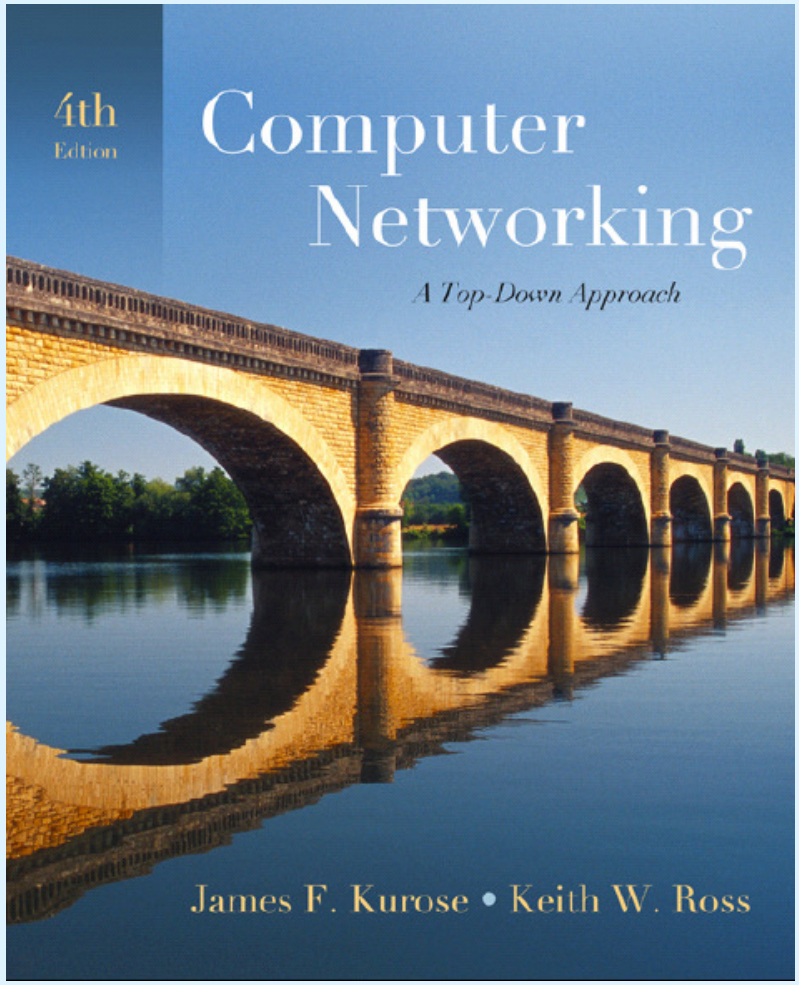
Security in Computer Networks

Network Management

Bildspelet omfattar till stor del bilder som hör till följande bok:



A note on the use of these ppt slides:

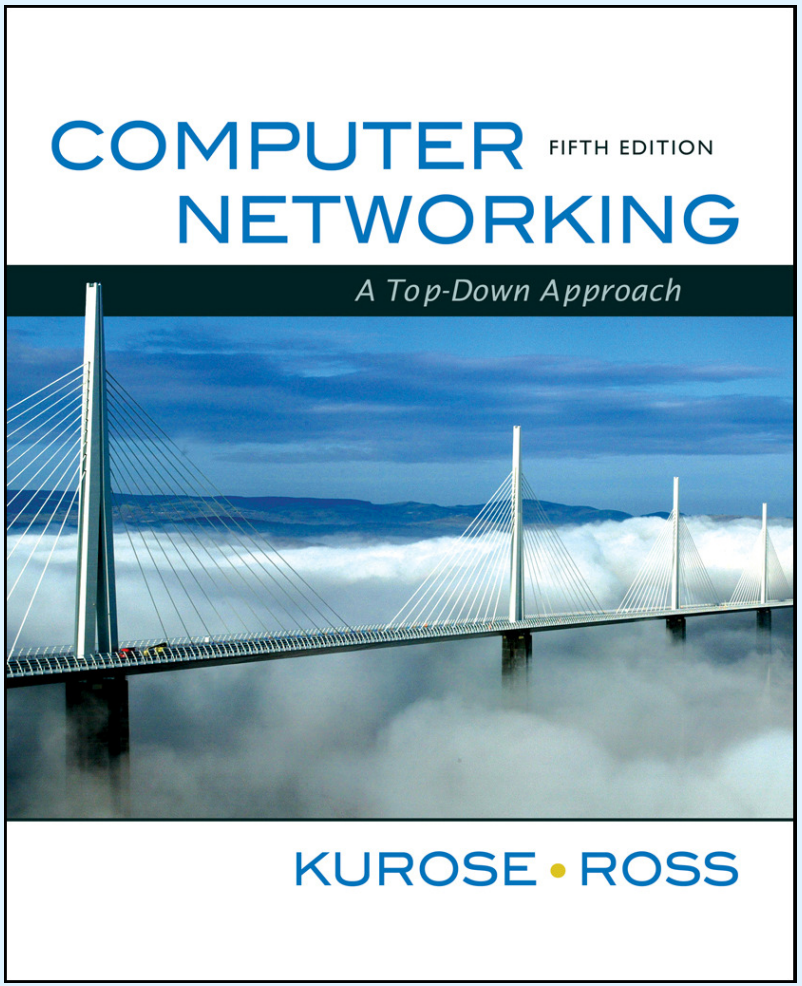
We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) in substantially unaltered form, that you mention their source (after all, we'd like people to use our book!)
- If you post any slides in substantially unaltered form on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

Computer Networking: A Top Down Approach , 4th edition.
Jim Kurose, Keith Ross, Addison-Wesley, July 2007.

Dessutom tre bilder från följande bok:



A note on the use of these ppt slides:

We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) in substantially unaltered form, that you mention their source (after all, we'd like people to use our book!)
- If you post any slides in substantially unaltered form on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

Computer Networking: A Top Down Approach , 5th edition.
Jim Kurose, Keith Ross, Addison-Wesley, April 2009.

What is network security?

Confidentiality: only sender, intended receiver should "understand" message contents

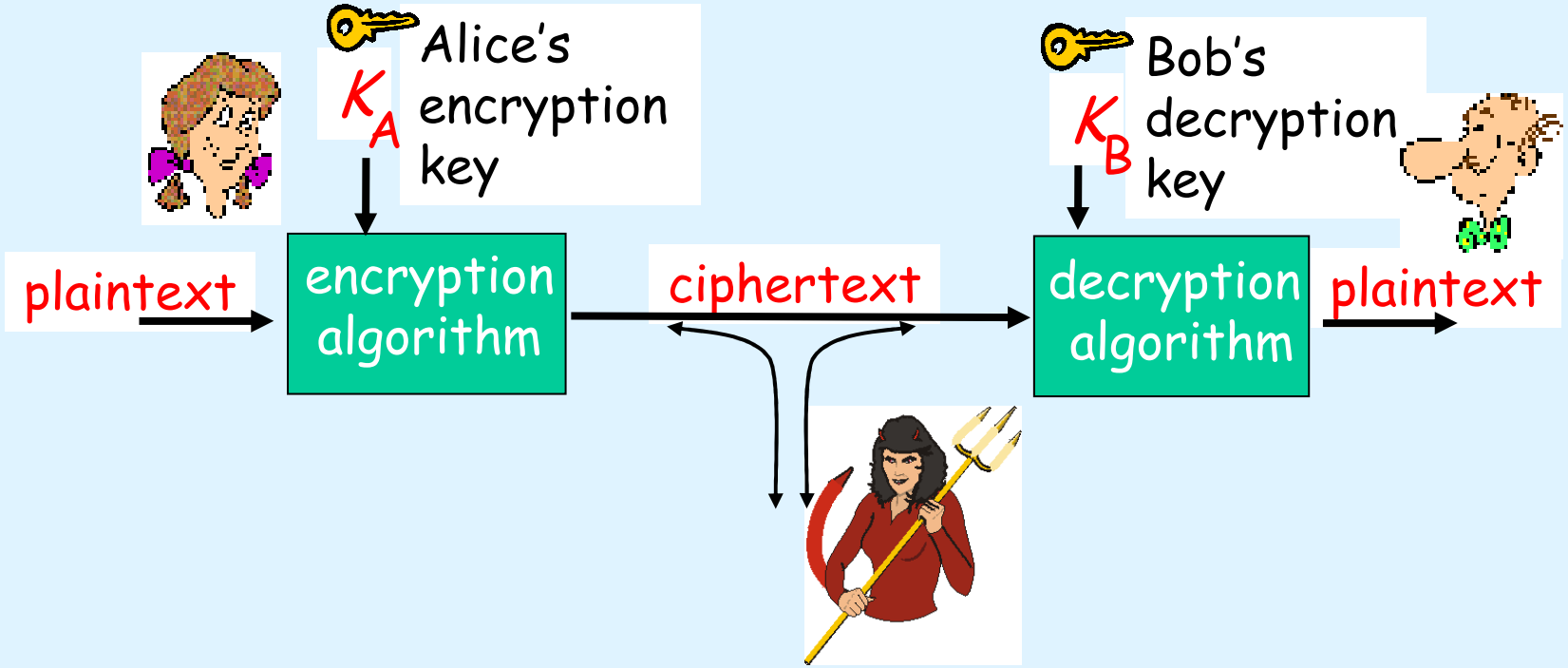
- sender encrypts message
- receiver decrypts message

Authentication: sender, receiver want to confirm identity of each other

Message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

Access and availability: services must be accessible and available to users, but NOT to intruders

The language of cryptography



symmetric key crypto: sender, receiver keys *identical*

public-key crypto: encryption key *public*, decryption key *secret* (private)

Kryperingsalgoritmer för symmetriska nycklar

- Data Encryption Standard (DES)
- 3DES
- Advanced Encryption Standard (AES)
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- WPA2

Kryperingsalgoritm för privat/publik nyckel

- Ron Rivest, Adi Shamir, Leonard Aldeman (RSA)
  - Faktorisering bestående av enbart primtal
  - Moduloberäkningar
  - Snabb algoritm
  - Det finns ingen känd snabb fakt.- algoritm för att knäcka nycklarna

Meddelandeintegritet (Message digest)

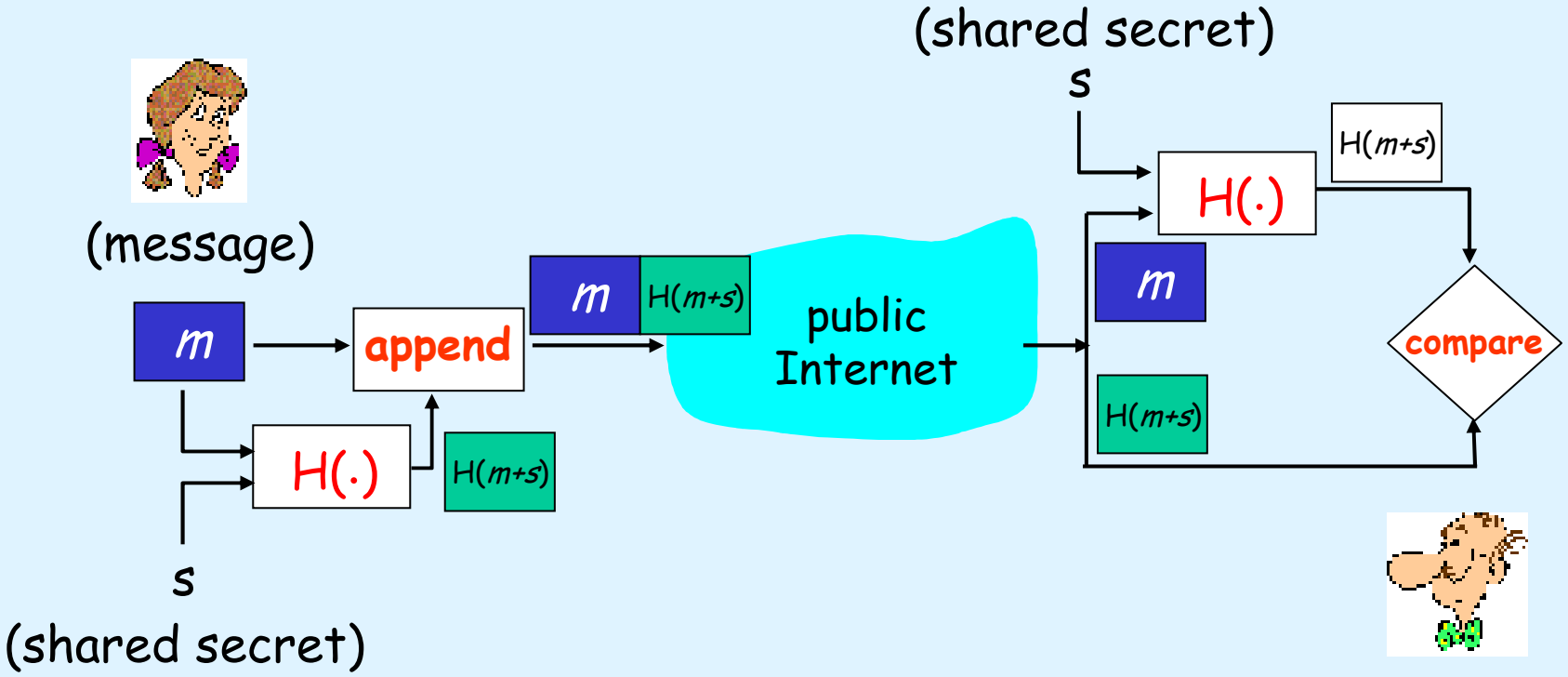
Sändaren

- Ett meddelande, m
- Hashfunktionen av meddelandet, H(m)
- Skickar m + H(m) (konkatenering)

Mottagaren

- Tar emot m' + H(m)
- Beräknar H(m')
- Mottagaren testar om H(m) = H(m')

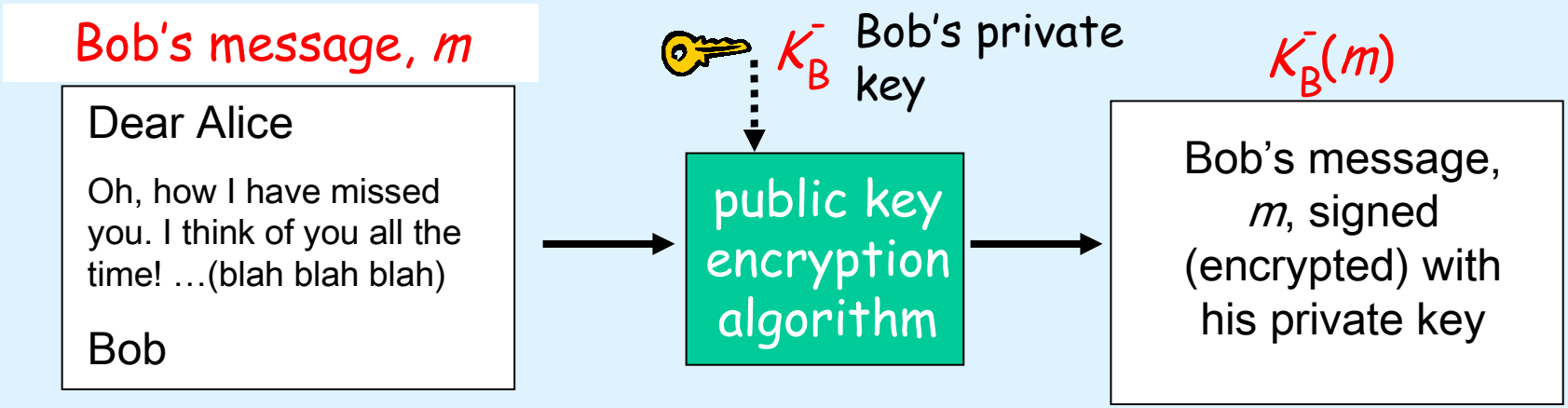
Message Authentication Code (MAC)



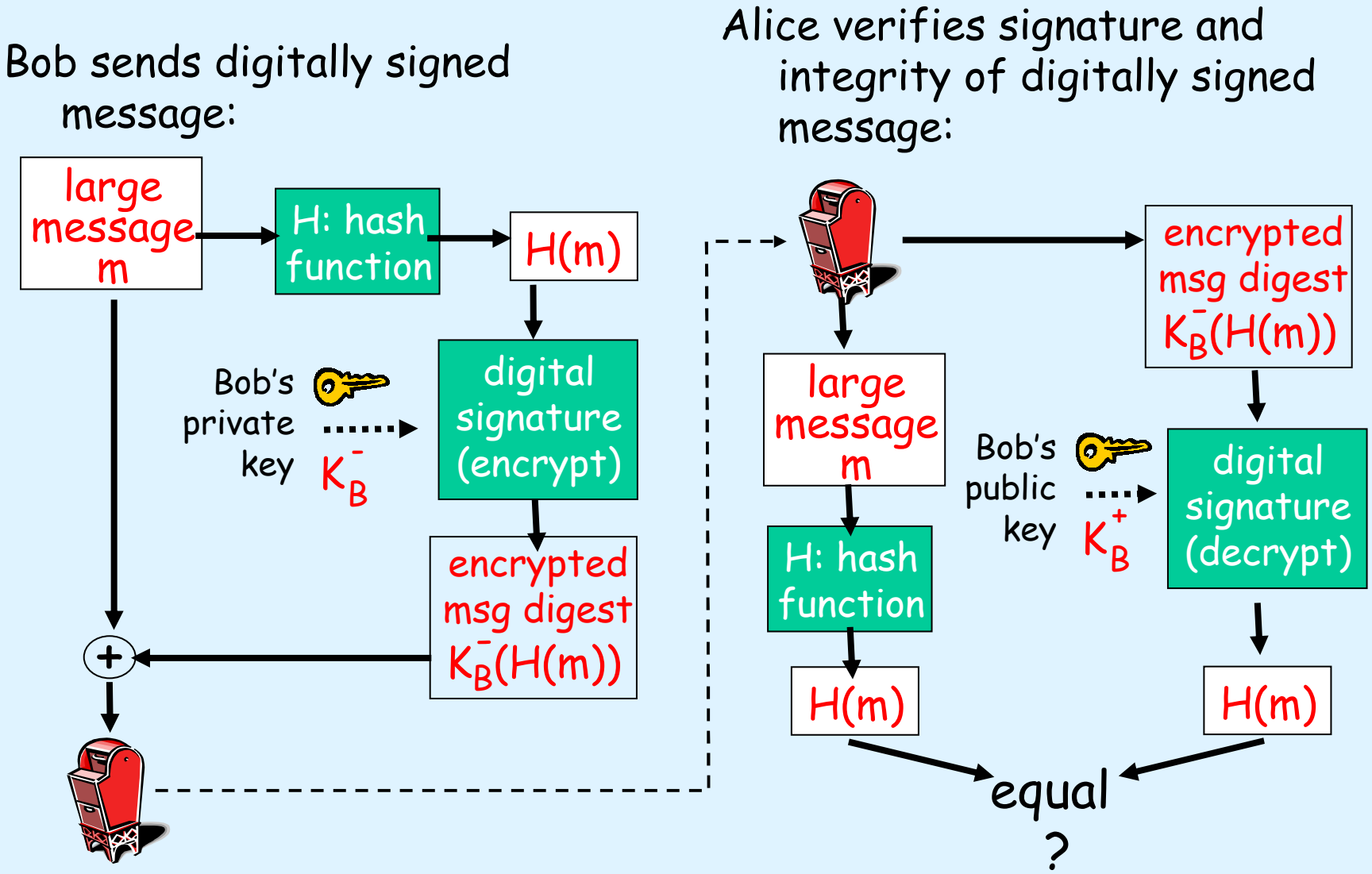
Digital Signatures

simple digital signature for message m:

- Bob "signs" m by encrypting with his private key K_B^-, creating "signed" message, $K_B^-(m)$

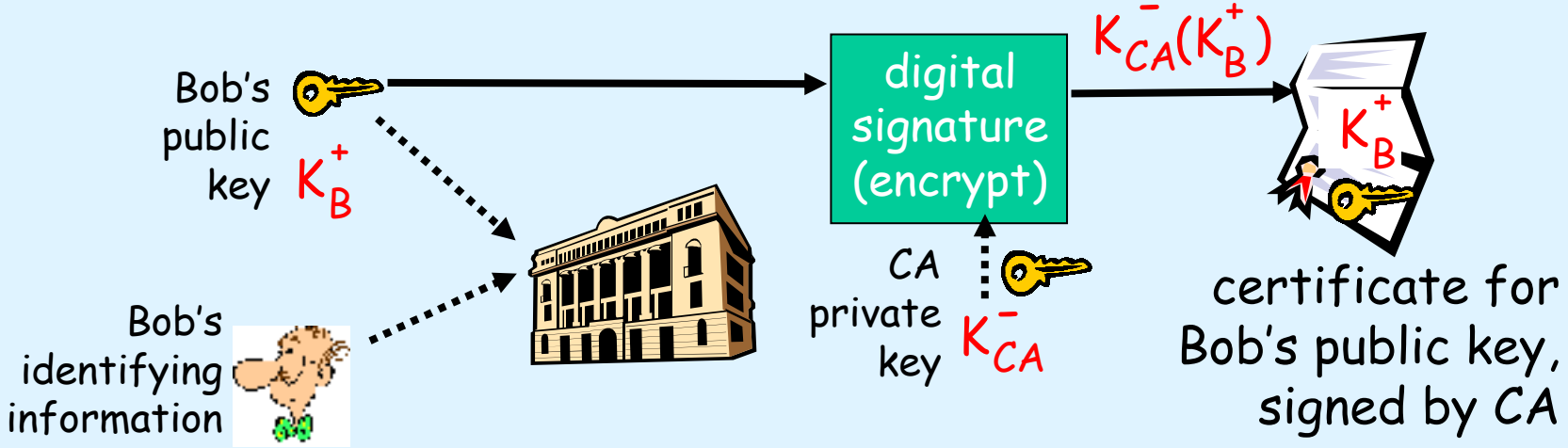


Digital signature = signed message digest



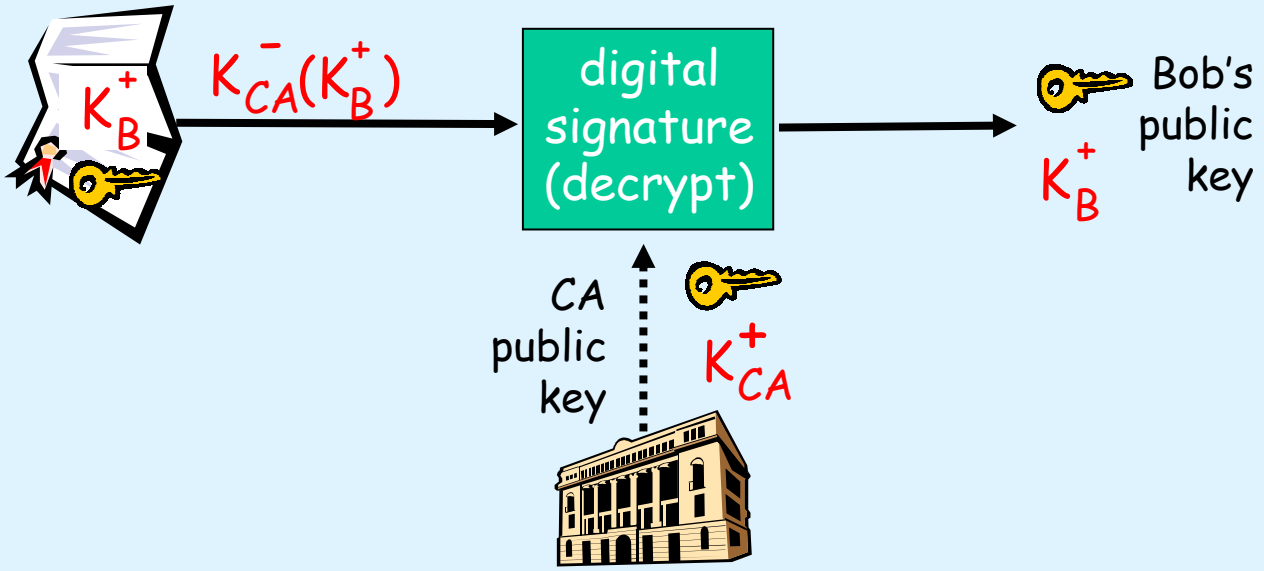
Certification Authorities

- Certification Authority (CA): binds public key to particular entity, E.
- E registers its public key with CA.
  - E provides "proof of identity" to CA.
  - CA creates certificate binding E to its public key.
  - certificate containing E's public key digitally signed by CA: CA says "This is E's public key."



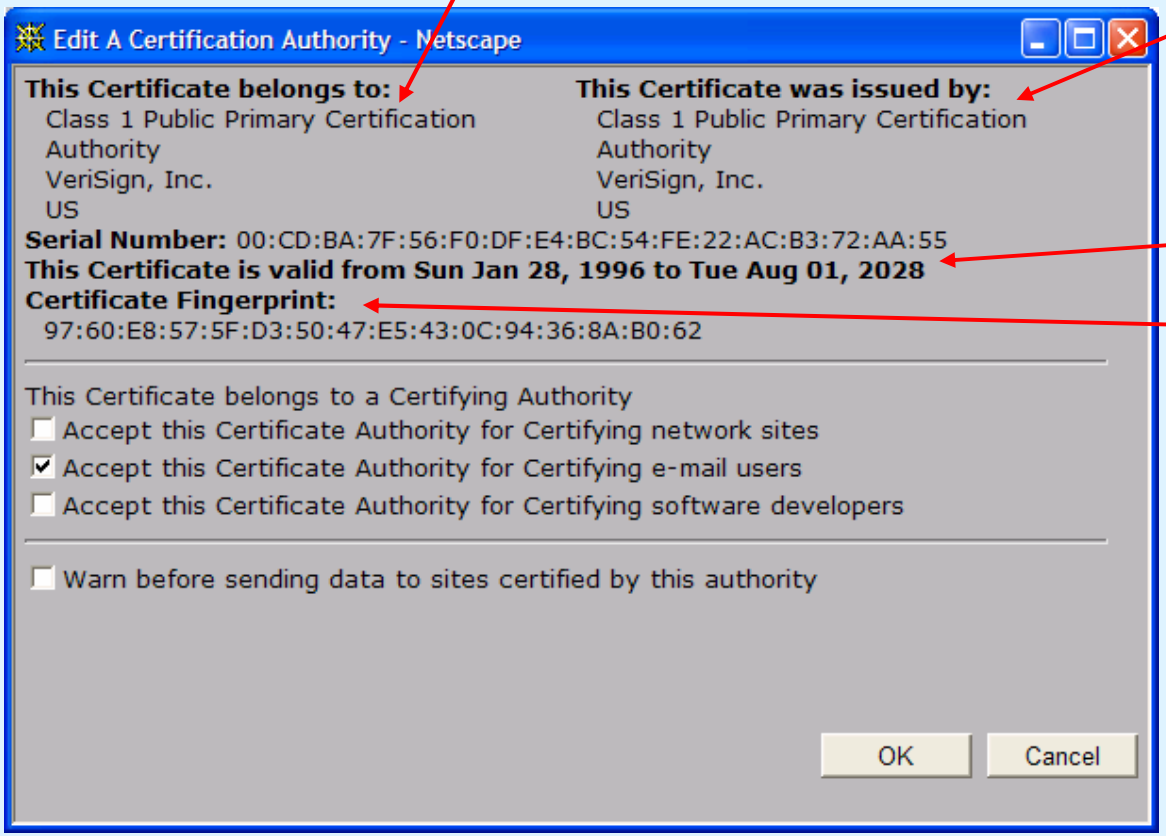
Certification Authorities

- when Alice wants Bob's public key:
  - gets Bob's certificate (Bob or elsewhere).
  - apply CA's public key to Bob's certificate, get Bob's public key



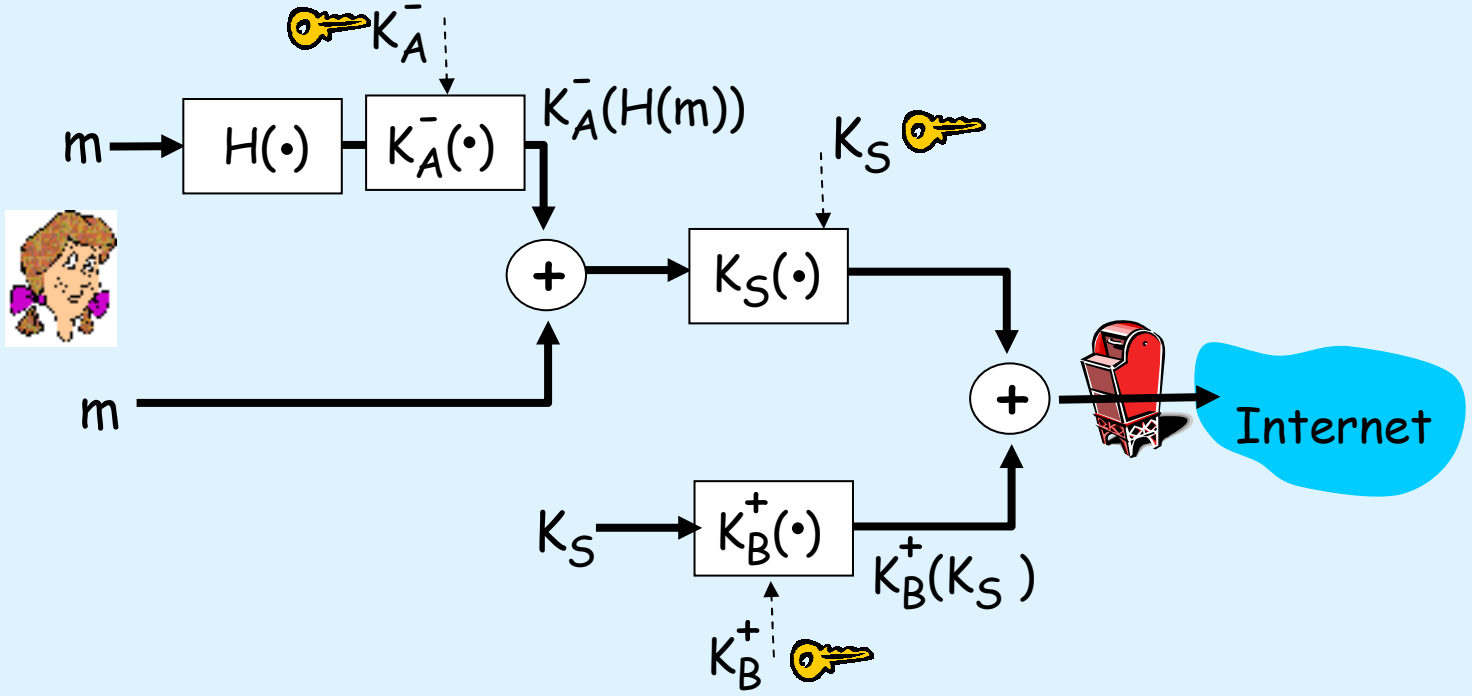
A certificate contains:

- Serial number (unique to issuer)
- info about certificate owner, including algorithm and key value itself (not shown)
- info about certificate issuer
- valid dates
- digital signature by issuer



Pretty Good Privacy (PGP) (1)

- Alice wants to provide secrecy, sender authentication, message integrity.



Alice uses three keys: her private key, Bob's public key, newly created symmetric key

Pretty good privacy (PGP) (2)

A PGP signed message:

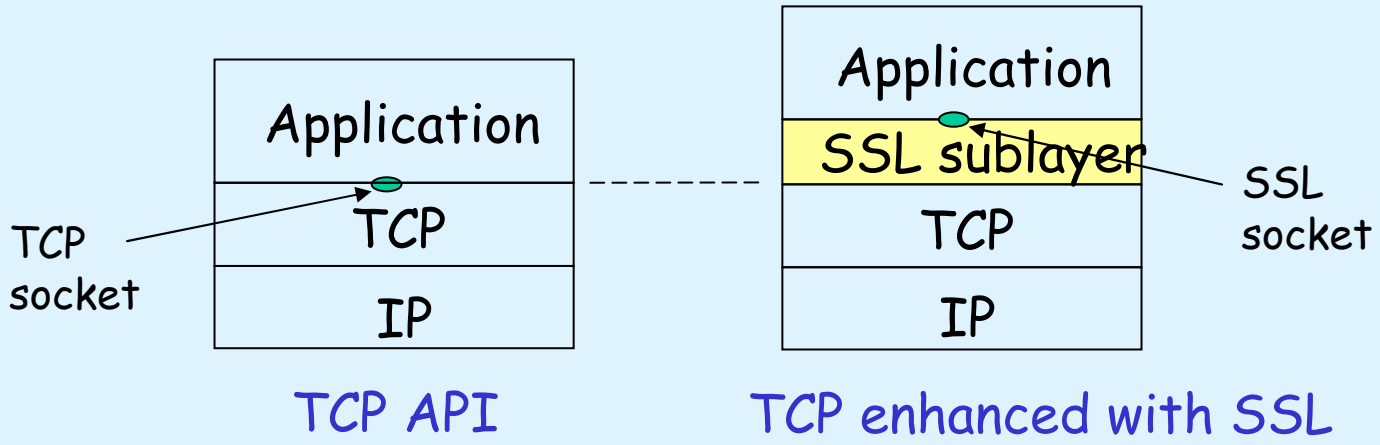
```
---BEGIN PGP SIGNED
   MESSAGE---
Hash: SHA1

Bob: See you on Saturday.
   Love you. Passionately
   yours, Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4
   vB3mqJhFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

Secure sockets layer (SSL)

- provides transport layer security to any TCP-based application using SSL services.
  - e.g., between Web browsers, servers for e-commerce (https://)
- security services:
  - server authentication, data encryption, client authentication (optional)



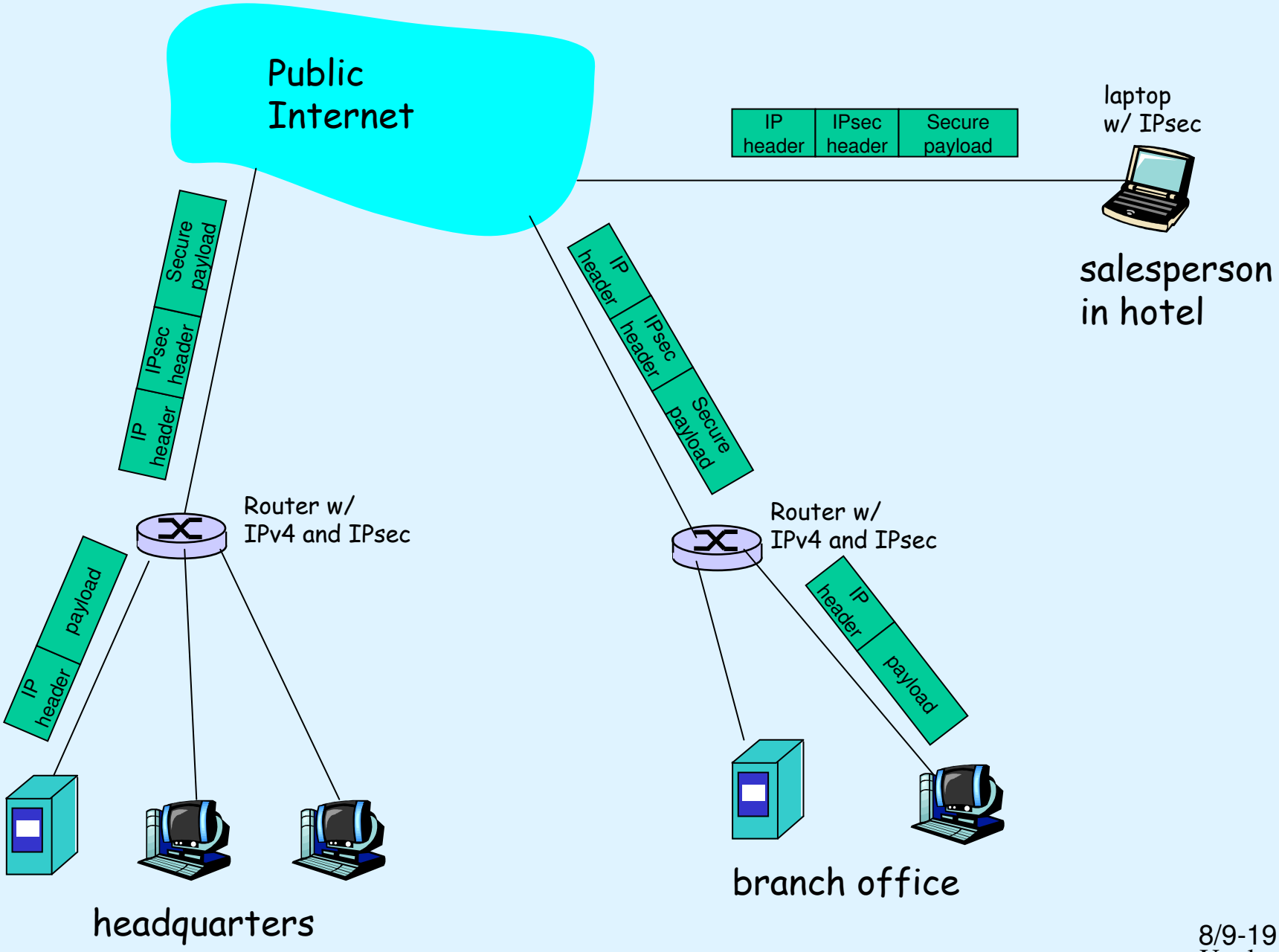
IP Security (IPsec) (1)

- Utökad säkerhet på Internet-nivå (nätverksnivå)
  - För både TCP och UDP
- Ger Virtual Private Network (VPN)
- Logisk simplexförbindelse (enkelriktad) s.k. Security Association (SA)
- Huvudprotokoll
  - Authentication Header (AH)

    Autenticitet och dataintegritet.
  - Encapsulation Security Payload (ESP)

    Autenticitet, dataintegritet och konfidentiell överföring.

Virtual Private Network (VPN)



IP Security (IPsec) (2)

- Security Association Database (SAD)
  - VPN-enhetens SAD håller ordning på en eller flera SA-entiteter.
- Varje SA (logisk simplexförbindelse) anges med:
  - Security Parameter Index (SPI, 32-bitars)
  - SA-sändarens och SA-mottagarens IP-adresser
    (Inte nödvändigtvis samma IP-adresser som till sändande och mottagande värdar eftersom SA kan hanteras av kantroutrarna.)
  - Verifieringsnyckel (authentication key)
  - Typ av integritetskontroll (t.ex. HMAC med MD5)
  - Typ av krypteringmetod (t.ex. 3DES) och nyckel
- Security Policy Database (SPD)
  - Anger det som ska göras med olika typer inkommande paket.

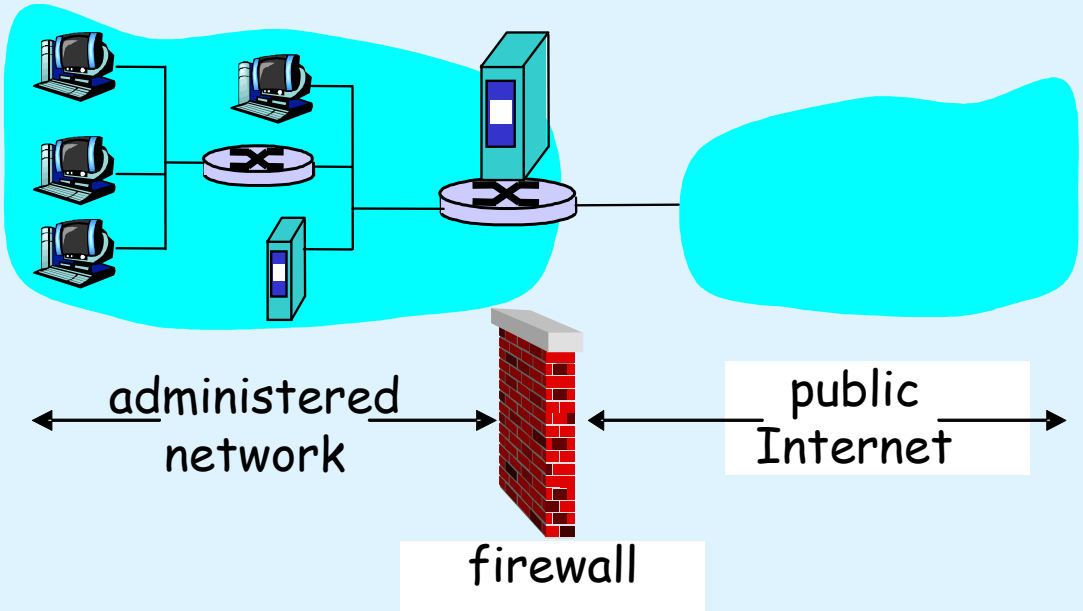
IP Security (IPsec) (3)

- VPN-tillstånd (med AH eller ESP)
  1. Transport
     Mellan värdar (utan inblandning av routrarna).
  2. Tunnel (typ 1)
     Mellan värdarnas kantroutrar.
  3. Tunnel (typ 2)
     Mellan en kantrouter och en värd (inte dess kantrouter).

Firewalls

firewall

isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.



Paketfiltrerande brandvägg (1)

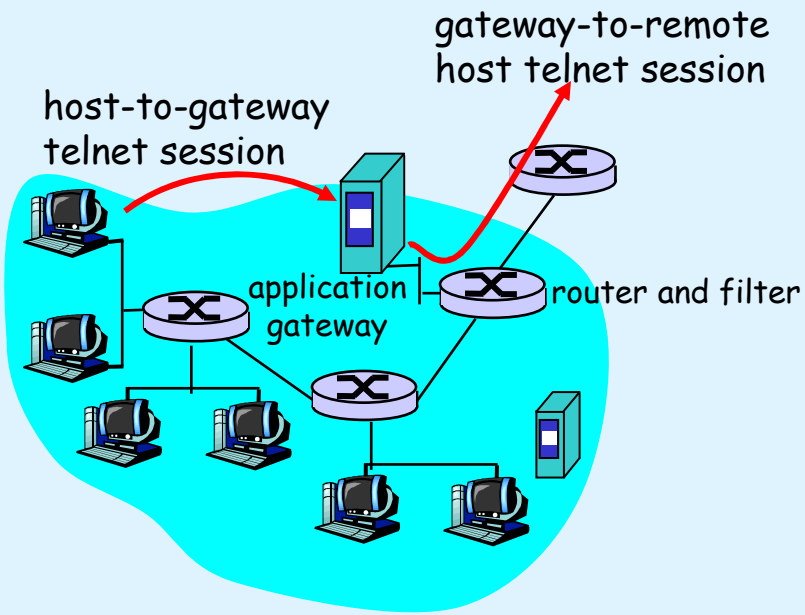
- Kan finnas i en standardgateway (små och medelstora nät)
- Kan finnas som separat enhet (stora nät)
- Filterparametrar (klassisk filtrering)
  - IP-adresser (sändare/mottagare)
  - TCP/UDP-portnummer (sändare/mottagare)
  - ICMP-typ
  - Användandet av TCP-SYN eller TCP-ACK

Paketfiltrerande brandvägg (2)

- Tillståndsfiltrering (stateful packet filter)
  - Följer TCP-segment från uppkoppling till nedkoppling
  - Avslöjar på så sätt inträngande paket

Application gateways

- filters packets on application data as well as on IP/TCP/UDP fields.
- example: allow select internal users to telnet outside.



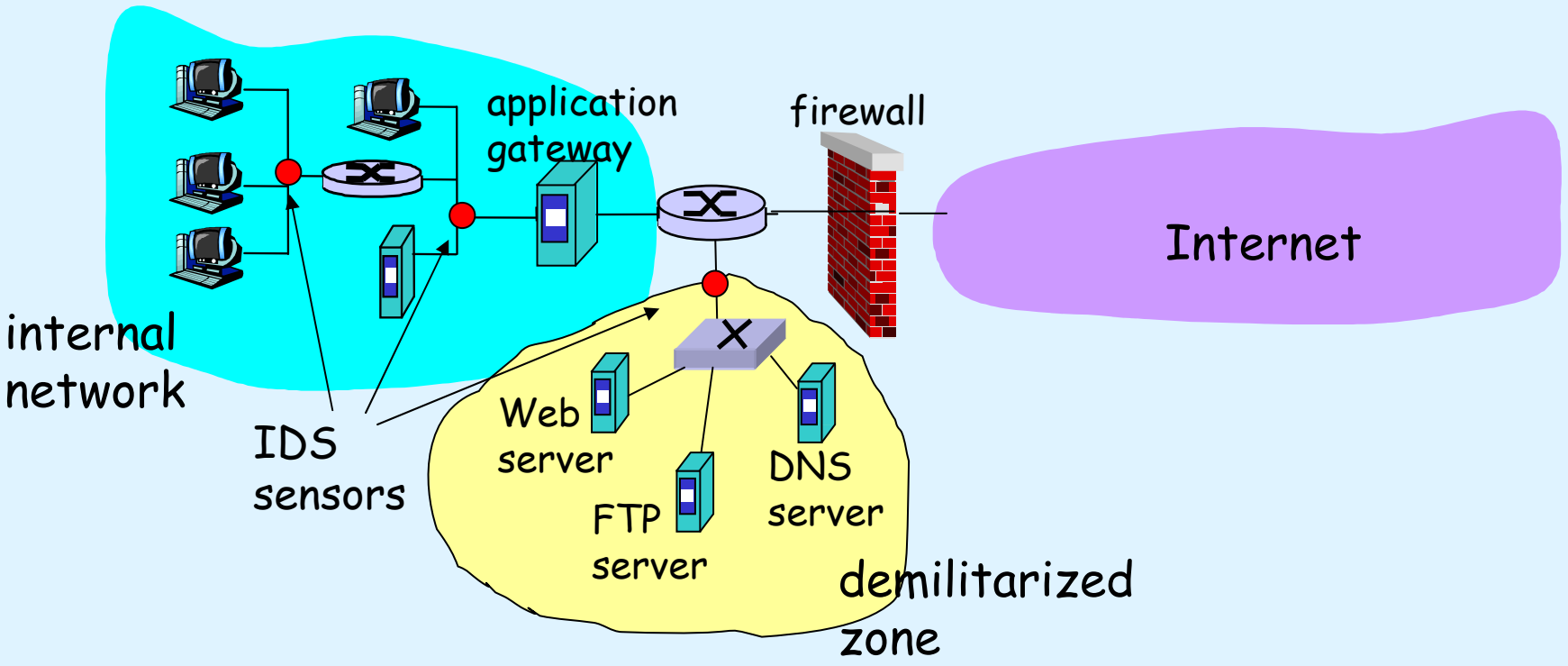
1. require all telnet users to telnet through gateway.
2. for authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
3. router filter blocks all telnet connections not originating from gateway.

Intrusion detection systems (IDS)

- packet filtering:
  - operates on TCP/IP headers only
  - no correlation check among sessions
- *IDS: intrusion detection system*
  - *deep packet inspection:* look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)
  - examine correlation among multiple packets
    - port scanning
    - network mapping
    - DoS attack

IDS

- multiple IDSs: different types of checking at different locations

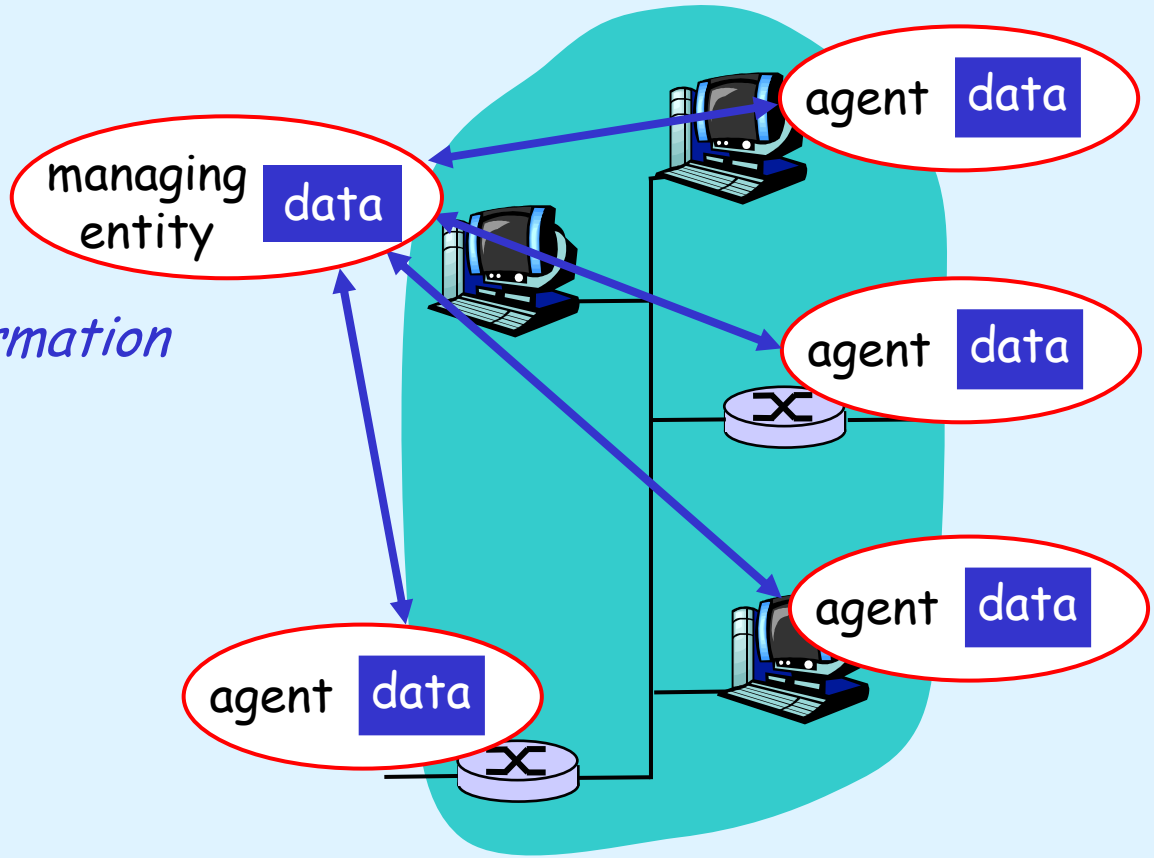


Network management

- Upptäcka fel på nätverkskort
- Övervaka värdar
- Övervaka trafik
- Upptäcka "route flapping"
- Övervaka Service Level Agreements (SLA)
- Upptäcka intrång

Infrastructure for network management

Management Information Base (MIB)

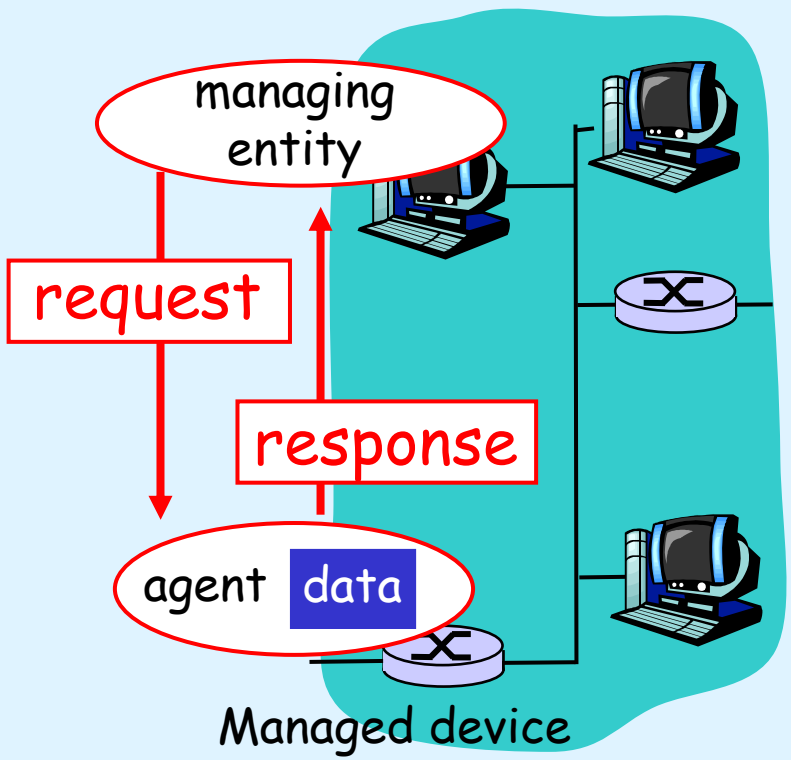


Simple Network Management Protocol (SNMP)

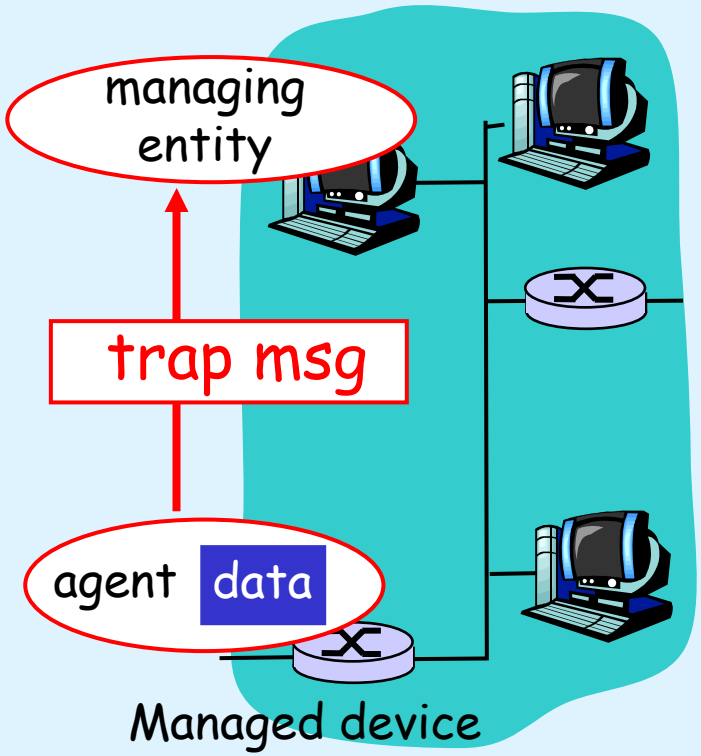
- Network Management Protocol
- SNMPv1, SNMPv2 och SNMPv3

SNMP protocol

Two ways to convey MIB info, commands:



request/response mode



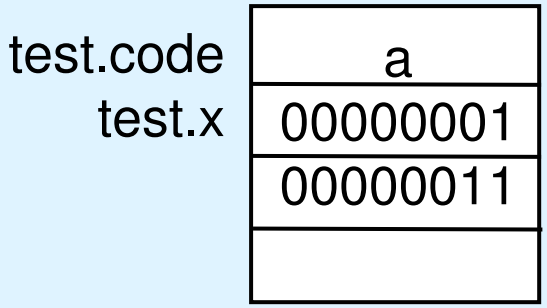
trap mode

The presentation problem

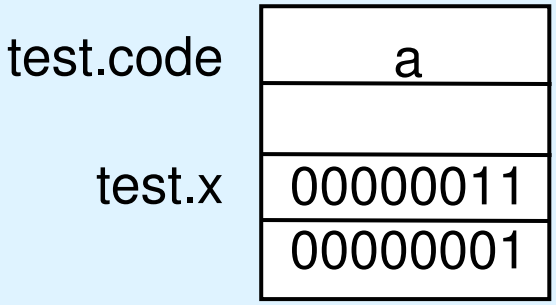
Q: does perfect memory-to-memory copy solve "the communication problem"?

A: not always!

```
struct {
   char code;
    int x;
    } test;
test.x = 769;
test.code='a'
```



host 1 format



host 2 format

problem: different data format, storage conventions

ASN.1: Abstract Syntax Notation 1

- ISO standard X.680
  - used extensively in Internet
- defined data types, object constructors
- BER: Basic Encoding Rules
  - specify how ASN.1-defined data objects to be transmitted
  - each transmitted object has Type, Length, Value (TLV) encoding

TLV Encoding

Idea: transmitted data is self-identifying

- T: data type, one of ASN.1-defined types
- L: length of data in bytes
- V: value of data, encoded according to ASN.1 standard

Tag Value	Type
1	Boolean
2	Integer
3	Bitstring
4	Octet string
5	Null
6	Object Identifier
9	Real