

Chapter 8

Network Security

A note on the use of these ppt slides:

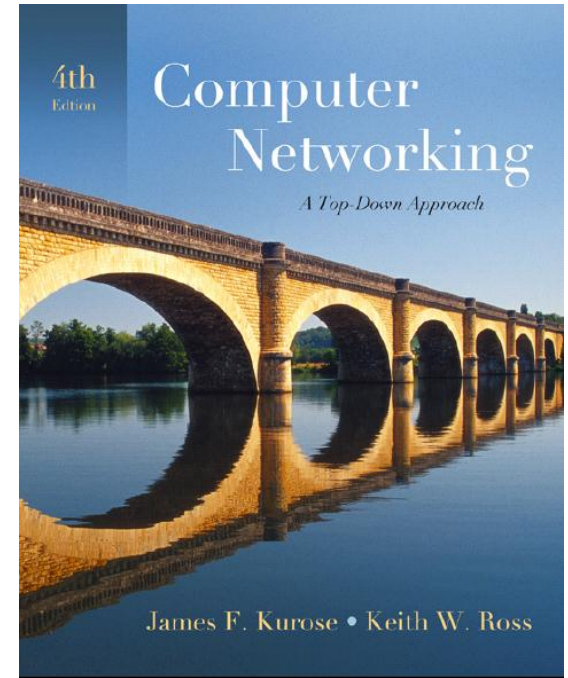
We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- ❑ 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

All material copyright 1996-2007

J.F Kurose and K.W. Ross, All Rights Reserved



*Computer Networking:
A Top Down Approach ,
4th edition.*

*Jim Kurose, Keith Ross
Addison-Wesley, July
2007.*

Chapter 8: Network Security

Chapter goals:

- ❑ understand principles of network security:
 - cryptography and its *many* uses beyond "confidentiality"
 - authentication
 - message integrity
- ❑ security in practice:
 - firewalls and intrusion detection systems
 - security in application, transport, network, link layers

Chapter 8 roadmap

8.1 What is network security?

8.2 Principles of cryptography

8.3 Message integrity

8.4 End point authentication

8.5 Securing e-mail

8.6 Securing TCP connections: SSL

8.7 Network layer security: IPsec

8.8 Securing wireless LANs

8.9 Operational security: firewalls and IDS

What is network security?

Confidentiality: only sender, intended receiver should “understand” message contents

- sender encrypts message
- receiver decrypts message

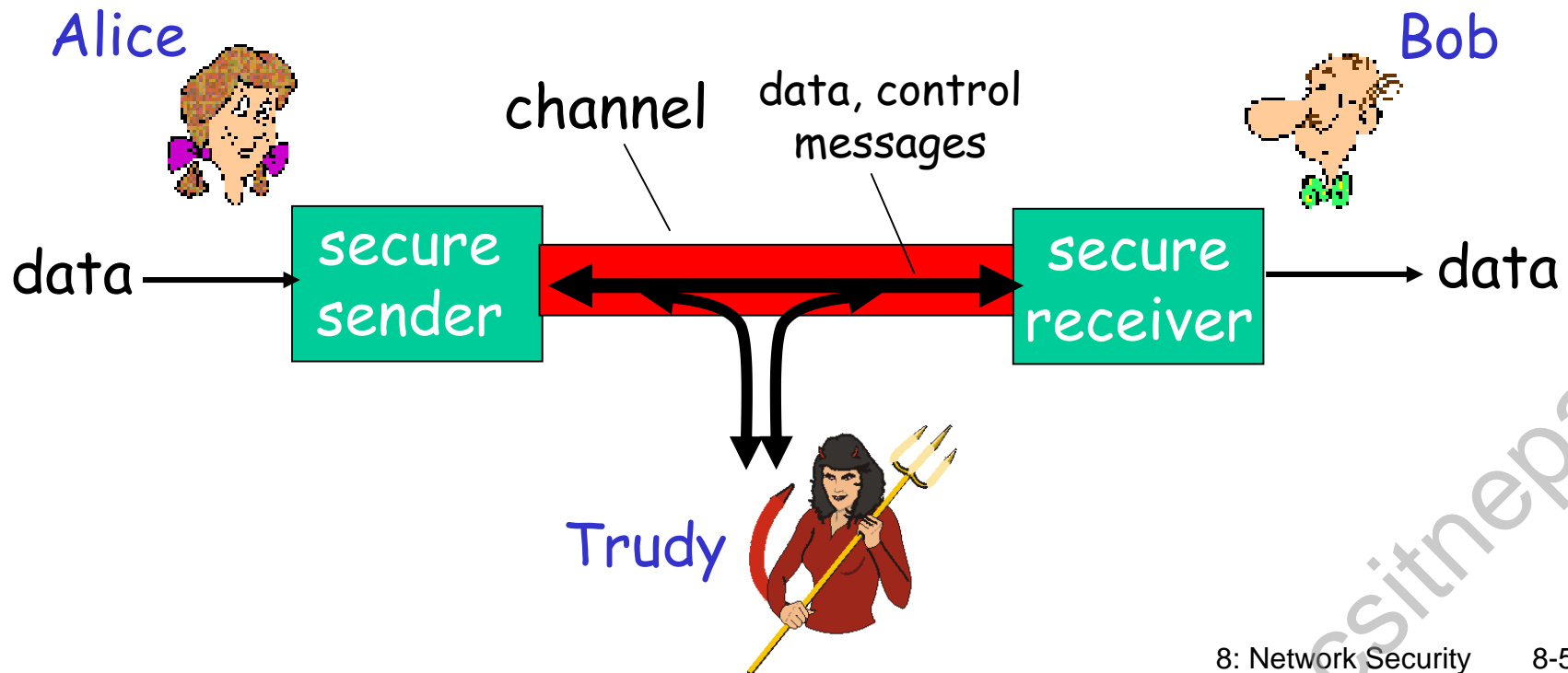
Authentication: sender, receiver want to confirm identity of each other

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

Friends and enemies: Alice, Bob, Trudy

- ❑ well-known in network security world
- ❑ Bob, Alice (lovers!) want to communicate "securely"
- ❑ Trudy (intruder) may intercept, delete, add messages



Who might Bob, Alice be?

- ❑ ... well, *real-life* Bobs and Alices!
- ❑ Web browser/server for electronic transactions (e.g., on-line purchases)
- ❑ on-line banking client/server
- ❑ DNS servers
- ❑ routers exchanging routing table updates
- ❑ other examples?

There are bad guys (and girls) out there!

Q: What can a “bad guy” do?

A: a lot!

- *eavesdrop*: intercept messages
- actively *insert* messages into connection
- *impersonation*: can fake (spoof) source address in packet (or any field in packet)
- *hijacking*: “take over” ongoing connection by removing sender or receiver, inserting himself in place
- *denial of service*: prevent service from being used by others (e.g., by overloading resources)

more on this later

Chapter 8 roadmap

8.1 What is network security?

8.2 Principles of cryptography

8.3 Message integrity

8.4 End point authentication

8.5 Securing e-mail

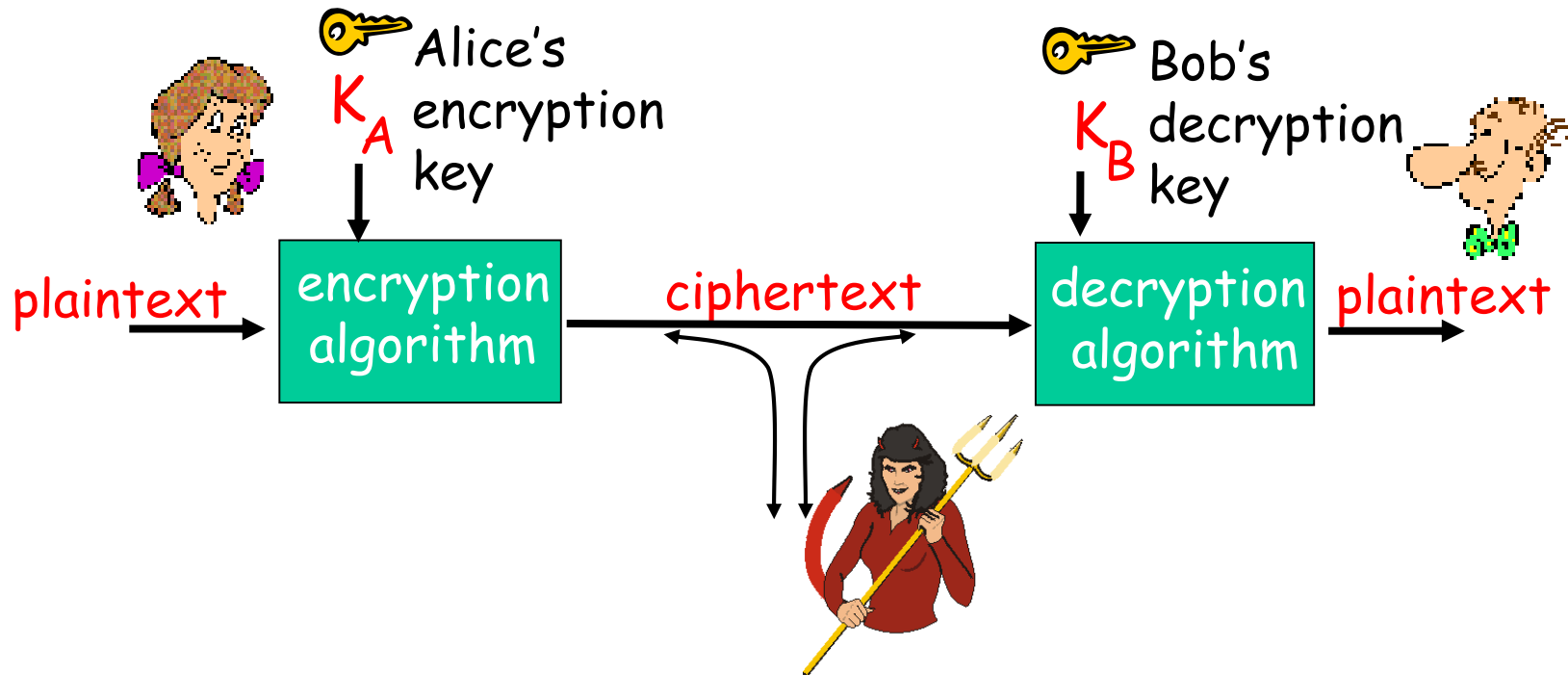
8.6 Securing TCP connections: SSL

8.7 Network layer security: IPsec

8.8 Securing wireless LANs

8.9 Operational security: firewalls and IDS

The language of cryptography



symmetric key crypto: sender, receiver keys *identical*
public-key crypto: encryption key *public*, decryption key *secret* (private)

Symmetric key cryptography

substitution cipher: substituting one thing for another

- monoalphabetic cipher: substitute one letter for another

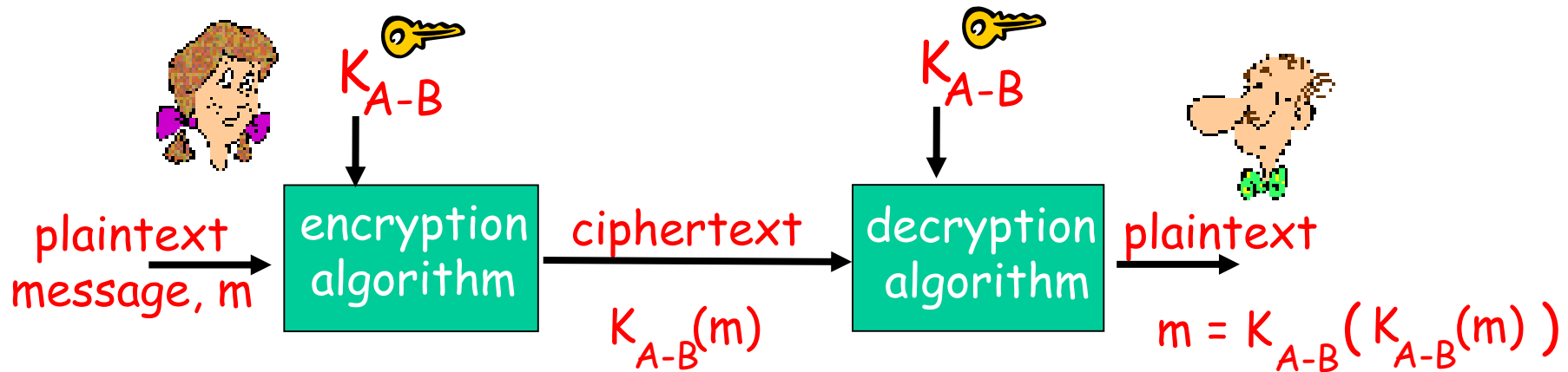
| | |
|-------------|----------------------------|
| plaintext: | abcdefghijklmnopqrstuvwxyz |
| | ↓ ↓ |
| ciphertext: | mnbvcxzasdfghjklpoiuytrewq |

E.g.: Plaintext: bob. i love you. alice
ciphertext: nkn. s gktc wky. mgsbc

Q: How hard to break this simple cipher?:

- ☐ brute force (how hard?)
- ☐ other?

Symmetric key cryptography



symmetric key crypto: Bob and Alice share know same (symmetric) key: K_{A-B}

- e.g., key is knowing substitution pattern in mono alphabetic substitution cipher
- Q: how do Bob and Alice agree on key value?

Symmetric key crypto: DES

DES: Data Encryption Standard

- ❑ US encryption standard [NIST 1993]
- ❑ 56-bit symmetric key, 64-bit plaintext input
- ❑ How secure is DES?
 - DES Challenge: 56-bit-key-encrypted phrase ("Strong cryptography makes the world a safer place") decrypted (brute force) in 4 months
 - no known "backdoor" decryption approach
- ❑ making DES more secure:
 - use three keys sequentially (3-DES) on each datum
 - use cipher-block chaining

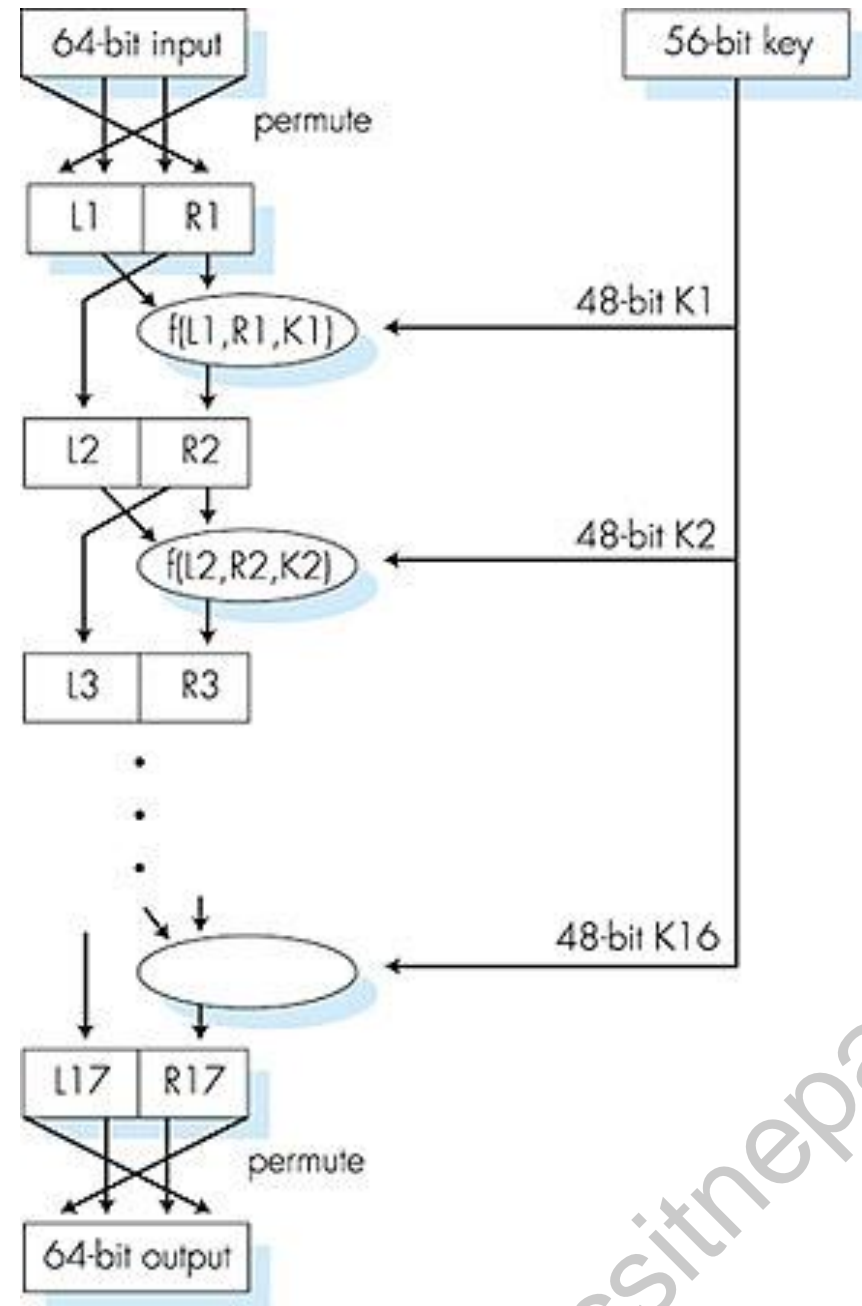
Symmetric key crypto: DES

DES operation

initial permutation

16 identical "rounds" of
function application,
each using different
48 bits of key

final permutation

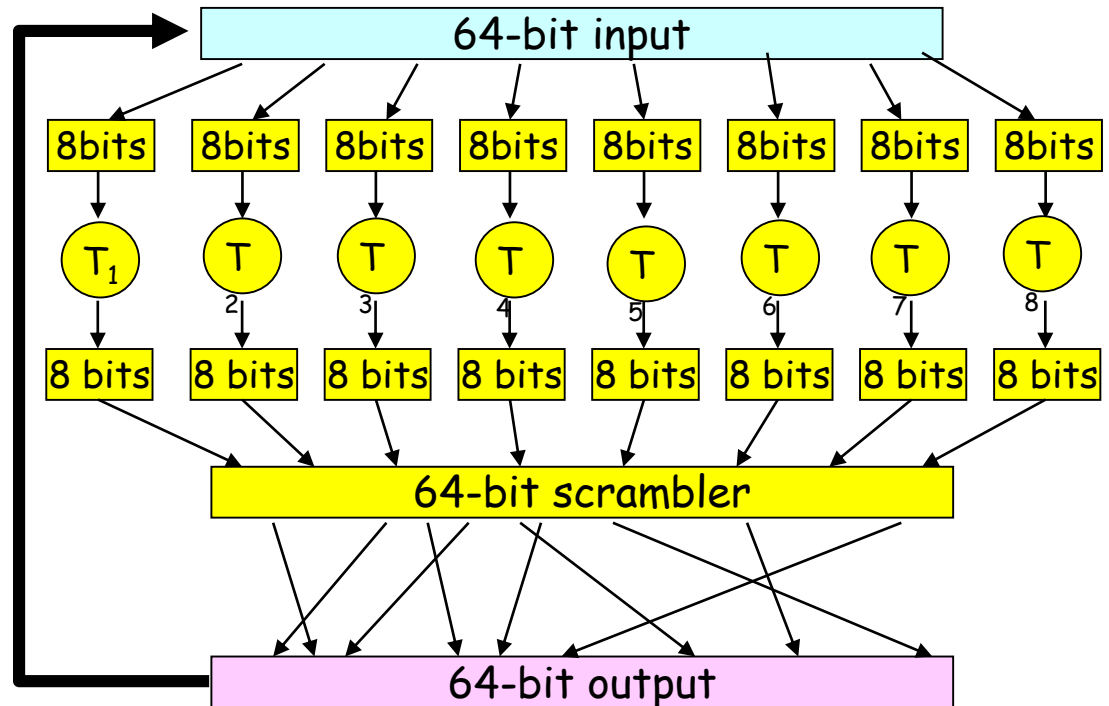


AES: Advanced Encryption Standard

- ❑ new (Nov. 2001) symmetric-key NIST standard, replacing DES
- ❑ processes data in 128 bit blocks
- ❑ 128, 192, or 256 bit keys
- ❑ brute force decryption (try each key) taking 1 sec on DES, takes 149 trillion years for AES

Block Cipher

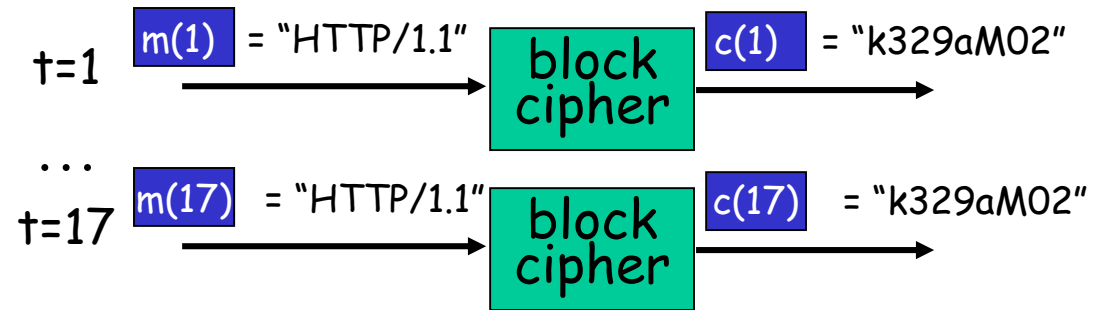
loop for
n rounds



- ❑ one pass through: one input bit affects eight output bits
- ❑ multiple passes: each input bit affects all output bits
- ❑ block ciphers: DES, 3DES, AES

Cipher Block Chaining

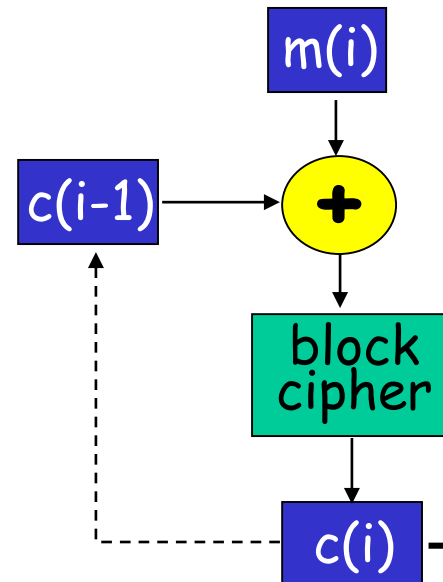
- ❑ cipher block: if input block repeated, will produce same cipher text:



- ❑ *cipher block chaining:*

XOR ith input block, $m(i)$, with previous block of cipher text, $c(i-1)$

- $c(0)$ transmitted to receiver in clear
- what happens in "HTTP/1.1" scenario from above?



Public key cryptography

symmetric key crypto

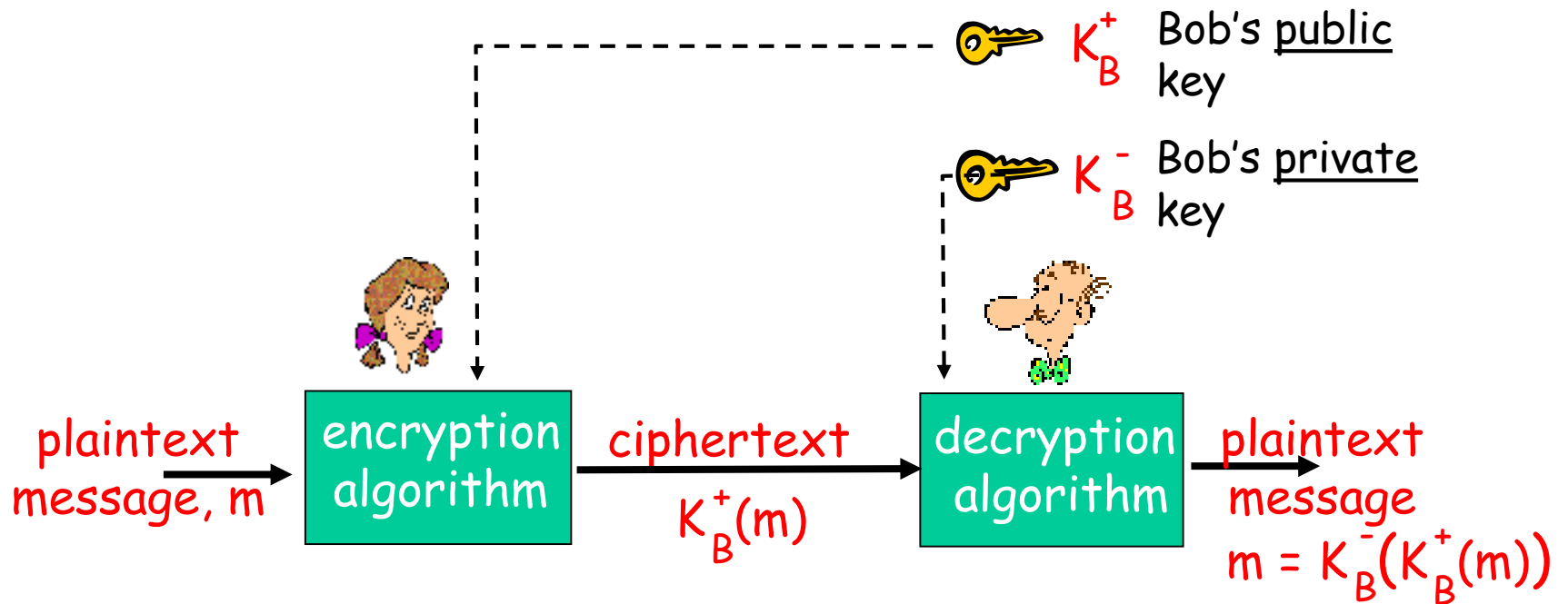
- ❑ requires sender, receiver know shared secret key
- ❑ Q: how to agree on key in first place (particularly if never "met")?

public key cryptography

- ❑ radically different approach [Diffie-Hellman76, RSA78]
- ❑ sender, receiver do *not* share secret key
- ❑ *public* encryption key known to *all*
- ❑ *private* decryption key known only to receiver



Public key cryptography



Public key encryption algorithms

Requirements:

- ① need $K_B^+(\cdot)$ and $K_B^-(\cdot)$ such that

$$K_B^-(K_B^+(m)) = m$$

- ② given public key K_B^+ , it should be impossible to compute private key K_B^-

RSA: Rivest, Shamir, Adleman algorithm

RSA: Choosing keys

1. Choose two large prime numbers p, q .
(e.g., 1024 bits each)
2. Compute $n = pq$, $z = (p-1)(q-1)$
3. Choose e (with $e < n$) that has no common factors with z . (e, z are "relatively prime").
4. Choose d such that $ed-1$ is exactly divisible by z .
(in other words: $ed \bmod z = 1$).
5. Public key is (n, e) . Private key is (n, d) .

$\underbrace{\hspace{1.5cm}}_{K_B^+}$

$\underbrace{\hspace{1.5cm}}_{K_B^-}$

RSA: Encryption, decryption

0. Given (n,e) and (n,d) as computed above
1. To encrypt bit pattern, m , compute
 $c = m^e \bmod n$ (i.e., remainder when m^e is divided by n)
2. To decrypt received bit pattern, c , compute
 $m = c^d \bmod n$ (i.e., remainder when c^d is divided by n)

Magic
happens!

$$m = \underbrace{(m^e \bmod n)}_c^d \bmod n$$

RSA example:

Bob chooses $p=5$, $q=7$. Then $n=35$, $z=24$.

$e=5$ (so e , z relatively prime).

$d=29$ (so $ed-1$ exactly divisible by z).

encrypt:

| <u>letter</u> | <u>m</u> | <u>m^e</u> | <u>$c = m^e \bmod n$</u> |
|---------------|----------|-------------------------|-------------------------------------|
| I | 12 | 1524832 | 17 |

decrypt:

| <u>c</u> | <u>c^d</u> | <u>$m = c^d \bmod n$</u> | <u>letter</u> |
|----------|--------------------------------------|-------------------------------------|---------------|
| 17 | 481968572106750915091411825223071697 | 12 | I |

RSA: Why is that $m = (m^e \bmod n)^d \bmod n$

Useful number theory result: If p, q prime and $n = pq$, then:

$$x^y \bmod n = x^{y \bmod (p-1)(q-1)} \bmod n$$

$$\begin{aligned} (m^e \bmod n)^d \bmod n &= m^{ed} \bmod n \\ &= m^{ed \bmod (p-1)(q-1)} \bmod n \\ &\quad \text{(using number theory result above)} \\ &= m^1 \bmod n \\ &\quad \text{(since we chose } ed \text{ to be divisible by } (p-1)(q-1) \text{ with remainder 1)} \\ &= m \end{aligned}$$

RSA: another important property

The following property will be *very* useful later:

$$\underbrace{K_B^-(K_B^+(m))}_{\text{use public key first, followed by private key}} = m = \underbrace{K_B^+(K_B^-(m))}_{\text{use private key first, followed by public key}}$$

use public key
first, followed
by private key

use private key
first, followed
by public key

Result is the same!

Chapter 8 roadmap

8.1 What is network security?

8.2 Principles of cryptography

8.3 Message integrity

8.4 End point authentication

8.5 Securing e-mail

8.6 Securing TCP connections: SSL

8.7 Network layer security: IPsec

8.8 Securing wireless LANs

8.9 Operational security: firewalls and IDS

Message Integrity

Bob receives msg from Alice, wants to ensure:

- ❑ message originally came from Alice
- ❑ message not changed since sent by Alice

Cryptographic Hash:

- ❑ takes input m , produces fixed length value, $H(m)$
 - e.g., as in Internet checksum
- ❑ computationally infeasible to find two different messages, x, y such that $H(x) = H(y)$
 - equivalently: given $m = H(x)$, (x unknown), can not determine x .
 - note: Internet checksum *fails* this requirement!

Internet checksum: poor crypto hash function

Internet checksum has some properties of hash function:

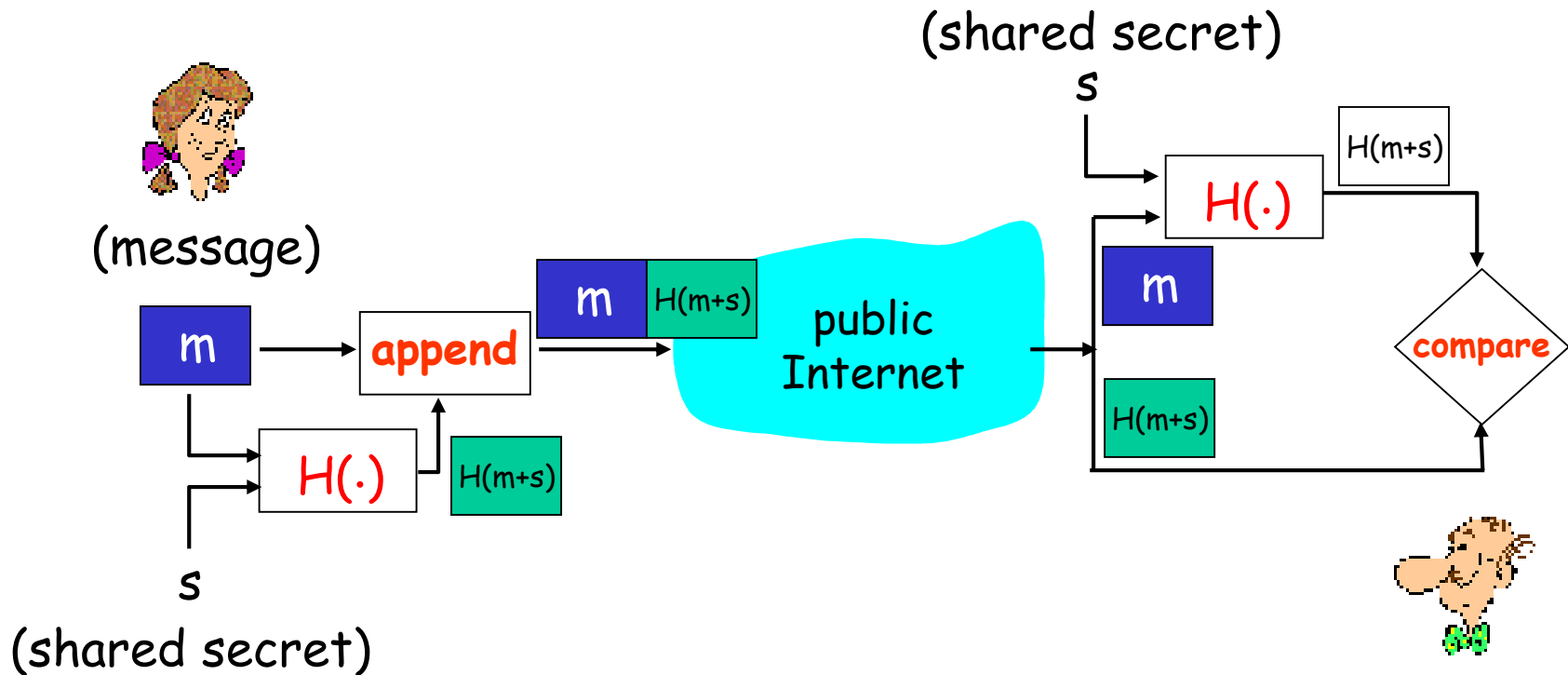
- ✓ produces fixed length digest (16-bit sum) of message
- ✓ is many-to-one

But given message with given hash value, it is easy to find another message with same hash value:

| <u>message</u> | <u>ASCII format</u> | | <u>message</u> | <u>ASCII format</u> |
|----------------|---------------------|--|----------------|---------------------|
| I O U 1 | 49 4F 55 31 | | I O U <u>9</u> | 49 4F 55 <u>39</u> |
| 0 0 . 9 | 30 30 2E 39 | | 0 0 . <u>1</u> | 30 30 2E <u>31</u> |
| 9 B O B | 39 42 4F 42 | | 9 B O B | 39 42 4F 42 |
| <hr/> | | | <hr/> | |
| B2 C1 D2 AC | | | B2 C1 D2 AC | |

different messages
but identical checksums!

Message Authentication Code



MACs in practice

- MD5 hash function widely used (RFC 1321)
 - computes 128-bit MAC in 4-step process.
 - arbitrary 128-bit string x , appears difficult to construct msg m whose MD5 hash is equal to x
 - recent (2005) attacks on MD5
- SHA-1 is also used
 - US standard [NIST, FIPS PUB 180-1]
 - 160-bit MAC

Digital Signatures

cryptographic technique analogous to handwritten signatures.

- ❑ sender (Bob) digitally signs document, establishing he is document owner/creator.
- ❑ **verifiable, nonforgeable**: recipient (Alice) can prove to someone that Bob, and no one else (including Alice), must have signed document


Digital Signatures

simple digital signature for message m :

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

Bob's message, m

Dear Alice
Oh, how I have missed
you. I think of you all the
time! ... (blah blah blah)
Bob

 K_B^- Bob's private
key

public key
encryption
algorithm

$K_B^-(m)$

Bob's message,
 m , signed
(encrypted) with
his private key

Digital Signatures (more)

- suppose Alice receives msg m , digital signature $K_B^-(m)$
- Alice verifies m signed by Bob by applying Bob's public key K_B^+ to $K_B^-(m)$ then checks $K_B^+(K_B^-(m)) = m$.
- if $K_B^+(K_B^-(m)) = m$, whoever signed m must have used Bob's private key.

Alice thus verifies that:

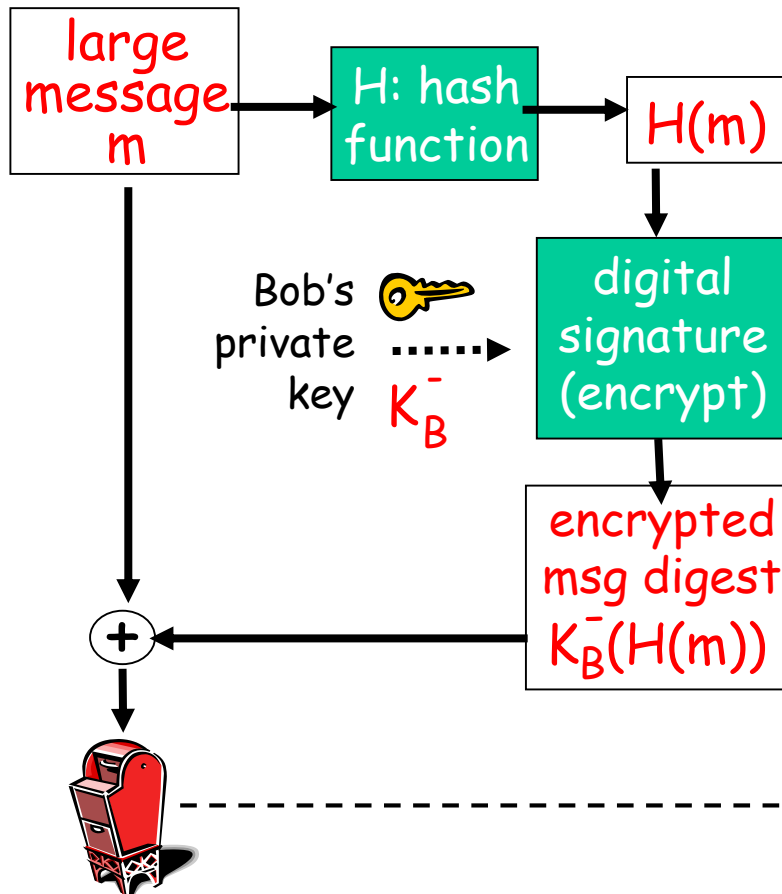
- ✓ Bob signed m .
- ✓ No one else signed m .
- ✓ Bob signed m and not m' .

non-repudiation:

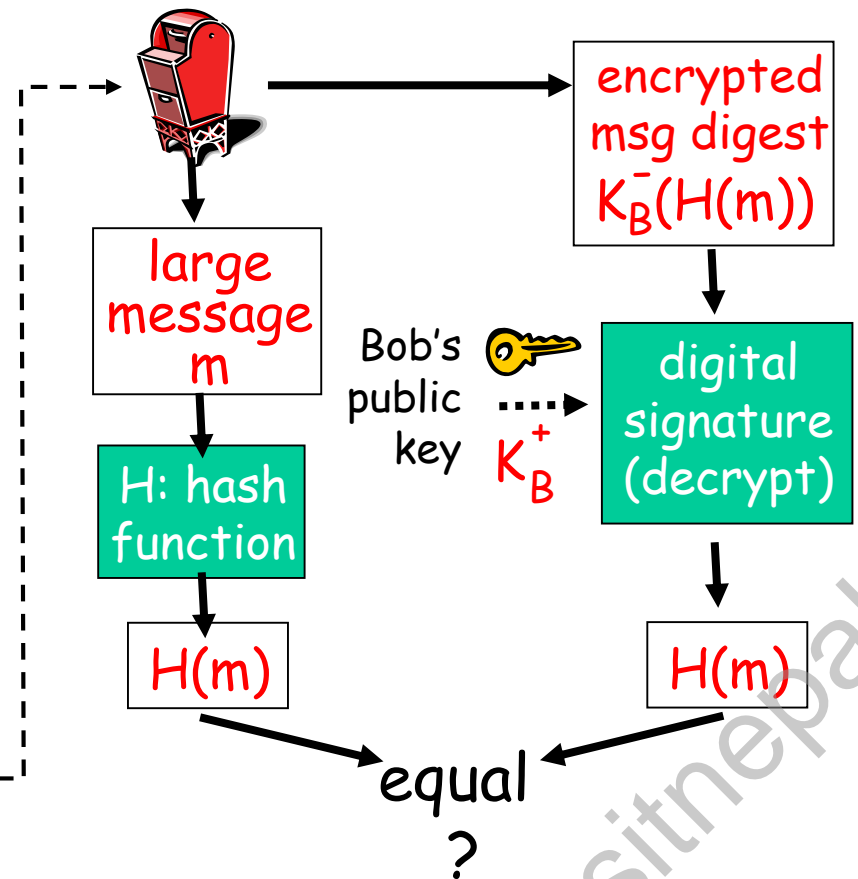
- ✓ Alice can take m , and signature $K_B^-(m)$ to court and prove that Bob signed m .

Digital signature = signed MAC

Bob sends digitally signed message:



Alice verifies signature and integrity of digitally signed message:



Public Key Certification

public key problem:

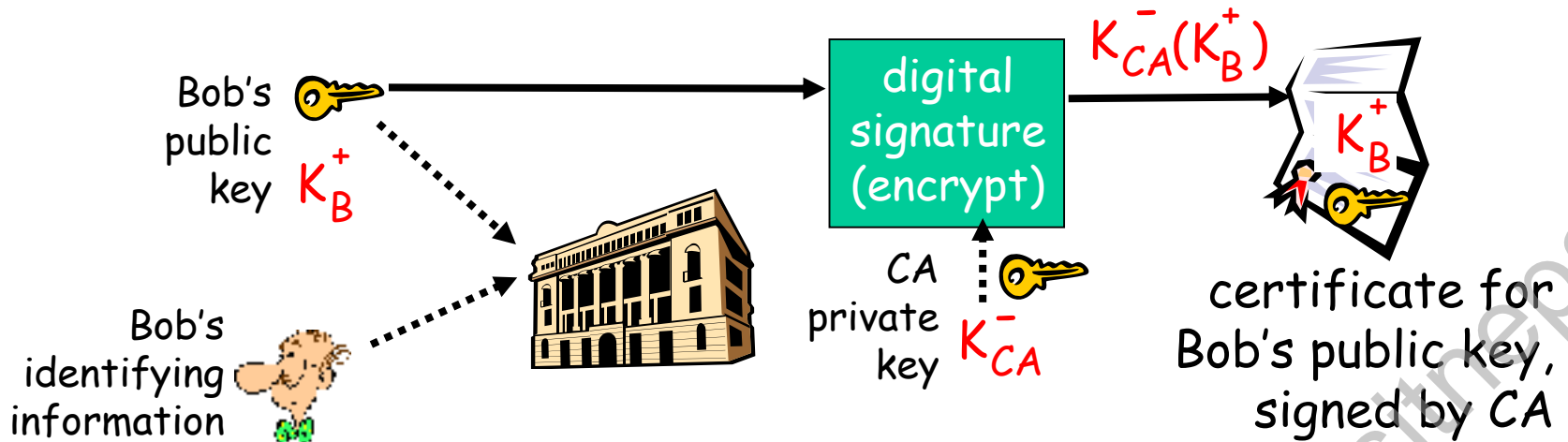
- When Alice obtains Bob's public key (from web site, e-mail, diskette), how does she *know* it is Bob's public key, not Trudy's?

solution:

- trusted certification authority (CA)

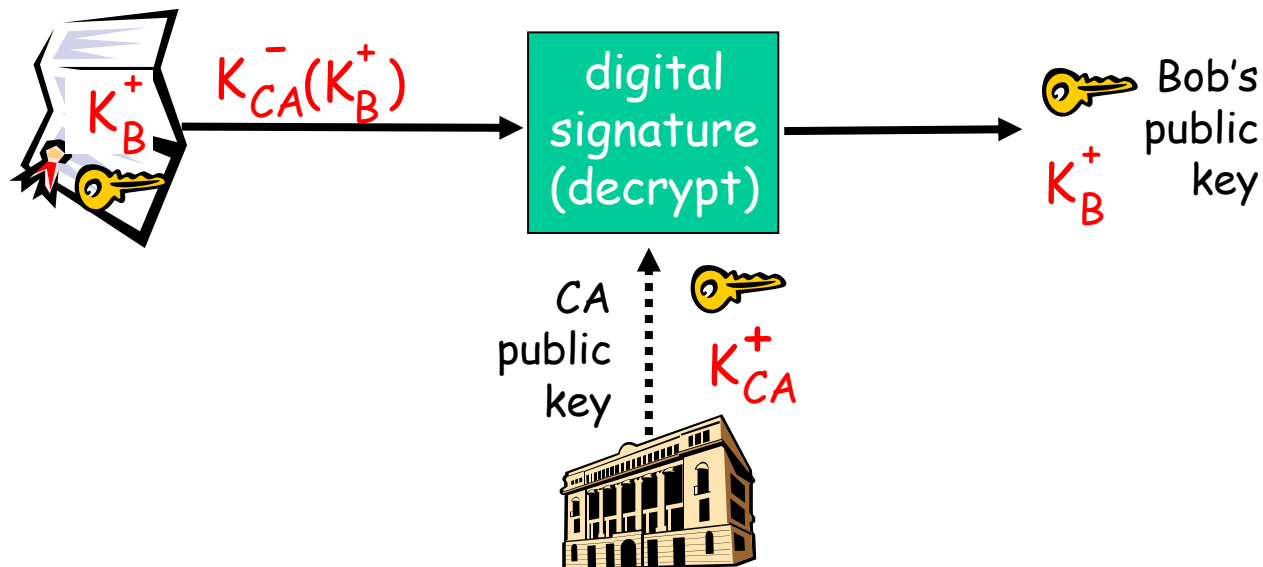
Certification Authorities

- ❑ **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."



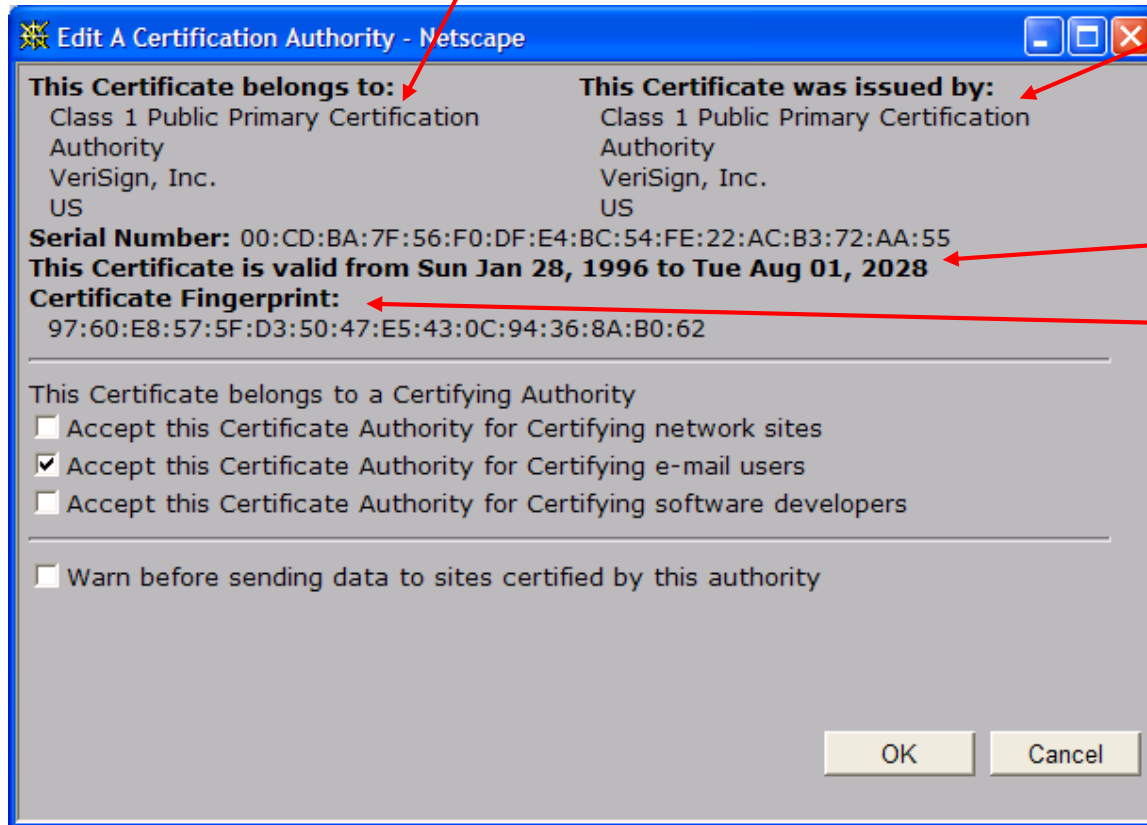
Certification Authorities

- 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



Chapter 8 roadmap

8.1 What is network security?

8.2 Principles of cryptography

8.3 Message integrity

8.4 End point authentication

8.5 Securing e-mail

8.6 Securing TCP connections: SSL

8.7 Network layer security: IPsec

8.8 Securing wireless LANs

8.9 Operational security: firewalls and IDS

Authentication

Goal: Bob wants Alice to “prove” her identity to him

Protocol ap1.0: Alice says “I am Alice”



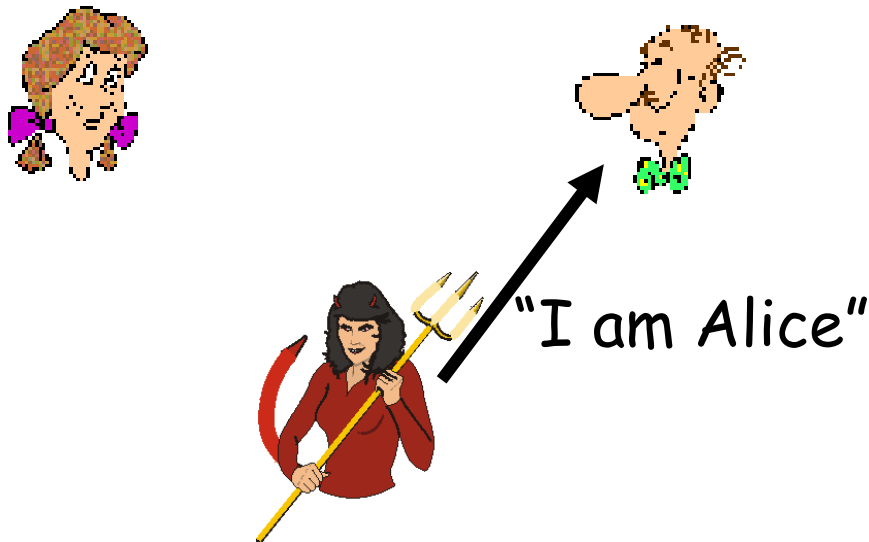
Failure scenario??



Authentication

Goal: Bob wants Alice to “prove” her identity to him

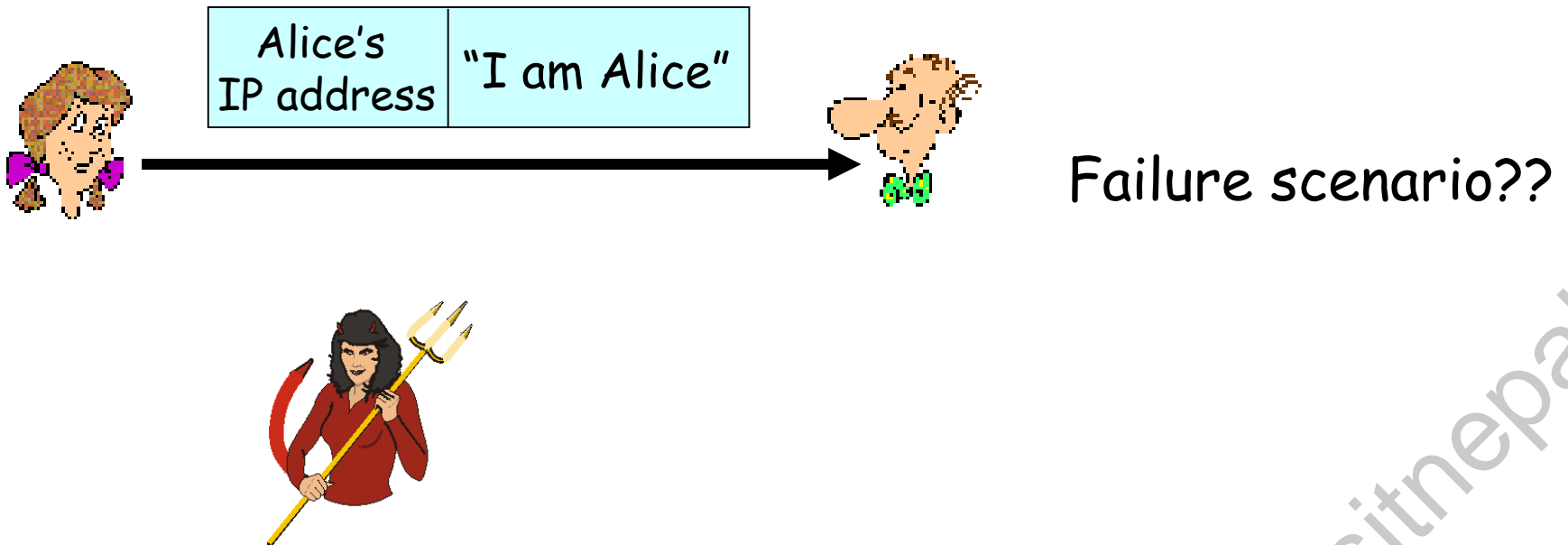
Protocol ap1.0: Alice says “I am Alice”



in a network,
Bob can not “see”
Alice, so Trudy simply
declares
herself to be Alice

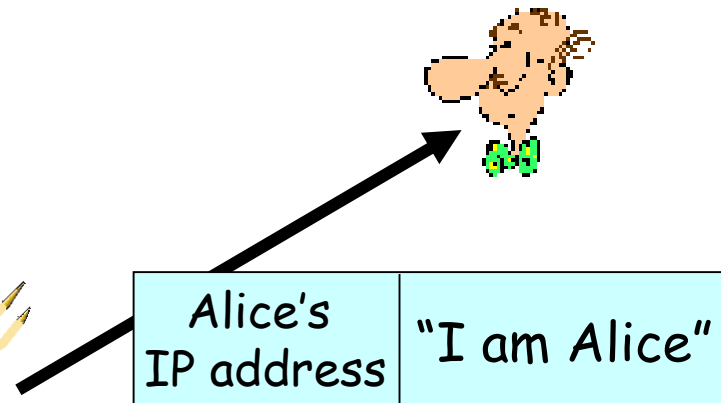
Authentication: another try

Protocol ap2.0: Alice says "I am Alice" in an IP packet containing her source IP address



Authentication: another try

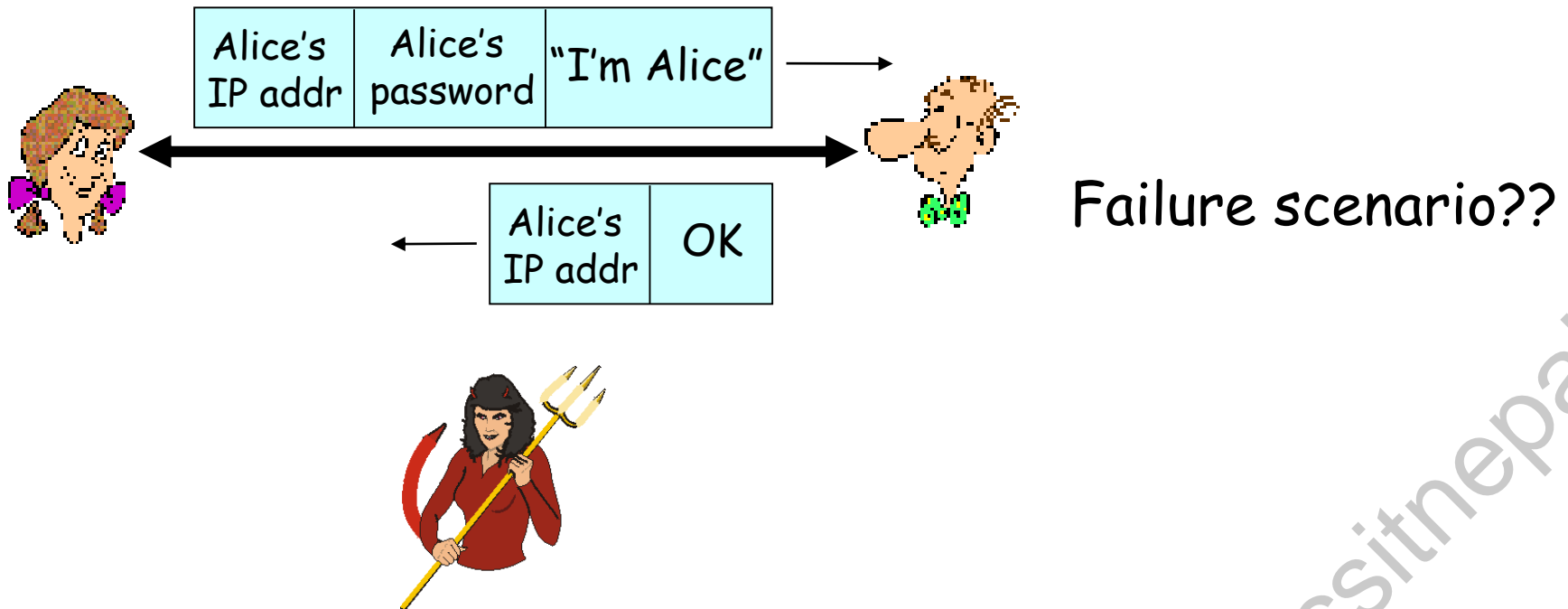
Protocol ap2.0: Alice says "I am Alice" in an IP packet containing her source IP address



Trudy can create a packet "spoofing" Alice's address

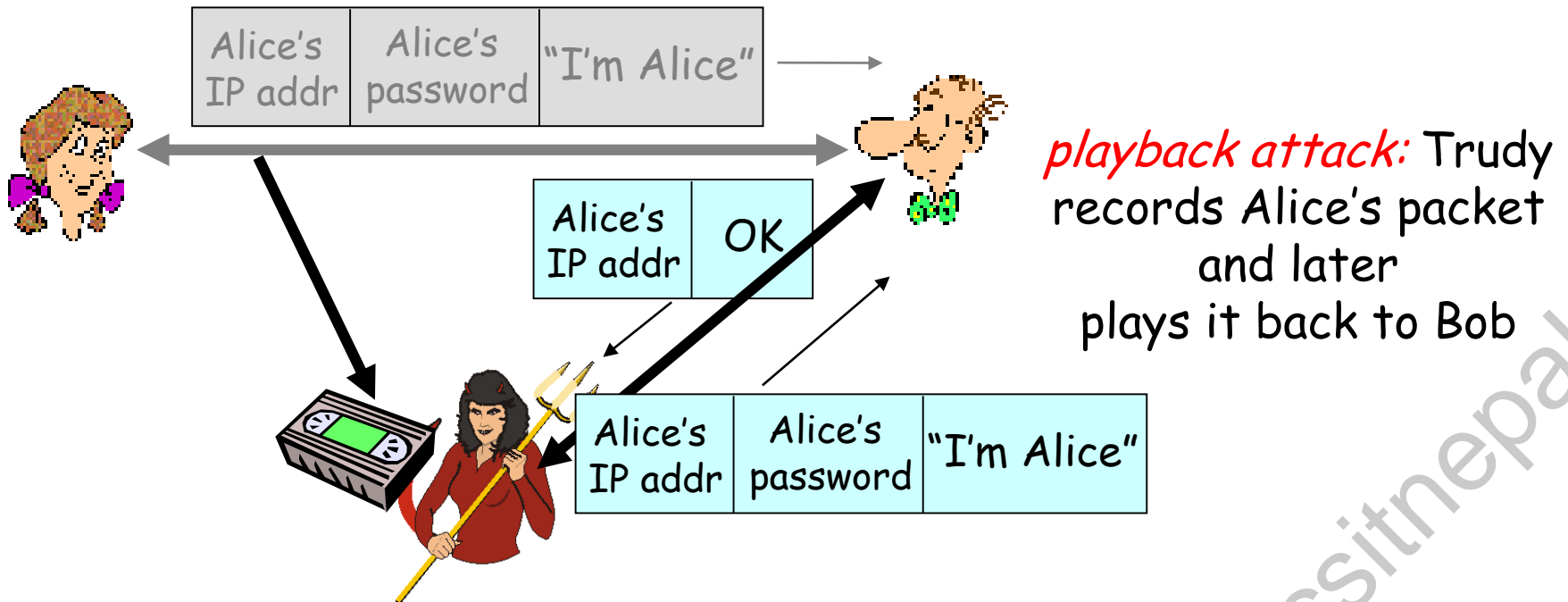
Authentication: another try

Protocol ap3.0: Alice says "I am Alice" and sends her secret password to "prove" it.



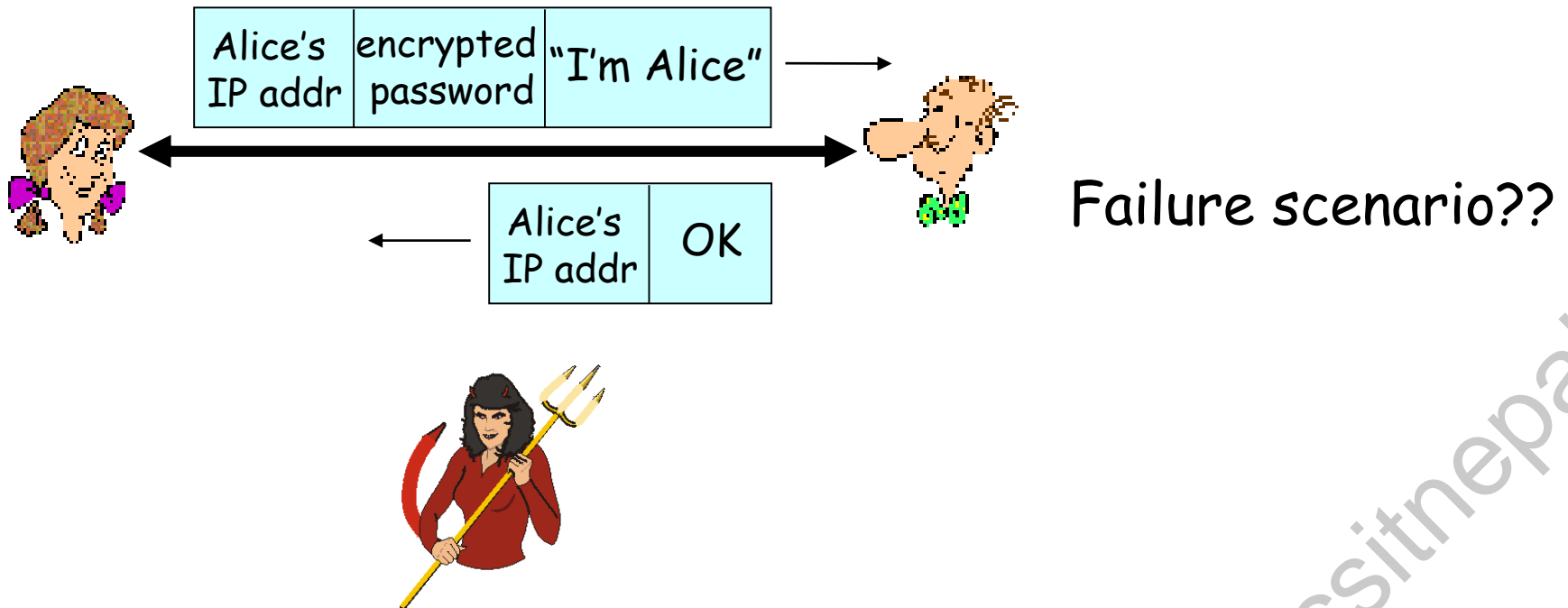
Authentication: another try

Protocol ap3.0: Alice says "I am Alice" and sends her secret password to "prove" it.



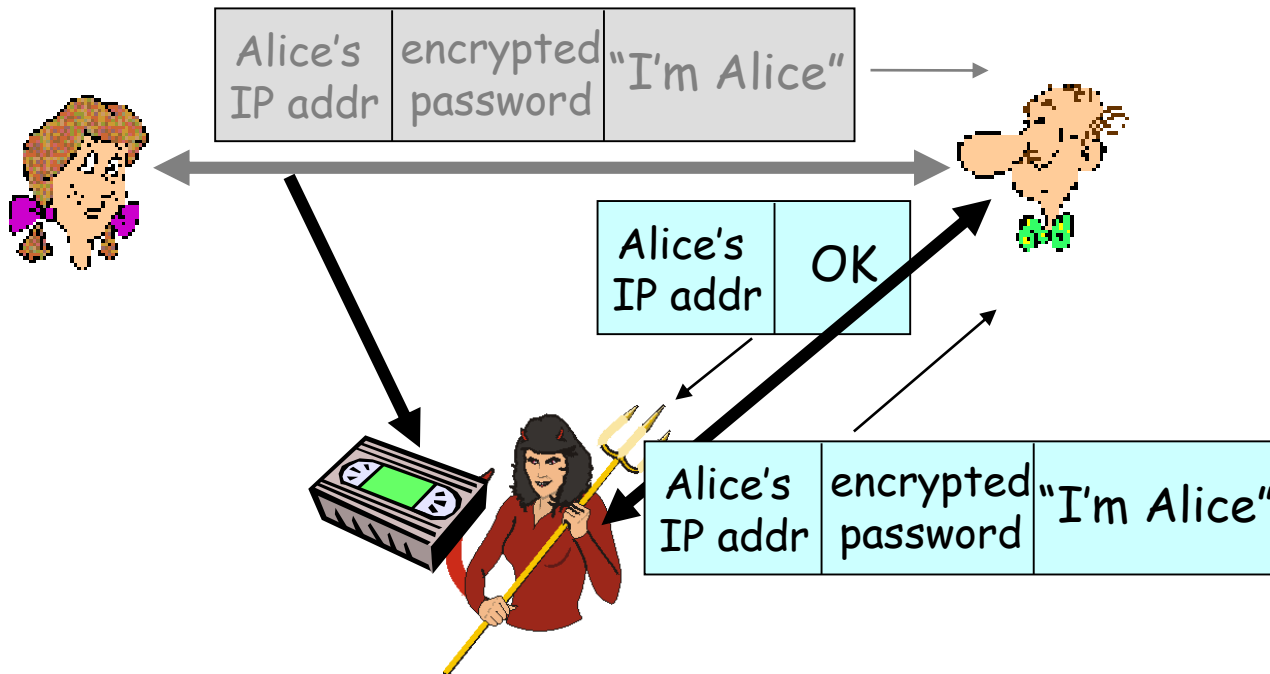
Authentication: yet another try

Protocol ap3.1: Alice says "I am Alice" and sends her *encrypted* secret password to "prove" it.



Authentication: another try

Protocol ap3.1: Alice says "I am Alice" and sends her *encrypted* secret password to "prove" it.



record
and
playback
still works!

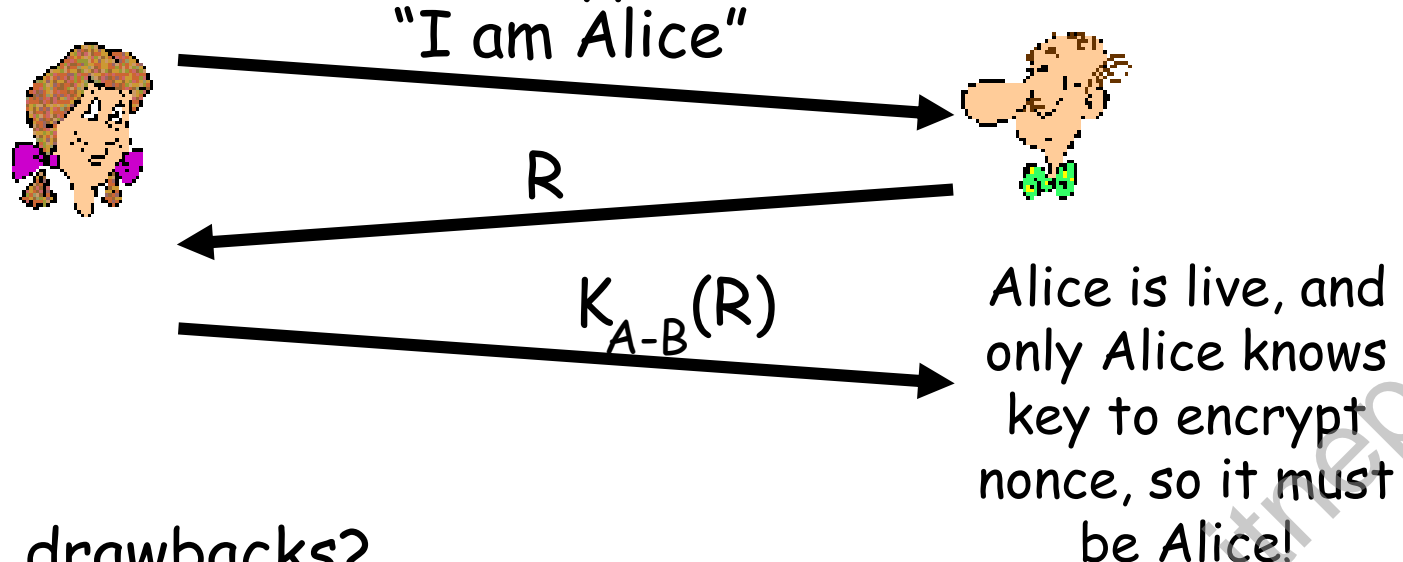
Authentication: yet another try

Goal: avoid playback attack

Nonce: number (R) used only *once -in-a-lifetime*

ap4.0: to prove Alice "live", Bob sends Alice **nonce**, R. Alice

must return R, encrypted with shared secret key



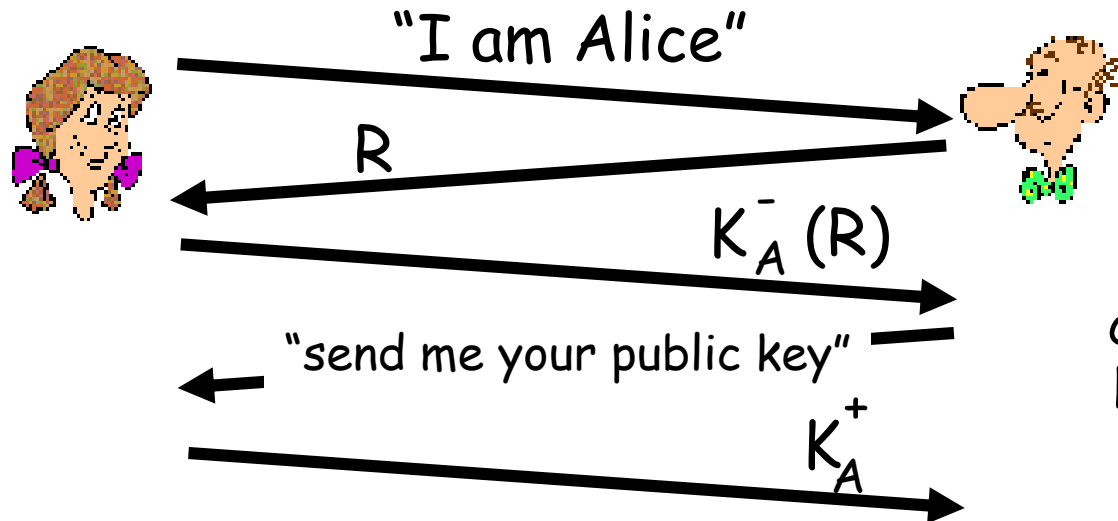
Failures, drawbacks?

Authentication: ap5.0

ap4.0 requires shared symmetric key

□ can we authenticate using public key techniques?

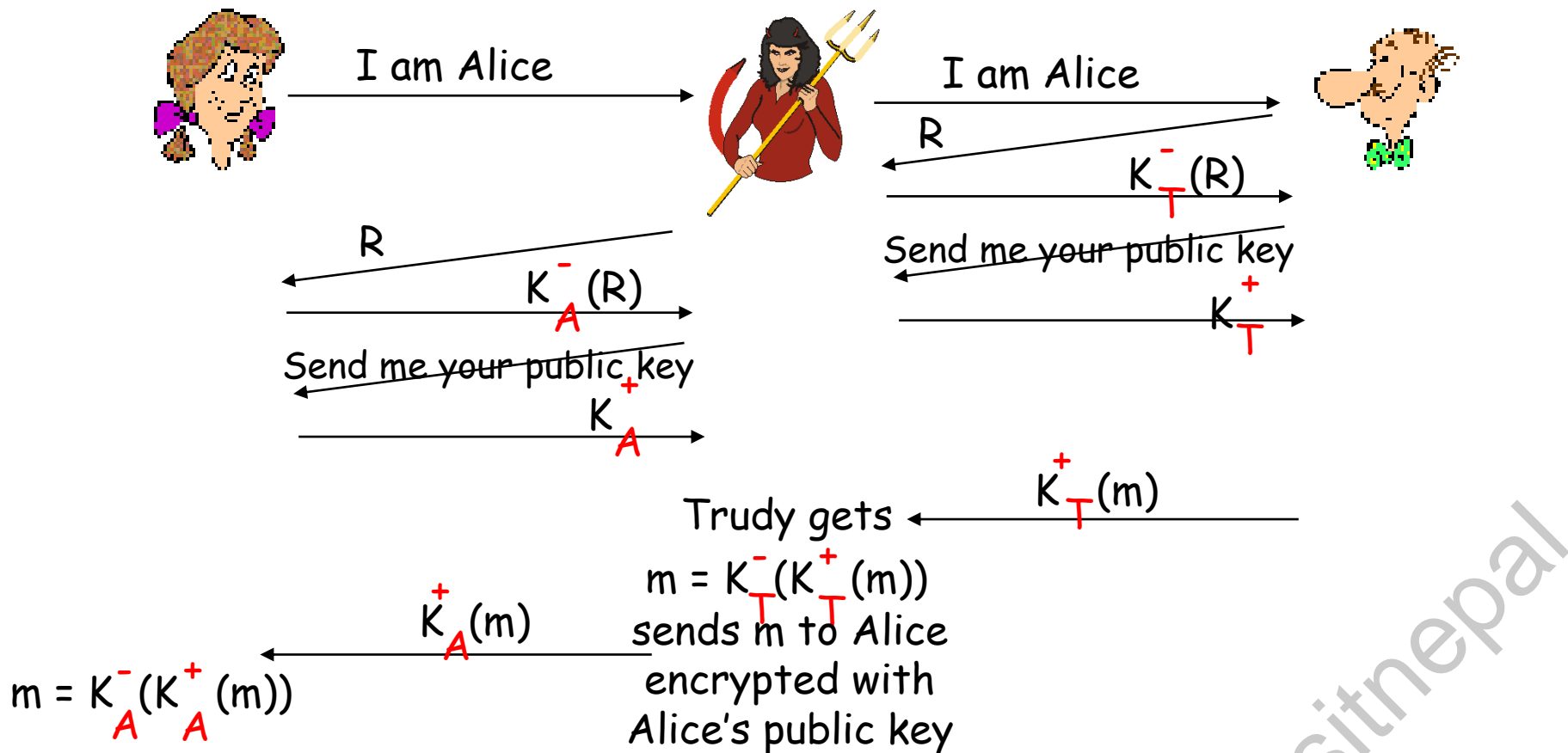
ap5.0: use nonce, public key cryptography



Bob computes
 $K_A^+(K_A^-(R)) = R$
and knows only Alice
could have the private
key, that encrypted R
such that
 $K_A^+(K_A^-(R)) = R$

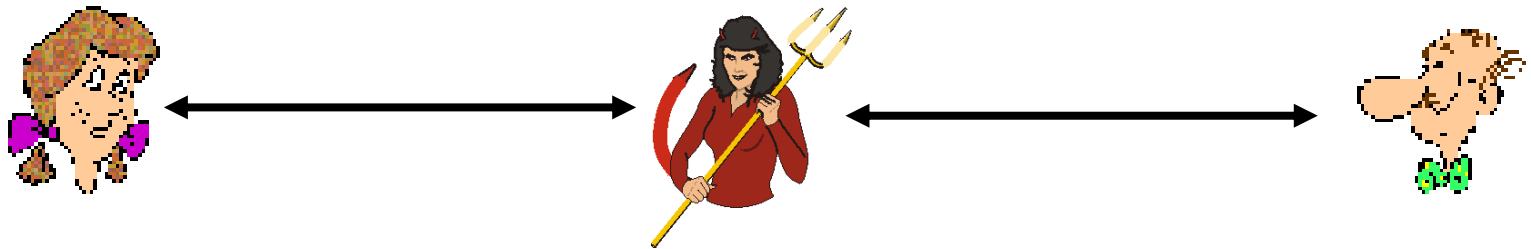
ap5.0: security hole

Man (woman) in the middle attack: Trudy poses as Alice (to Bob) and as Bob (to Alice)



ap5.0: security hole

Man (woman) in the middle attack: Trudy poses as Alice (to Bob) and as Bob (to Alice)



Difficult to detect:

- ❑ Bob receives everything that Alice sends, and vice versa. (e.g., so Bob, Alice can meet one week later and recall conversation)
- ❑ problem is that Trudy receives all messages as well!

Chapter 8 roadmap

8.1 What is network security?

8.2 Principles of cryptography

8.3 Message integrity

8.4 End point authentication

8.5 Securing e-mail

8.6 Securing TCP connections: SSL

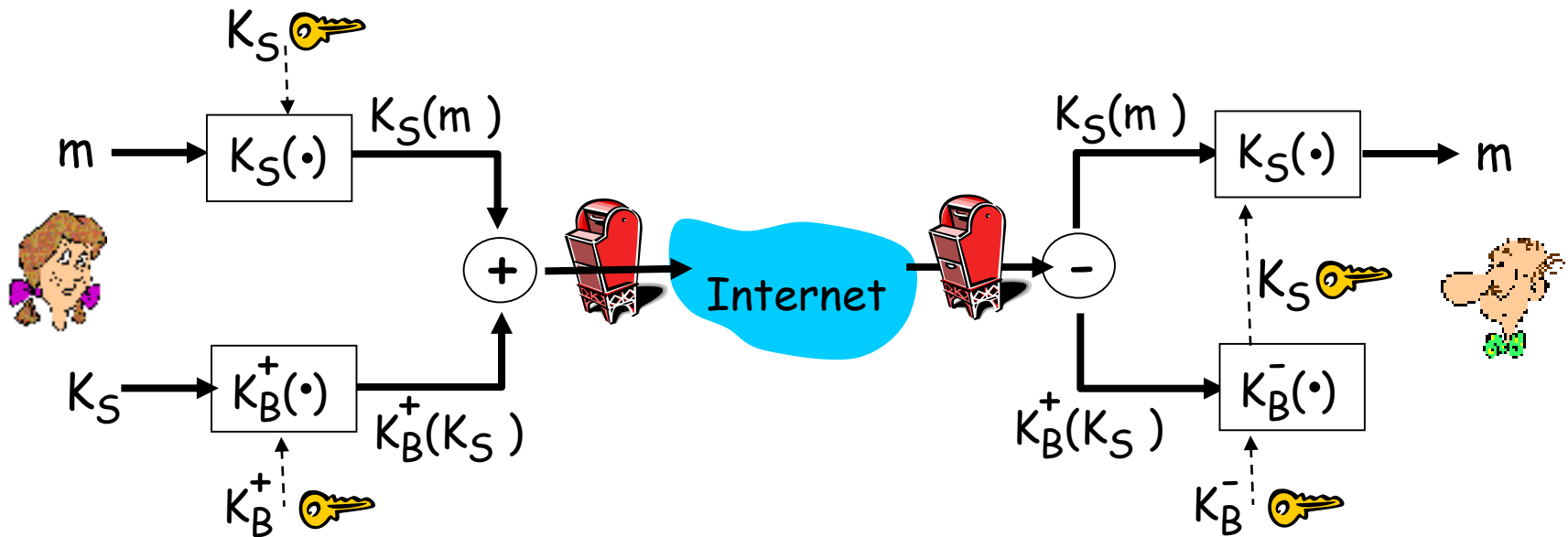
8.7 Network layer security: IPsec

8.8 Securing wireless LANs

8.9 Operational security: firewalls and IDS

Secure e-mail

- Alice wants to send confidential e-mail, m , to Bob.

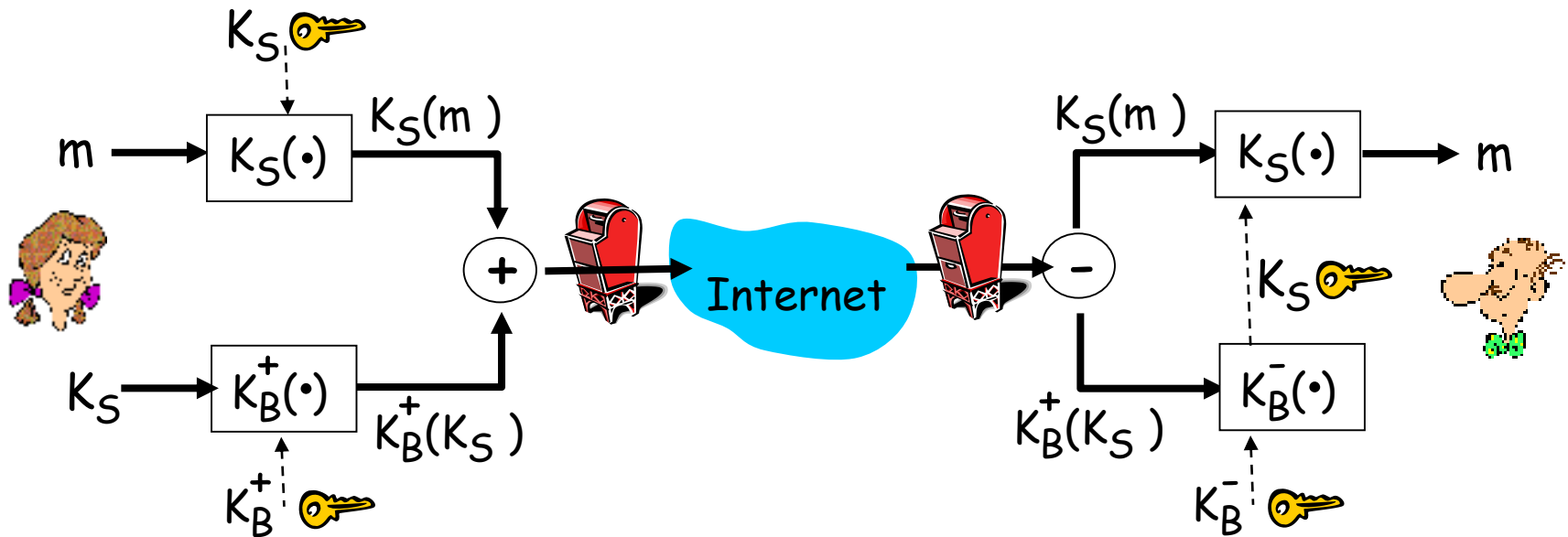


Alice:

- generates random *symmetric* private key, K_S .
- encrypts message with K_S (for efficiency)
- also encrypts K_S with Bob's public key.
- sends both $K_S(m)$ and $K_B(K_S)$ to Bob.

Secure e-mail

- Alice wants to send confidential e-mail, m , to Bob.

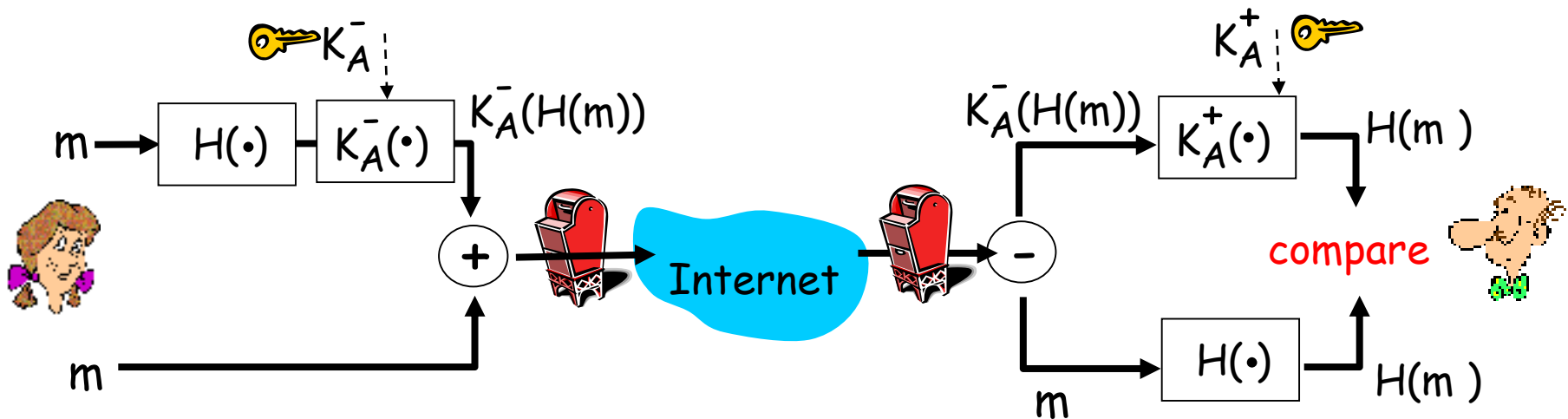


Bob:

- uses his private key to decrypt and recover K_S
- uses K_S to decrypt $K_S(m)$ to recover m

Secure e-mail (continued)

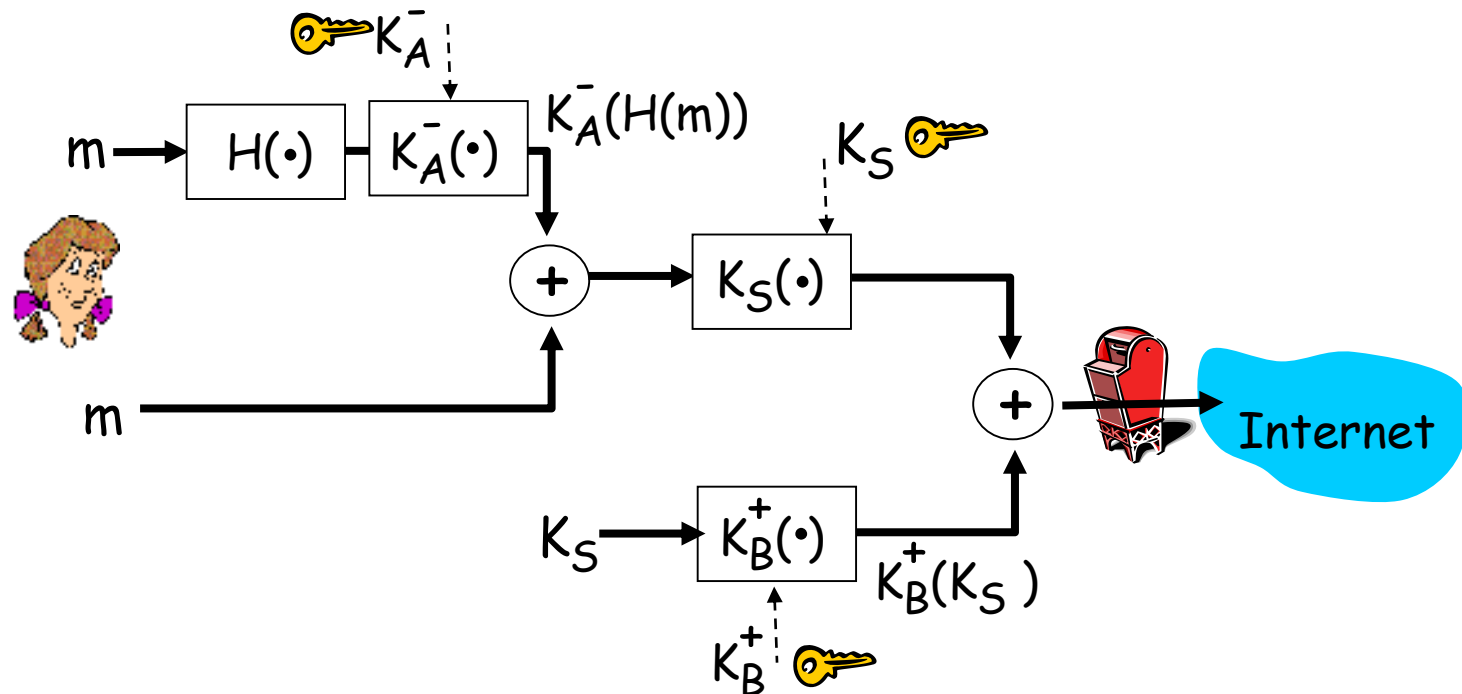
- Alice wants to provide sender authentication message integrity.



- Alice digitally signs message.
- sends both message (in the clear) and digital signature.

Secure e-mail (continued)

- 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)

- ❑ Internet e-mail encryption scheme, de-facto standard.
- ❑ uses symmetric key cryptography, public key cryptography, hash function, and digital signature as described.
- ❑ provides secrecy, sender authentication, integrity.
- ❑ inventor, Phil Zimmerman, was target of 3-year federal investigation.

A PGP signed message:

```
---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---
```


Chapter 8 roadmap

8.1 What is network security?

8.2 Principles of cryptography

8.3 Message integrity

8.4 End point authentication

8.5 Securing e-mail

8.6 Securing TCP connections: SSL

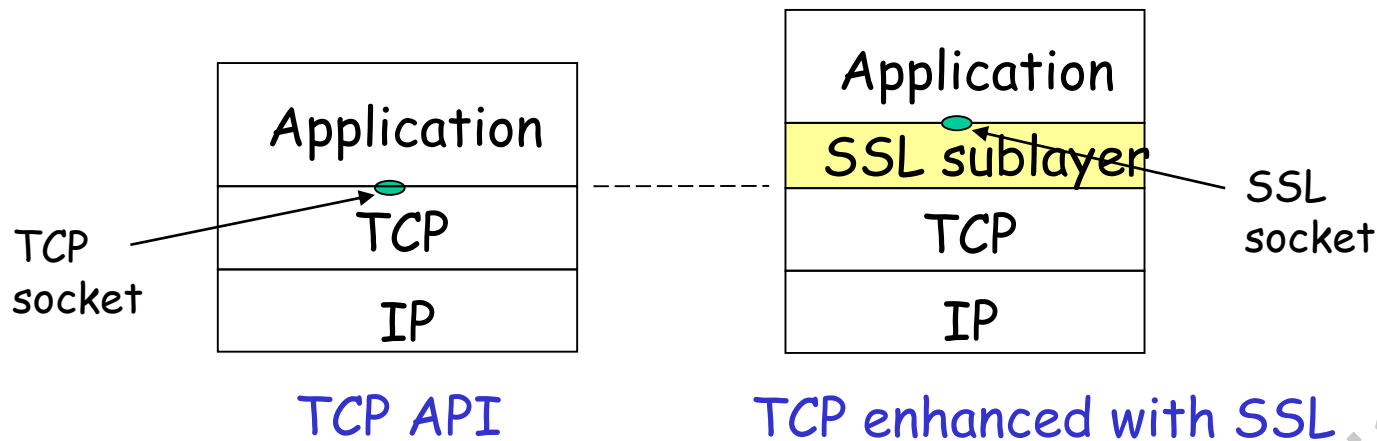
8.7 Network layer security: IPsec

8.8 Securing wireless LANs

8.9 Operational security: firewalls and IDS

Secure sockets layer (SSL)

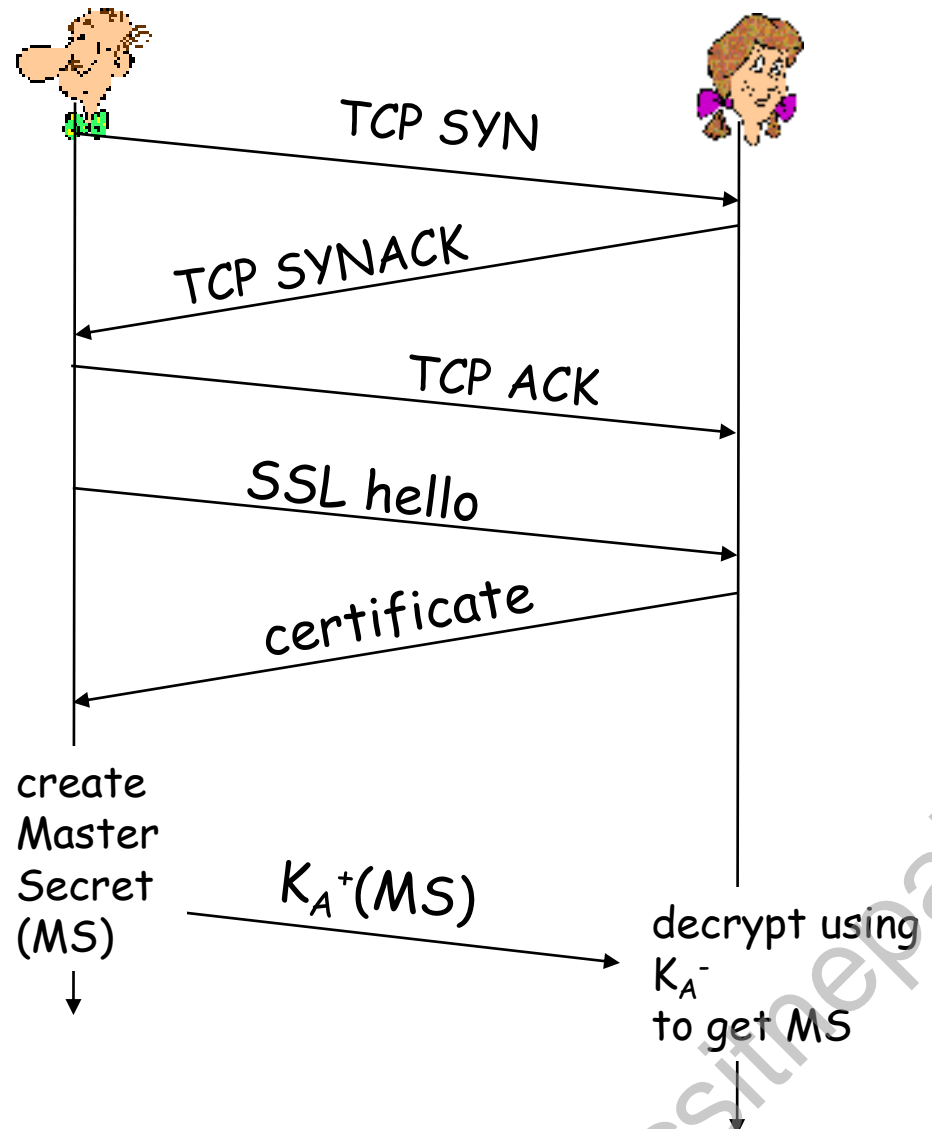
- ❑ provides transport layer security to any TCP-based application using SSL services.
 - e.g., between Web browsers, servers for e-commerce (shttp)
- ❑ security services:
 - server authentication, data encryption, client authentication (optional)



SSL: three phases

1. Handshake:

- ❑ Bob establishes TCP connection to Alice
- ❑ authenticates Alice via CA signed certificate
- ❑ creates, encrypts (using Alice's public key), sends master secret key to Alice
 - nonce exchange not shown



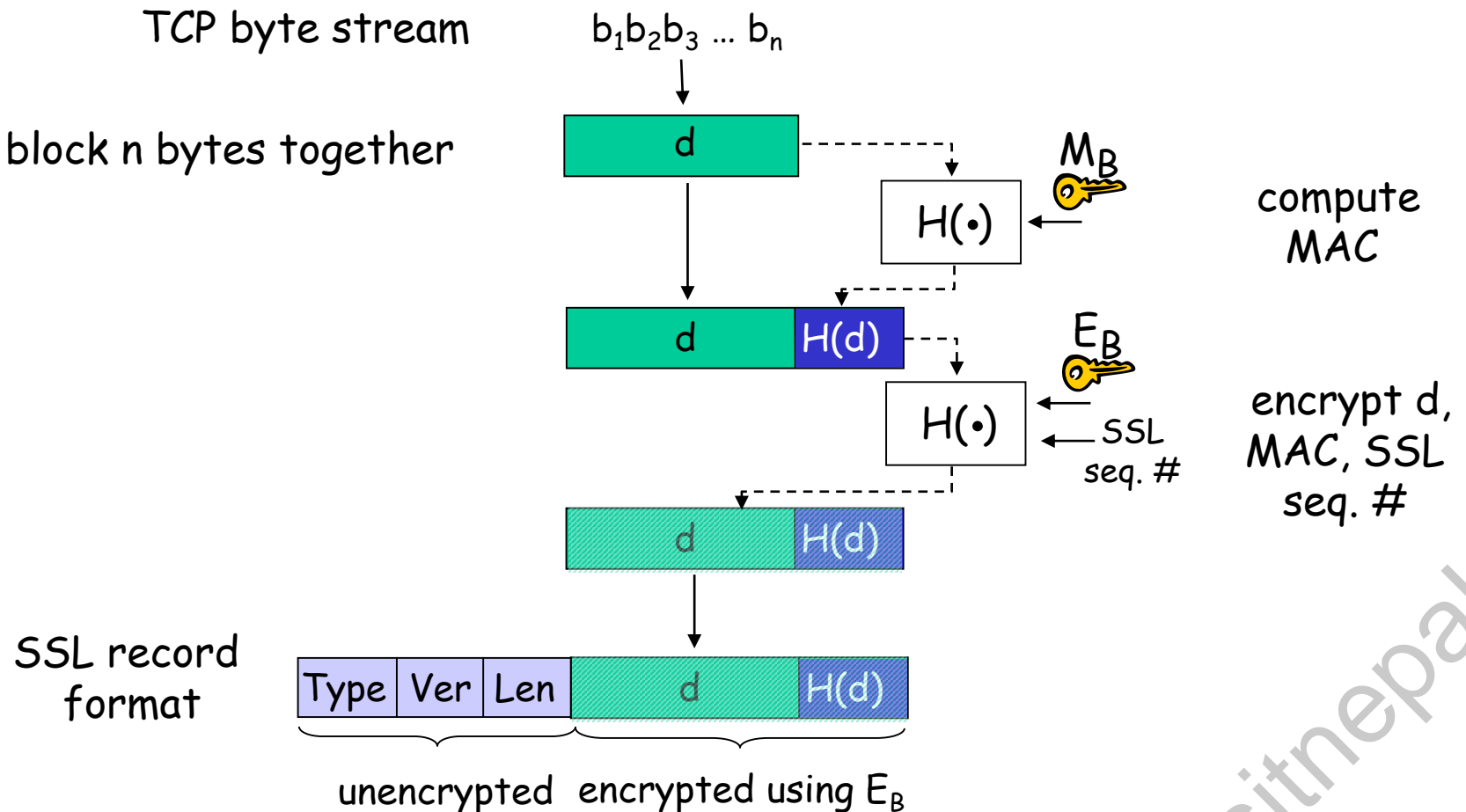
SSL: three phases

2. Key Derivation:

- ❑ Alice, Bob use shared secret (MS) to generate 4 keys:
 - E_B : Bob→Alice data encryption key
 - E_A : Alice→Bob data encryption key
 - M_B : Bob→Alice MAC key
 - M_A : Alice→Bob MAC key
- ❑ encryption and MAC algorithms negotiable between Bob, Alice
- ❑ why 4 keys?

SSL: three phases

3. Data transfer



Chapter 8 roadmap

8.1 What is network security?

8.2 Principles of cryptography

8.3 Message integrity

8.4 End point authentication

8.5 Securing e-mail

8.6 Securing TCP connections: SSL

8.7 Network layer security: IPsec

8.8 Securing wireless LANs

8.9 Operational security: firewalls and IDS

IPsec: Network Layer Security

- ❑ network-layer secrecy:
 - sending host encrypts the data in IP datagram
 - TCP and UDP segments; ICMP and SNMP messages.
- ❑ network-layer authentication
 - destination host can authenticate source IP address
- ❑ two principal protocols:
 - authentication header (AH) protocol
 - encapsulation security payload (ESP) protocol
- ❑ for both AH and ESP, source, destination handshake:
 - create network-layer logical channel called a security association (SA)
- ❑ each SA unidirectional.
- ❑ uniquely determined by:
 - security protocol (AH or ESP)
 - source IP address
 - 32-bit connection ID

Authentication Header (AH) Protocol

- ❑ provides source authentication, data integrity, no confidentiality
- ❑ AH header inserted between IP header, data field.
- ❑ protocol field: 51
- ❑ intermediate routers process datagrams as usual

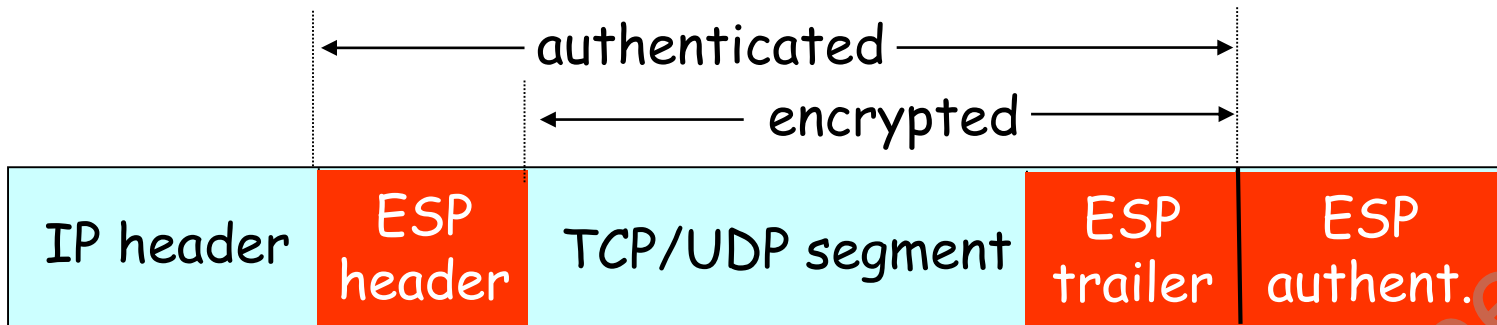
AH header includes:

- ❑ connection identifier
- ❑ authentication data: source- signed message digest calculated over original IP datagram.
- ❑ next header field: specifies type of data (e.g., TCP, UDP, ICMP)



ESP Protocol

- ❑ provides secrecy, host authentication, data integrity.
- ❑ data, ESP trailer encrypted.
- ❑ next header field is in ESP trailer.
- ❑ ESP authentication field is similar to AH authentication field.
- ❑ Protocol = 50.



Chapter 8 roadmap

8.1 What is network security?

8.2 Principles of cryptography

8.3 Message integrity

8.4 End point authentication

8.5 Securing e-mail

8.6 Securing TCP connections: SSL

8.7 Network layer security: IPsec

8.8 Securing wireless LANs

8.9 Operational security: firewalls and IDS

IEEE 802.11 security

- ❑ *war-driving*: drive around Bay area, see what 802.11 networks available?
 - More than 9000 accessible from public roadways
 - 85% use no encryption/authentication
 - packet-sniffing and various attacks easy!
- ❑ *securing 802.11*
 - encryption, authentication
 - first attempt at 802.11 security: Wired Equivalent Privacy (WEP): a failure
 - current attempt: 802.11i

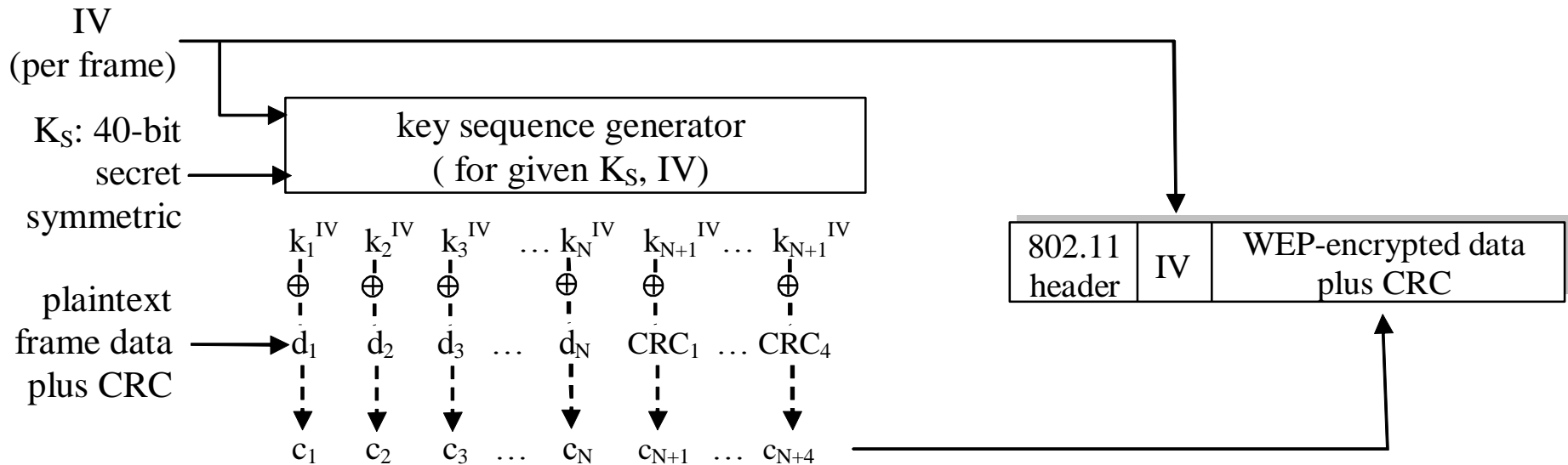
Wired Equivalent Privacy (WEP):

- ❑ authentication as in protocol *ap4.0*
 - host requests authentication from access point
 - access point sends 128 bit nonce
 - host encrypts nonce using shared symmetric key
 - access point decrypts nonce, authenticates host
- ❑ no key distribution mechanism
- ❑ authentication: knowing the shared key is enough

WEP data encryption

- ❑ host/AP share 40 bit symmetric key (semi-permanent)
- ❑ host appends 24-bit initialization vector (IV) to create 64-bit key
- ❑ 64 bit key used to generate stream of keys, k_i^{IV}
- ❑ k_i^{IV} used to encrypt ith byte, d_i , in frame:
$$c_i = d_i \text{ XOR } k_i^{IV}$$
- ❑ IV and encrypted bytes, c_i sent in frame

802.11 WEP encryption



Sender-side WEP encryption

Breaking 802.11 WEP encryption

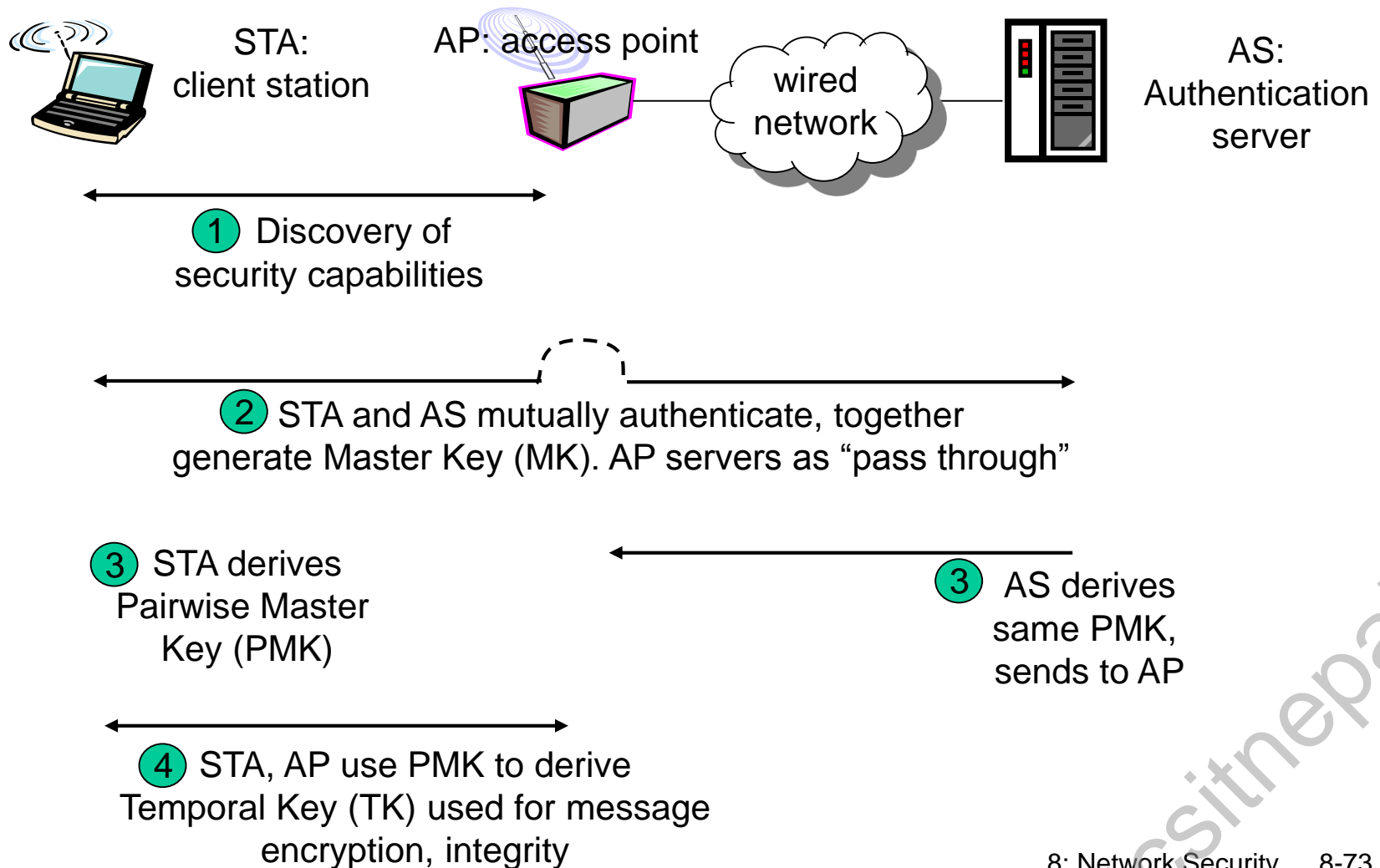
security hole:

- ❑ 24-bit IV, one IV per frame, -> IV's eventually reused
- ❑ IV transmitted in plaintext -> IV reuse detected
- ❑ **attack:**
 - Trudy causes Alice to encrypt known plaintext $d_1 d_2 d_3 d_4 \dots$
 - Trudy sees: $c_i = d_i \text{ XOR } k_i^{\text{IV}}$
 - Trudy knows $c_i d_i$, so can compute k_i^{IV}
 - Trudy knows encrypting key sequence $k_1^{\text{IV}} k_2^{\text{IV}} k_3^{\text{IV}} \dots$
 - Next time IV is used, Trudy can decrypt!

802.11i: improved security

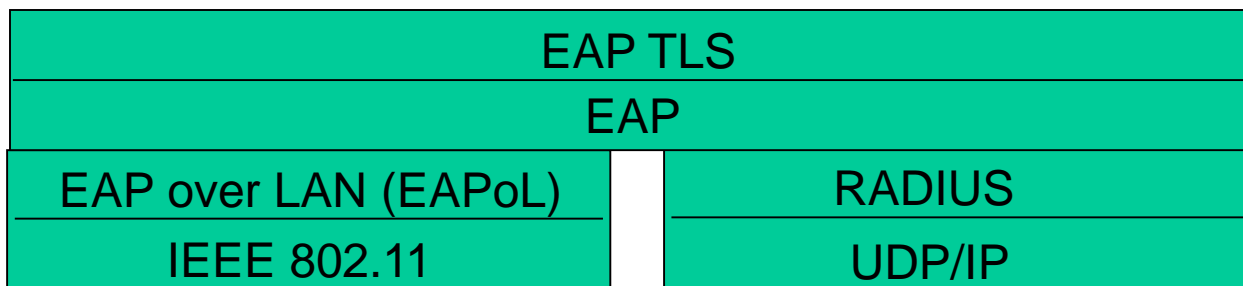
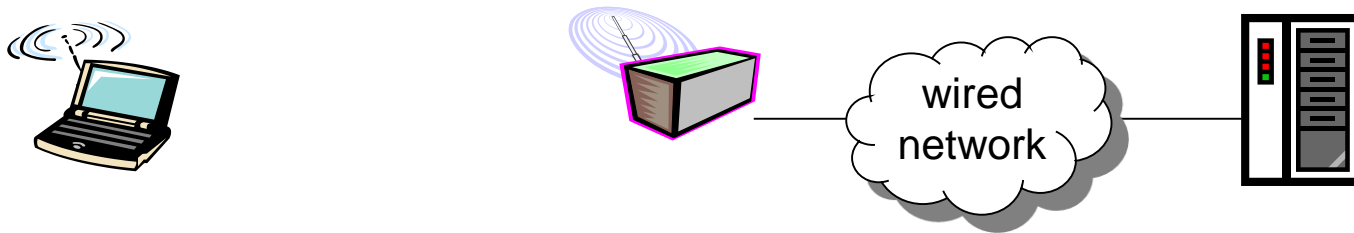
- ❑ numerous (stronger) forms of encryption possible
- ❑ provides key distribution
- ❑ uses authentication server separate from access point

802.11i: four phases of operation



EAP: extensible authentication protocol

- ❑ EAP: end-end client (mobile) to authentication server protocol
- ❑ EAP sent over separate "links"
 - mobile-to-AP (EAP over LAN)
 - AP to authentication server (RADIUS over UDP)



Chapter 8 roadmap

8.1 What is network security?

8.2 Principles of cryptography

8.3 Message integrity

8.4 End point authentication

8.5 Securing e-mail

8.6 Securing TCP connections: SSL

8.7 Network layer security: IPsec

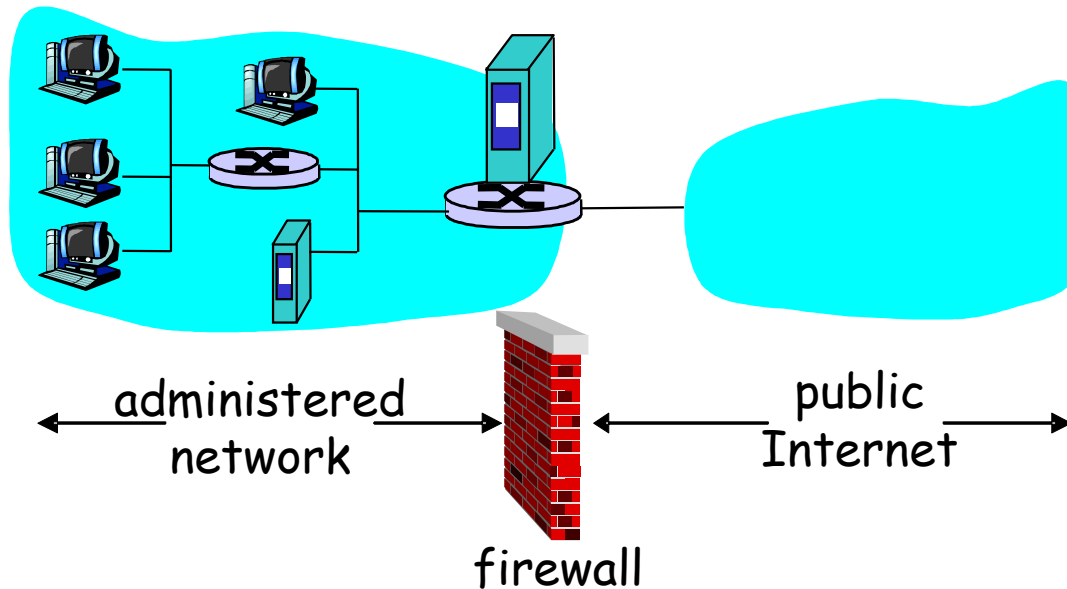
8.8 Securing wireless LANs

8.9 Operational security: firewalls and IDS

Firewalls

firewall

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



Firewalls: Why

prevent denial of service attacks:

- SYN flooding: attacker establishes many bogus TCP connections, no resources left for “real” connections

prevent illegal modification/access of internal data.

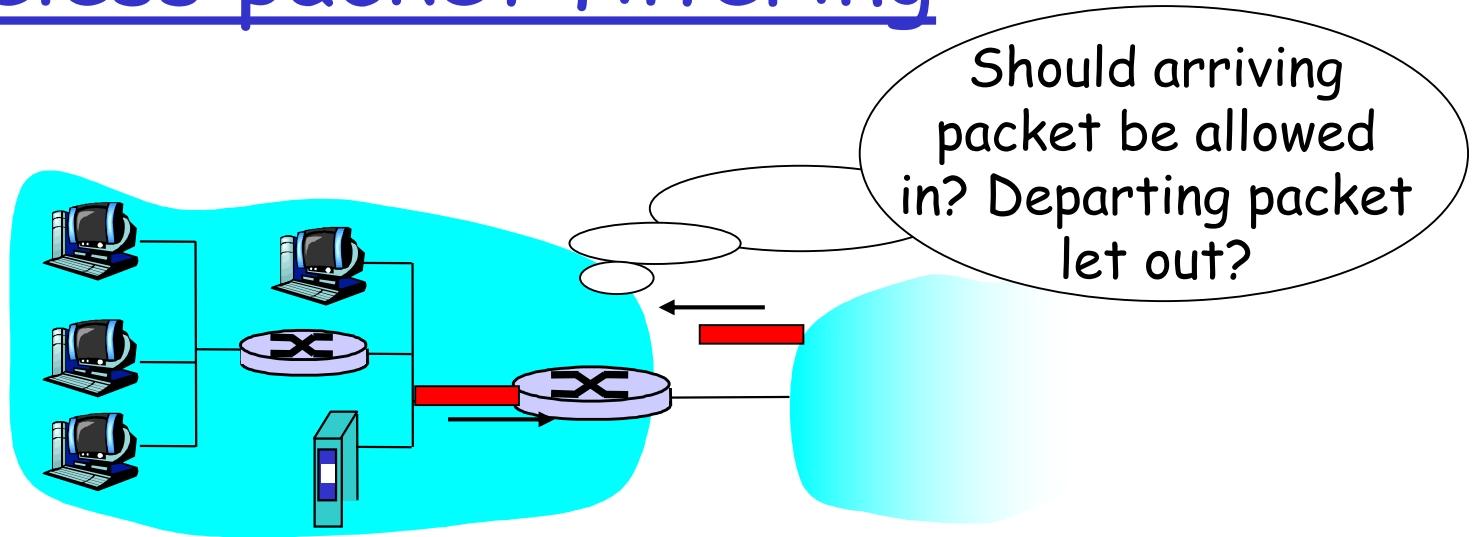
- e.g., attacker replaces CIA's homepage with something else

allow only authorized access to inside network (set of authenticated users/hosts)

three types of firewalls:

- stateless packet filters
- stateful packet filters
- application gateways

Stateless packet filtering



- ❑ internal network connected to Internet via **router firewall**
- ❑ router **filters packet-by-packet**, decision to forward/drop packet based on:
 - source IP address, destination IP address
 - TCP/UDP source and destination port numbers
 - ICMP message type
 - TCP SYN and ACK bits

Stateless packet filtering: example

- ❑ example 1: block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23.
 - all incoming, outgoing UDP flows and telnet connections are blocked.
- ❑ example 2: Block inbound TCP segments with ACK=0.
 - prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

Stateless packet filtering: more examples

| <u>Policy</u> | <u>Firewall Setting</u> |
|---|---|
| No outside Web access. | Drop all outgoing packets to any IP address, port 80 |
| No incoming TCP connections, except those for institution's public Web server only. | Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80 |
| Prevent Web-radios from eating up the available bandwidth. | Drop all incoming UDP packets - except DNS and router broadcasts. |
| Prevent your network from being used for a smurf DoS attack. | Drop all ICMP packets going to a "broadcast" address (eg 130.207.255.255). |
| Prevent your network from being tracerouted | Drop all outgoing ICMP TTL expired traffic |

Access Control Lists

- **ACL**: table of rules, applied top to bottom to incoming packets: (action, condition) pairs

| action | source address | dest address | protocol | source port | dest port | flag bit |
|--------|----------------------|----------------------|----------|-------------|-----------|----------|
| allow | 222.22/16 | outside of 222.22/16 | TCP | > 1023 | 80 | any |
| allow | outside of 222.22/16 | 222.22/16 | TCP | 80 | > 1023 | ACK |
| allow | 222.22/16 | outside of 222.22/16 | UDP | > 1023 | 53 | --- |
| allow | outside of 222.22/16 | 222.22/16 | UDP | 53 | > 1023 | ---- |
| deny | all | all | all | all | all | all |

Stateful packet filtering

- ❑ stateless packet filter: heavy handed tool
 - admits packets that "make no sense," e.g., dest port = 80, ACK bit set, even though no TCP connection established:

| action | source address | dest address | protocol | source port | dest port | flag bit |
|--------|----------------------|--------------|----------|-------------|-----------|----------|
| allow | outside of 222.22/16 | 222.22/16 | TCP | 80 | > 1023 | ACK |

- ❑ *stateful packet filter*: track status of every TCP connection
 - track connection setup (SYN), teardown (FIN): can determine whether incoming, outgoing packets "makes sense"
 - timeout inactive connections at firewall: no longer admit packets

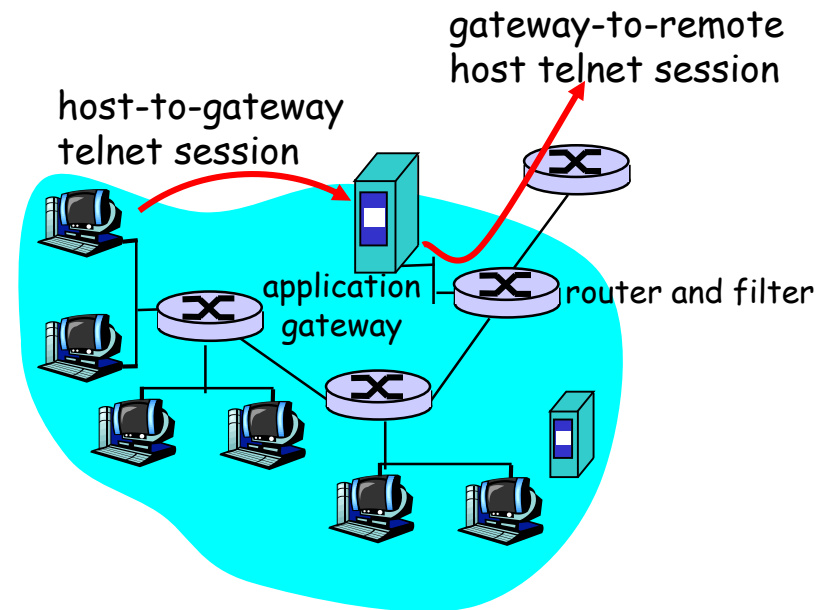
Stateful packet filtering

- ACL augmented to indicate need to check connection state table before admitting packet

| action | source address | dest address | proto | source port | dest port | flag bit | check conxion |
|--------|----------------------|----------------------|-------|-------------|-----------|----------|---------------|
| allow | 222.22/16 | outside of 222.22/16 | TCP | > 1023 | 80 | any | |
| allow | outside of 222.22/16 | 222.22/16 | TCP | 80 | > 1023 | ACK | × |
| allow | 222.22/16 | outside of 222.22/16 | UDP | > 1023 | 53 | --- | |
| allow | outside of 222.22/16 | 222.22/16 | UDP | 53 | > 1023 | ---- | × |
| deny | all | all | all | all | all | all | |

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.

Limitations of firewalls and gateways

- ❑ IP spoofing: router can't know if data "really" comes from claimed source
- ❑ if multiple app's. need special treatment, each has own app. gateway.
- ❑ client software must know how to contact gateway.
 - e.g., must set IP address of proxy in Web browser
- ❑ filters often use all or nothing policy for UDP.
- ❑ tradeoff: **degree of communication with outside world, level of security**
- ❑ many highly protected sites still suffer from attacks.

Intrusion detection systems

❑ packet filtering:

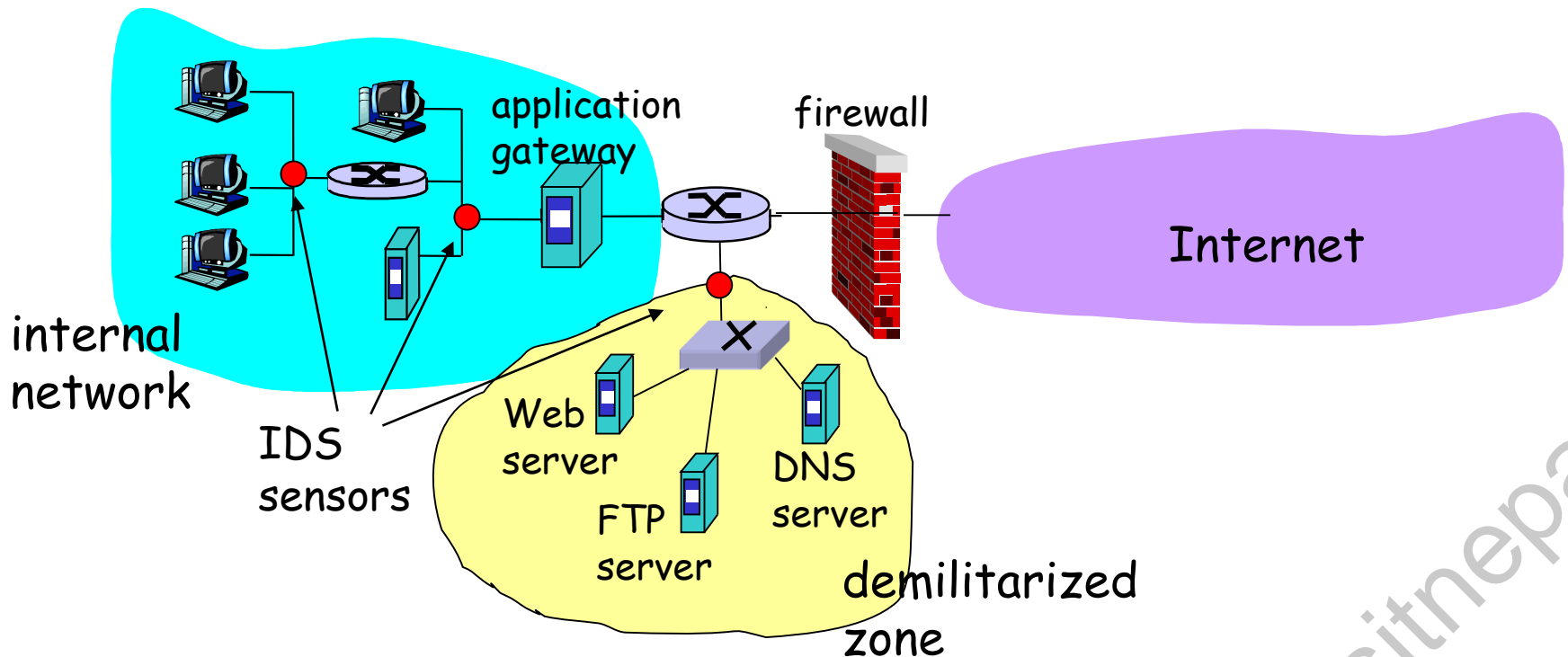
- operates on TCP/IP headers only
- no correlation check among sessions

❑ *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

Intrusion detection systems

- multiple IDSs: different types of checking at different locations



Network Security (summary)

Basic techniques.....

- cryptography (symmetric and public)
- message integrity
- end-point authentication

.... used in many different security scenarios

- secure email
- secure transport (SSL)
- IP sec
- 802.11

Operational Security: firewalls and IDS