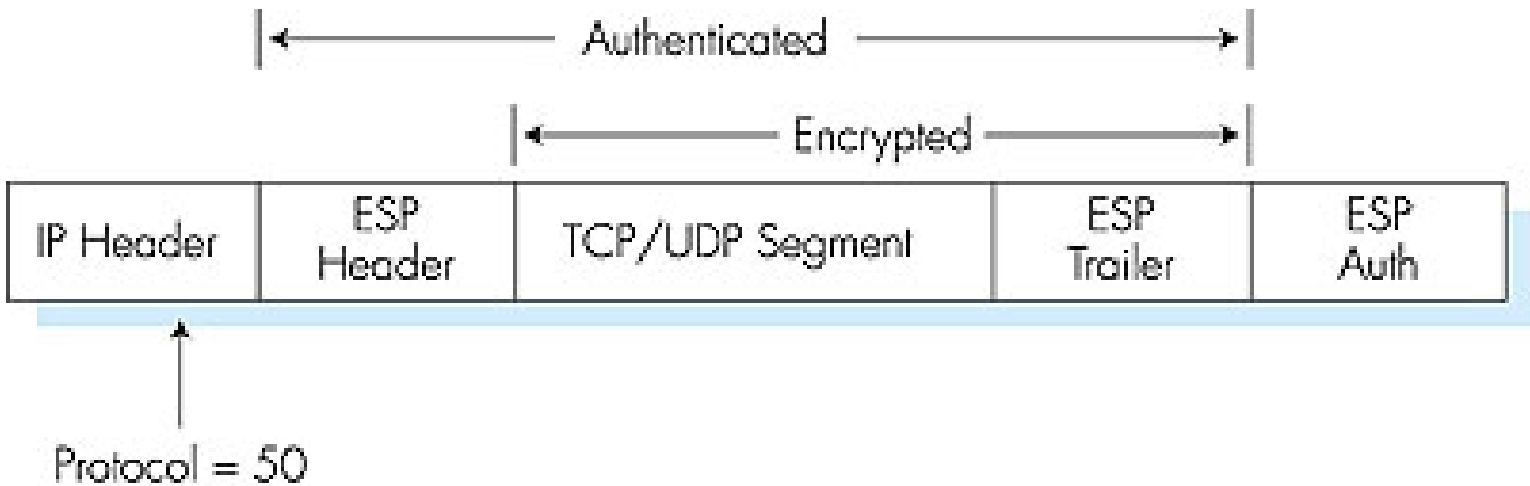
Sicurezza a livello di rete: Protocollo AH

- Fornisce autenticazione host, integrità dati, ma non segretezza.
- Header AH inserita fra header IP e campo dati IP.
- Protocollo = 51.
- I router intermedi processano i datagram come solito.

Header AH include:

- identificatore di connessione
- dati di autenticazione: digest di msg firmato, calcolato su datagram IP originale, fornendo autenticazione di sorgente, integrità dati.
- Campo *header successivo* specifica tipo di dati (TCP, UDP, ICMP, etc.)



Sicurezza a livello di rete: Protocollo ESP

- Fornisce segretezza, autenticazione host, integrità dei dati.
- Dati e ESP trailer entrambi criptati.
- Il campo *header successivo* è in ESP trailer.
- Campo di autenticazione ESP è simile al campo di autenticazione AH.
- Protocollo = 50.