USC Viterbi
School of Engineering

Overview of Network Security

EE450: Introduction to Computer Networks

Professor A. Zahid

USC

Outline

- What is network security?
- Principles of cryptography
- Authentication
- Integrity
- Key Distribution and certification
- Access control: firewalls
- Attacks and counter measures
- Security in many layers

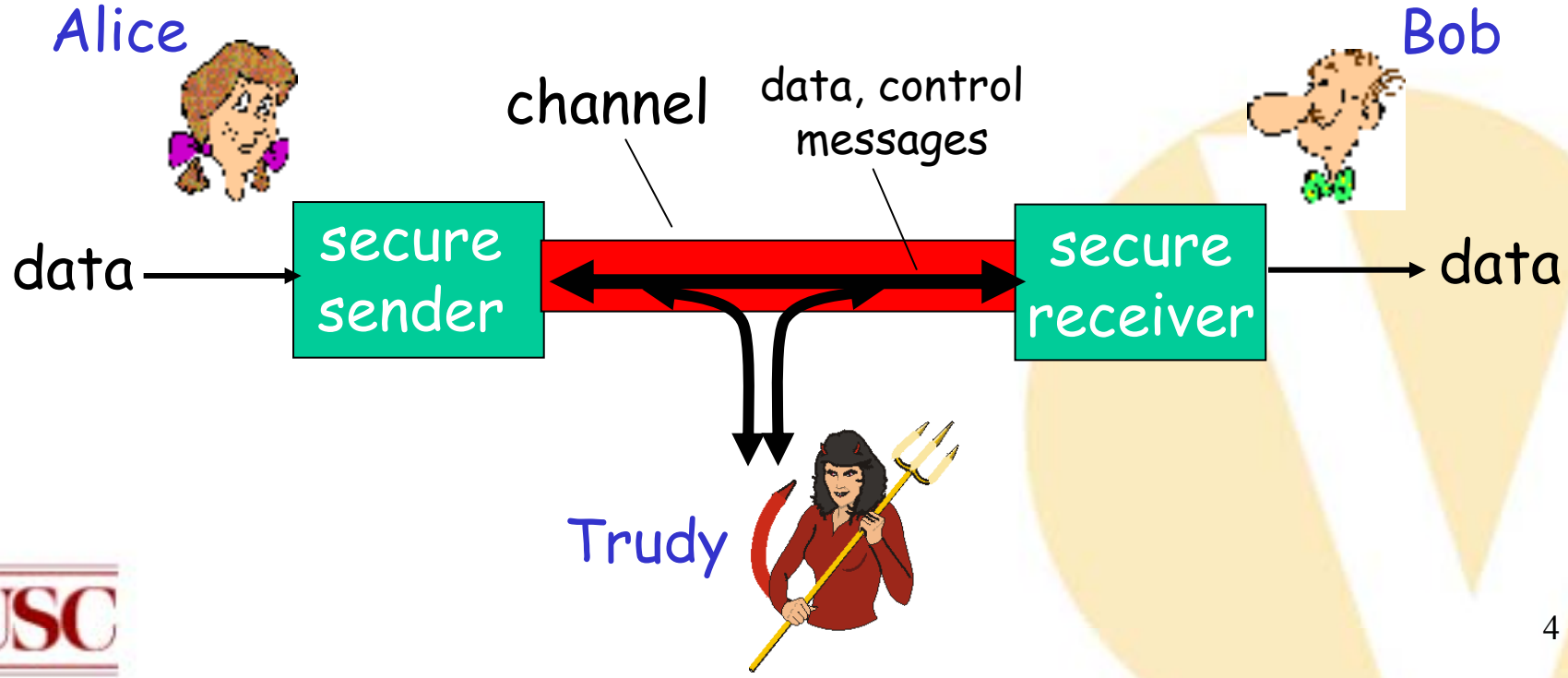
Network Security

- **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

ACL:access control list

Let us meet the Players

- Bob, Alice want to communicate "securely"
- Trudy (intruder) may intercept, delete, add messages



Who might Bob and Alice be?

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

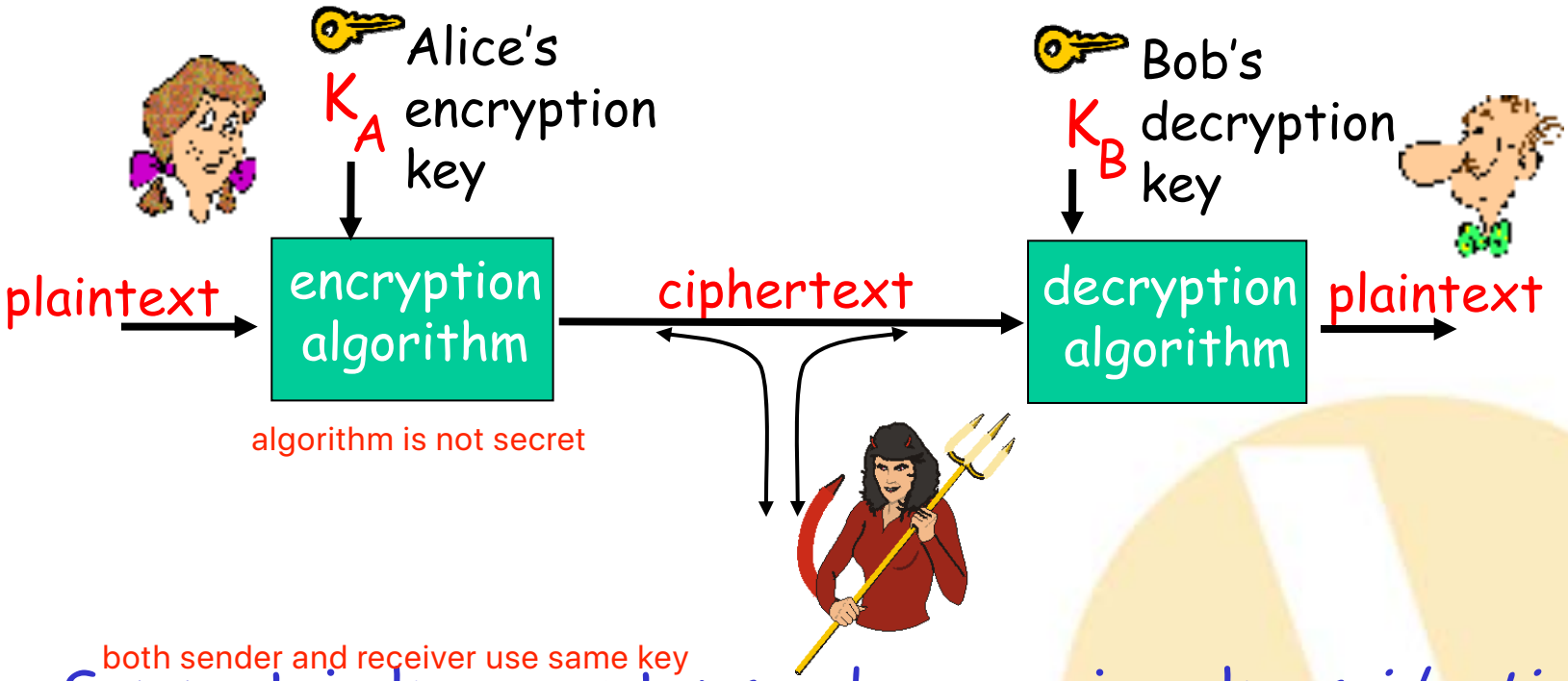
Bad Guys and Bad Girls

- Q: What can Trudy 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) use other people's IP address
  - hijacking: "take over" ongoing connection by removing sender or receiver, inserting herself in place
  - denial of service: prevent service from being used by others (e.g., by overloading resources)

Message Confidentiality

The concept of how to achieve message confidentiality or privacy has not changed for thousands of years. The message must be encrypted at the sender site and decrypted at the receiver site. This can be done using either symmetric-key cryptography or asymmetric-key cryptography.

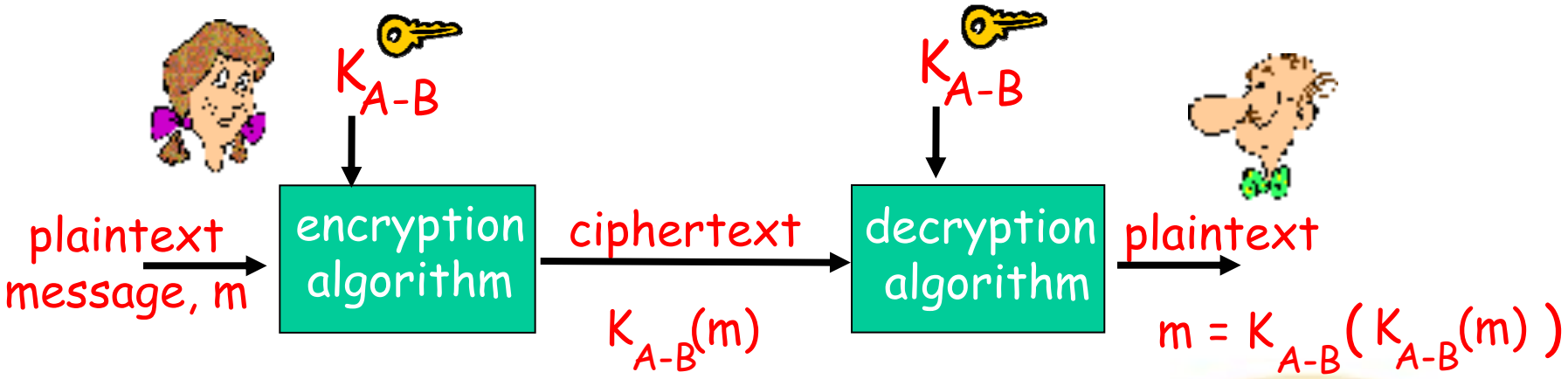
Cryptography



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

asymmetric key: decrytion is private

Symmetric Key Cryptography



- symmetric key crypto: Bob and Alice share same (symmetric) key: K
- e.g., key is knowing substitution pattern in mono alphabetic substitution cipher
- Challenge : How do Bob and Alice agree on key value?

Ex: Data Encryption Standard, DES

Example: Substitution Cipher

- substitution cipher: substituting one thing for another
  - Mono-alphabetic cipher: substitute one letter for another

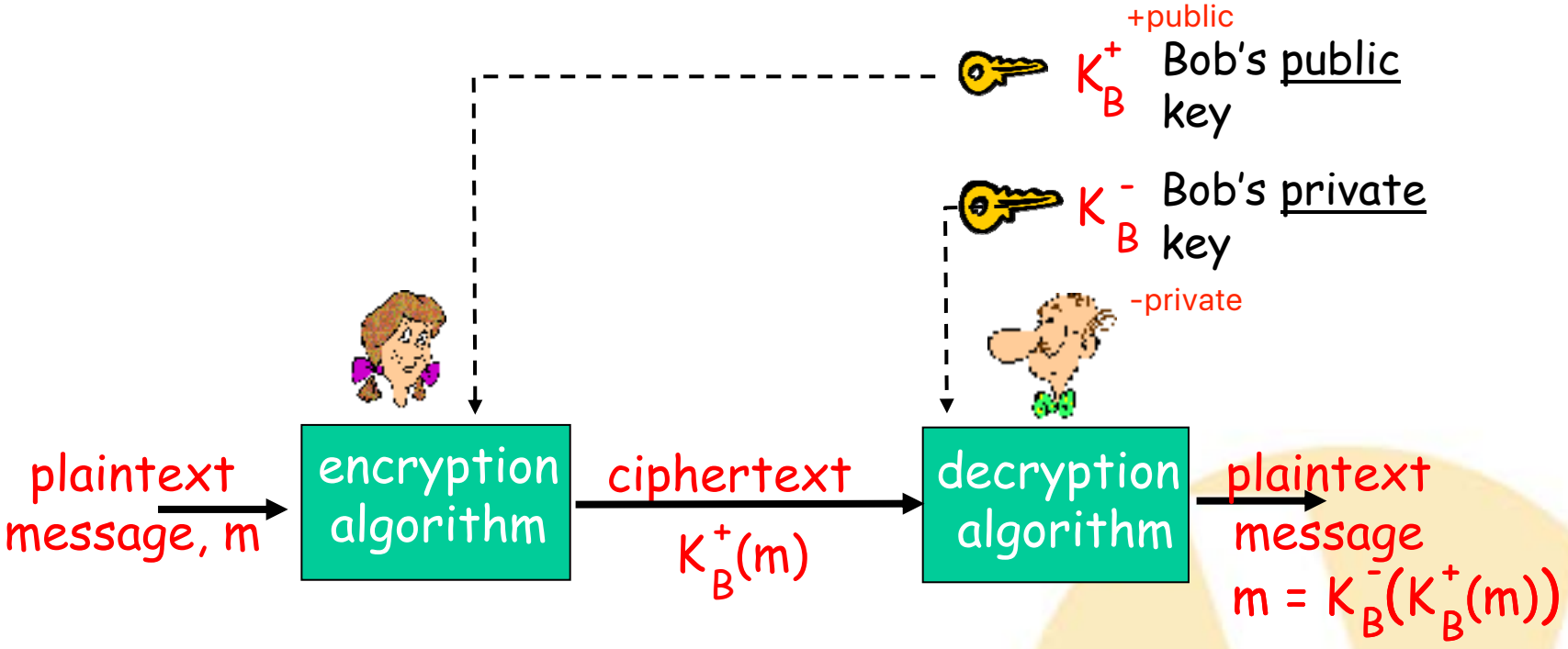
plaintext: abcdefghijklmnopqrstuvwxyz

ciphertext: mnbvcxzasdfghjklpoiuytrewq

Plaintext: Bob. i love you. Alice

ciphertext: nkn. s gktc wky. mgsbc

Public Key (Asymmetric) Cryptography



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

is equal to

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

sender, receiver do not share secret key

public encryption key known to all

private decryption key known only to receiver

Ex: Rivest, Shamir, Adelson (RSA) Algorithm

how to make sure this public key belong to someone

Authentication

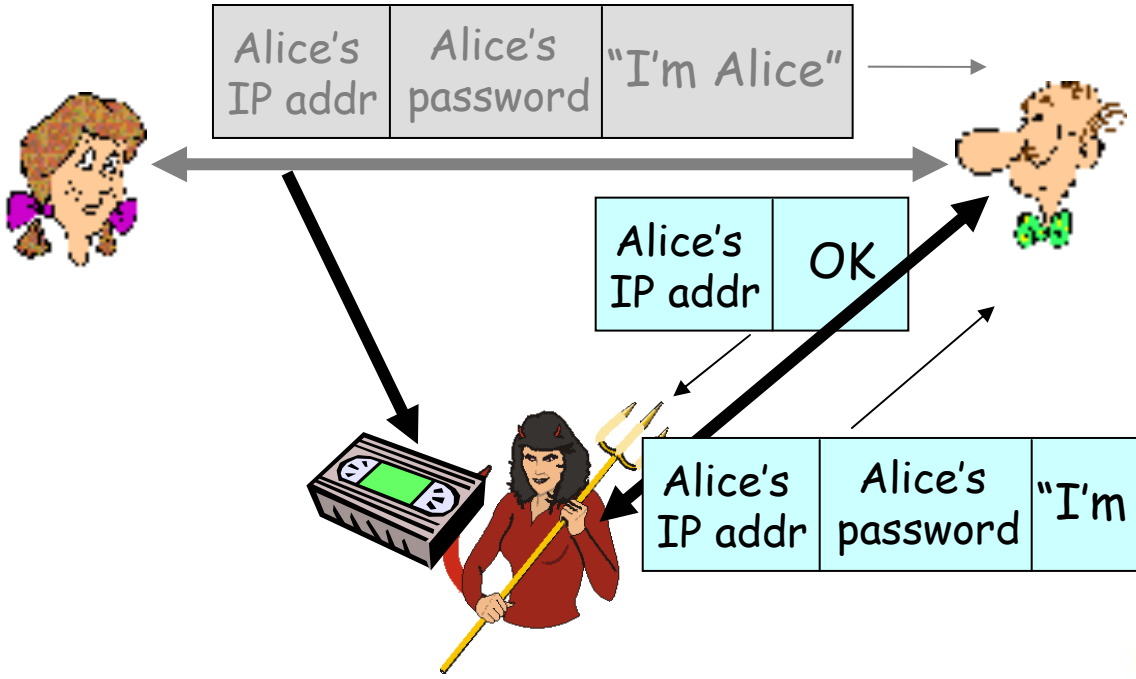
Entity authentication is a technique designed to let one party prove the identity of another party. An entity can be a person, a process, a client, or a server. The entity whose identity needs to be proved is called the claimant; the party that tries to prove the identity of the claimant is called the verifier.

Failure scenarios??

charge to to prove

record something and play it back

Playback Attack?



playback attack: Trudy records Alice's packet and later plays it back to Bob

Even if Alice encrypt her pass word, playback attack is still applicable

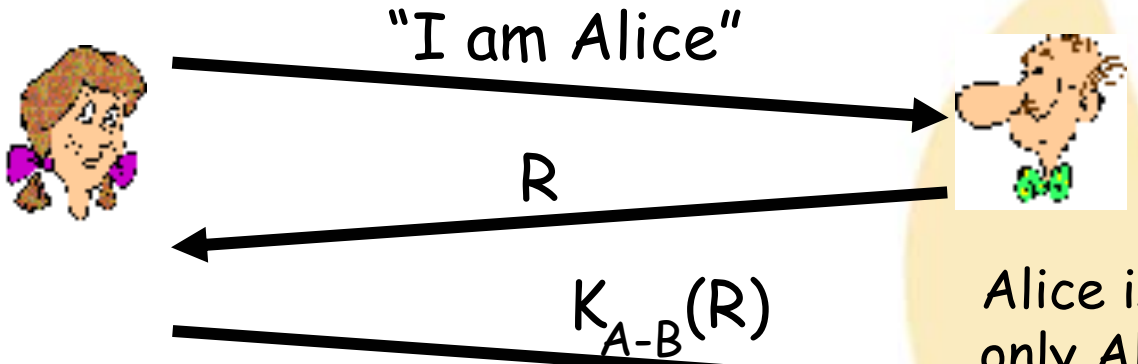
trudy cannot dencryt password but she can copy this password

Challenge/Response Authentication using a Nonce

Goal: avoid playback attack

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

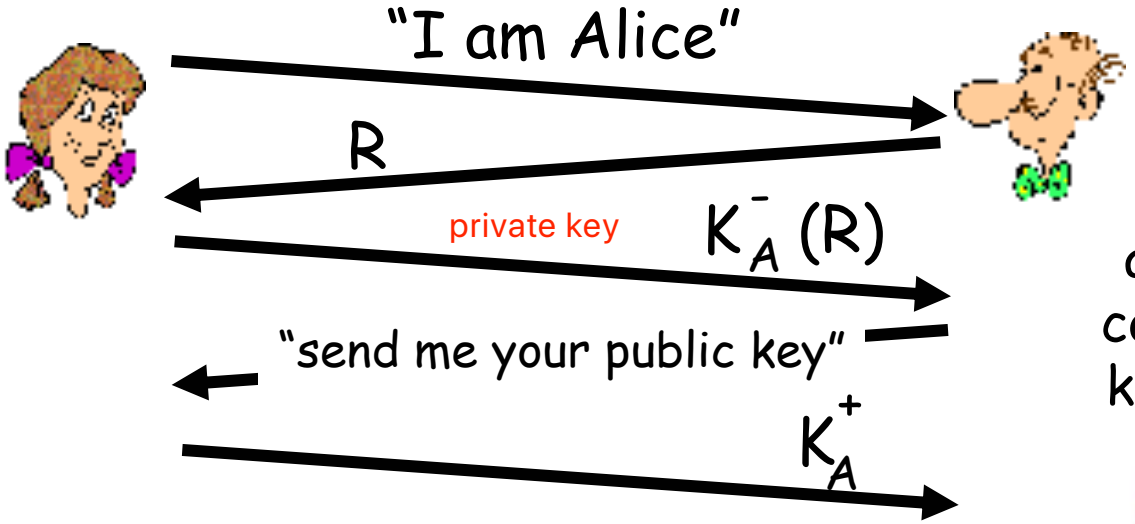
To prove Alice "live", Bob sends Alice nonce, R. Alice must return R, encrypted with shared secret key



check is that the same R with K,if R is the same, then it will be Alice

Alice is live, and only Alice knows key to encrypt nonce, so it must be Alice!

Nonce Authentication with Public Key



Bob computes

$K_A^+(K_A^-(R)) = R$

and knows only Alice could have the private key, that encrypted R such that

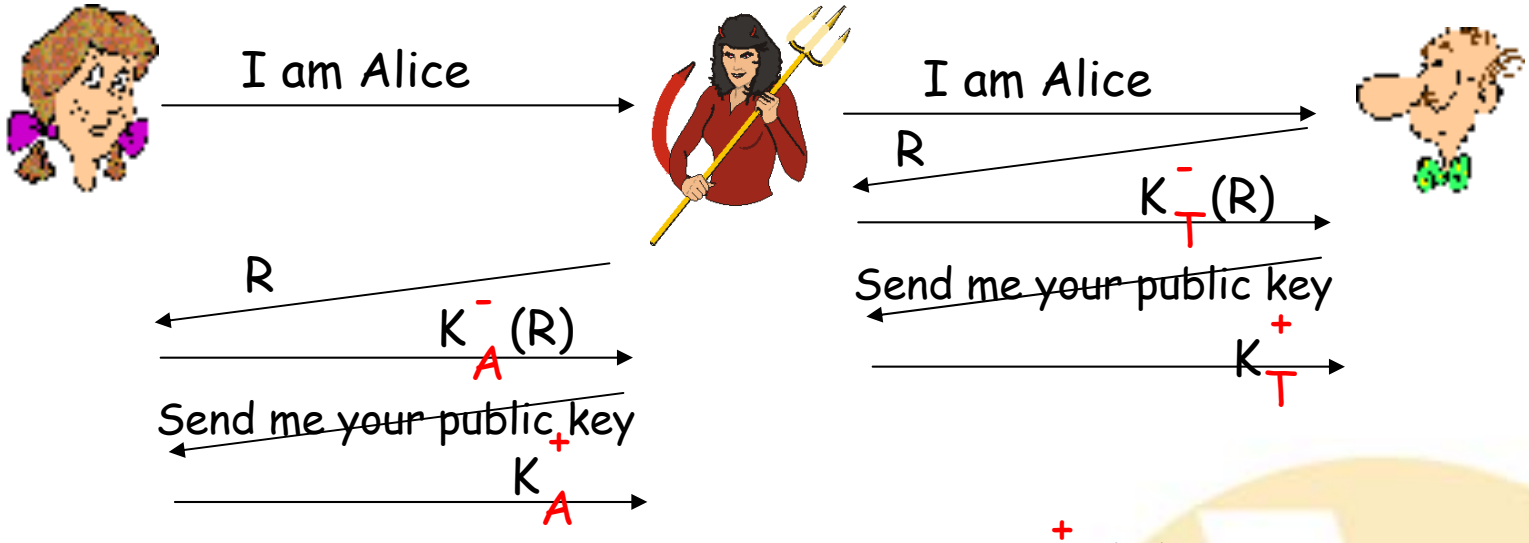
$K_A^+(K_A^-(R)) = R$

recover the R , then make sure is alice

Failure scenarios??

Security Hole?

problem: Bob should get the public key by himself instead of ask Alice to send public key



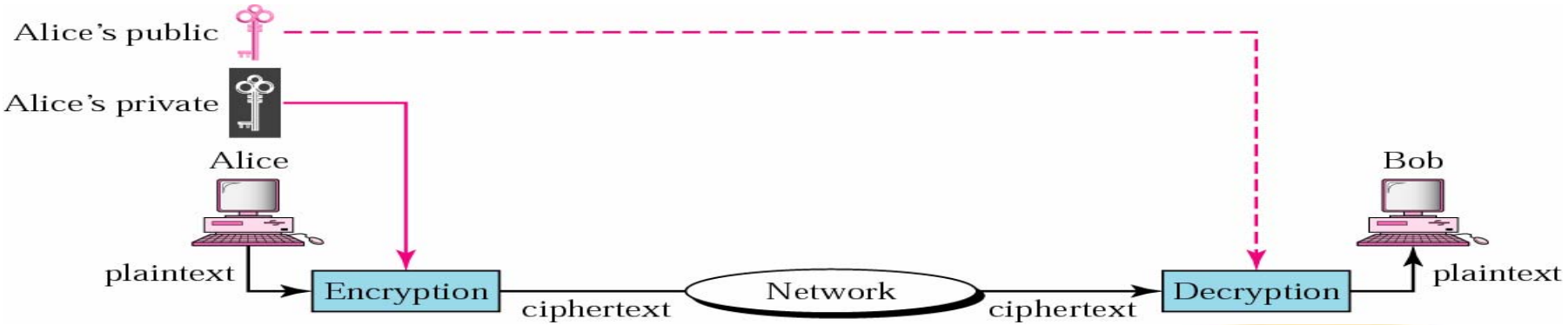
Man (woman) in the middle attack: Trudy poses as Alice (to Bob) and as Bob (to Alice)

KDC
CA

Message Integrity: Digital Signature

Signing the whole document

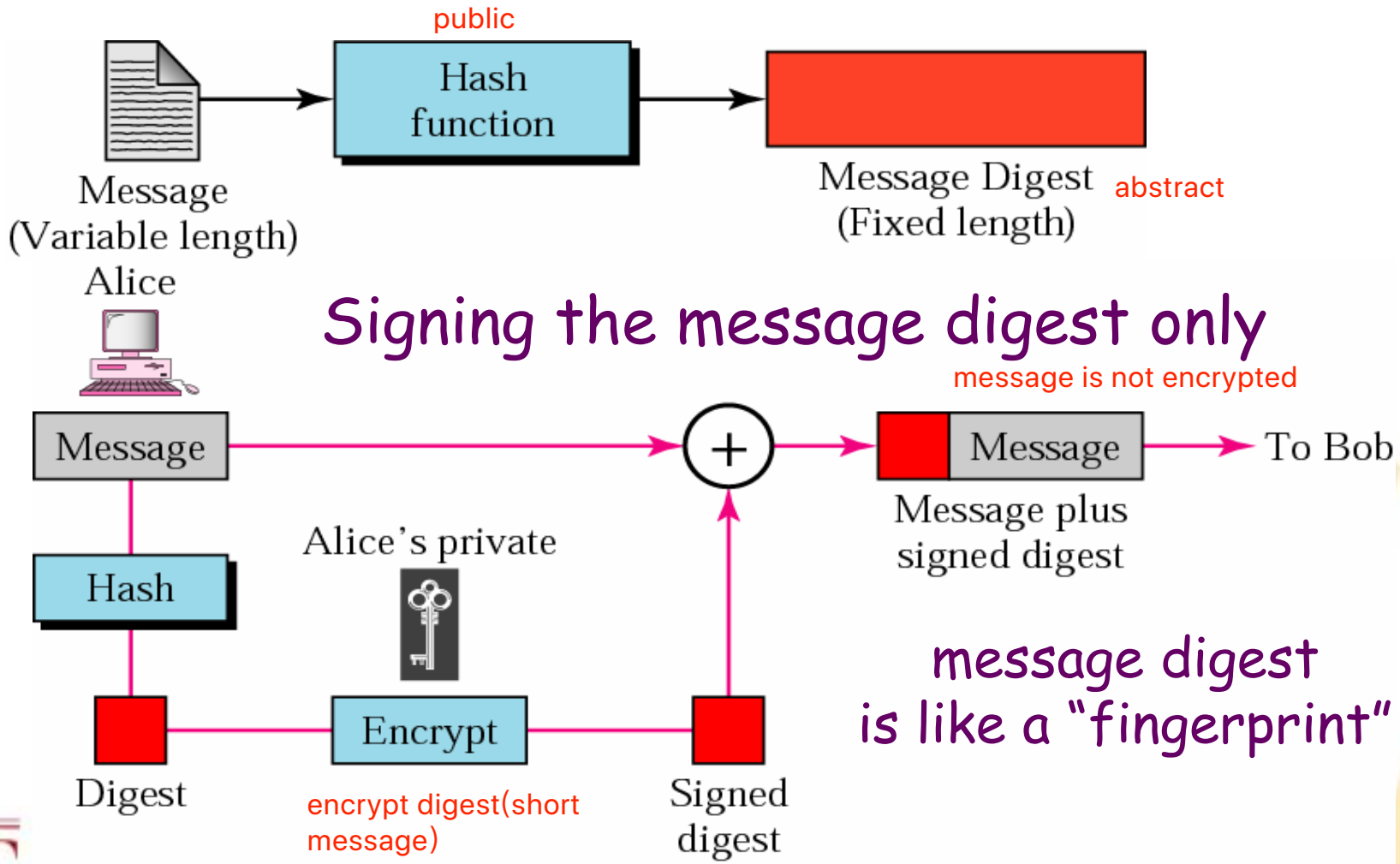
不管多少人看过，但是绝对不能改



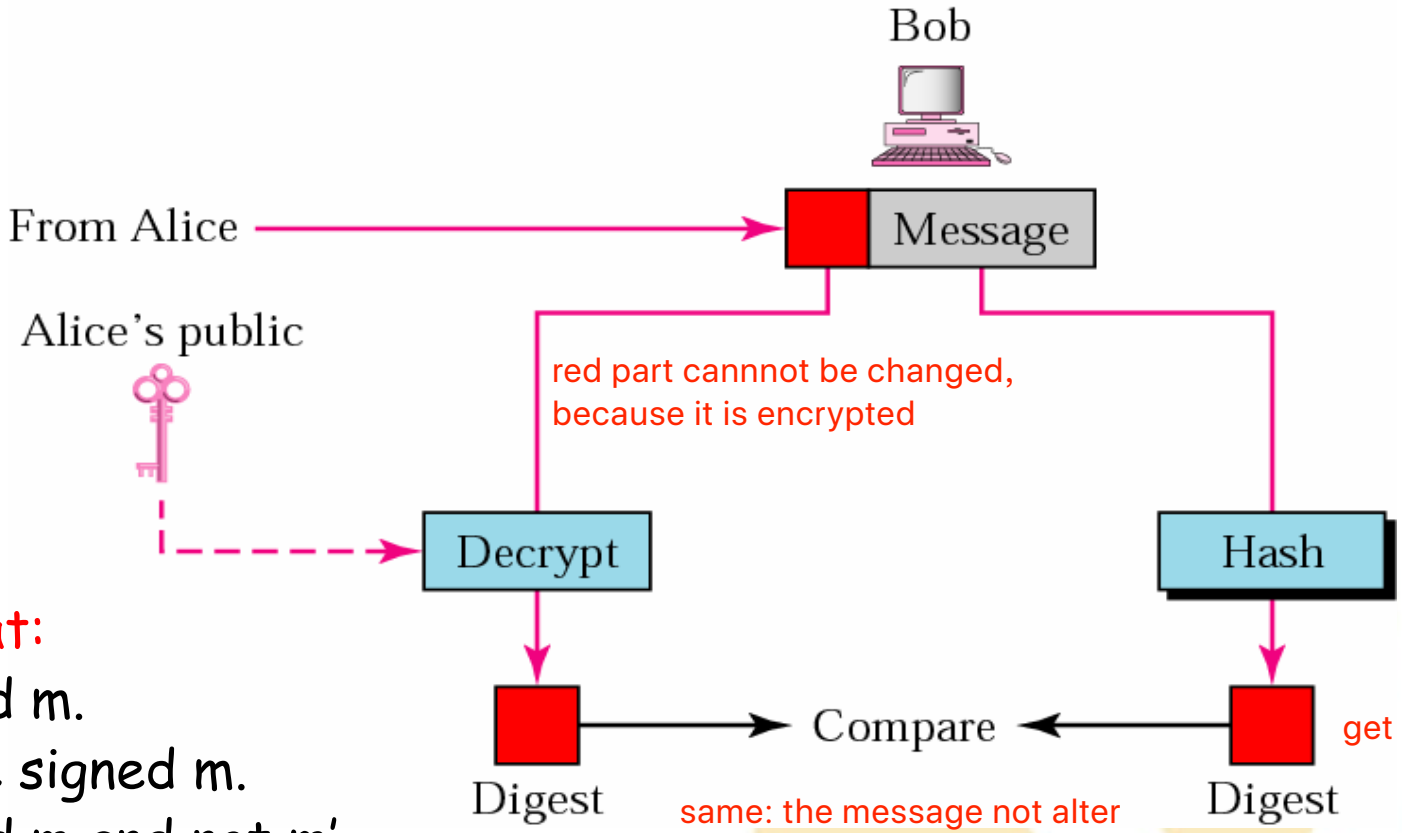
Digital signature does not provide privacy. If there is a need for privacy, another layer of encryption/decryption must be applied.

don't care about how many people read the message
the only care thing is not alter the message

Digital Signature: Sender Site



Digital Signature: Receiver Site



Bob can verify that:

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

Non-repudiation:

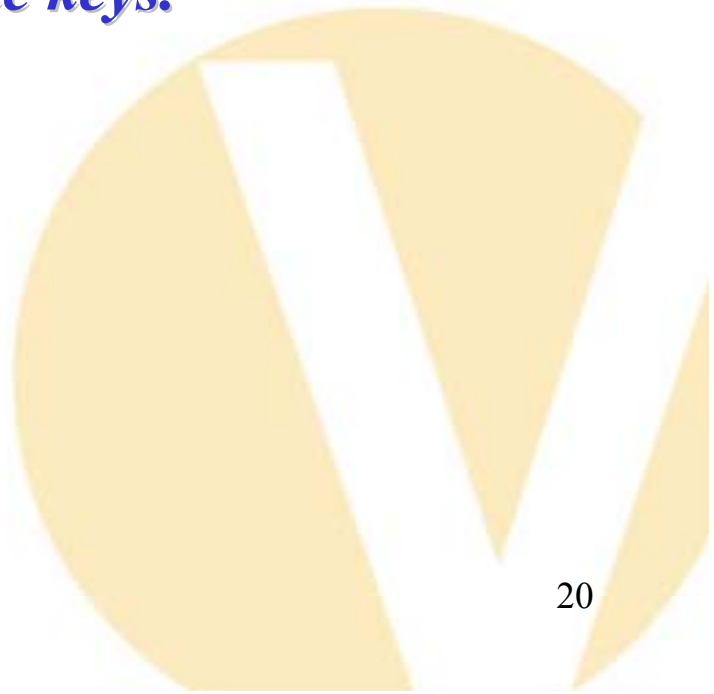
- ✓ Bob can take m, and signature $K_B(m)$ to court and prove that Alice signed m.

get a digest
not get the digest
if the message is altered,
the digest will be

Key Management

We never discussed how secret keys in symmetric-key cryptography and how public keys in asymmetric-key cryptography are distributed and maintained. In this section, we touch on these two issues. We first discuss the distribution of symmetric keys; we then discuss the distribution of asymmetric keys.

distribute public key



Key Problems

- **Symmetric key problem:**
- How do two entities establish shared secret key over network?
- Solution:
- trusted key distribution center (KDC) acting as intermediary between entities

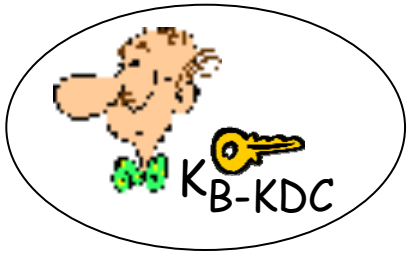
- **Public key problem:**
- When Alice obtains Bob's public key (from web site, e-mail, diskette), how does she know it is Bob's public key, not Trudy's?
- Solution:
- trusted certification authority (CA)

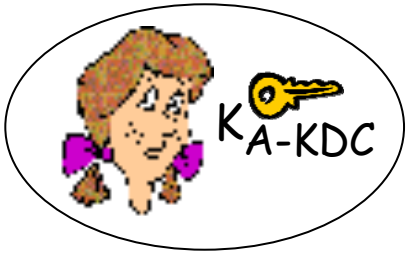
for distribution of shared key

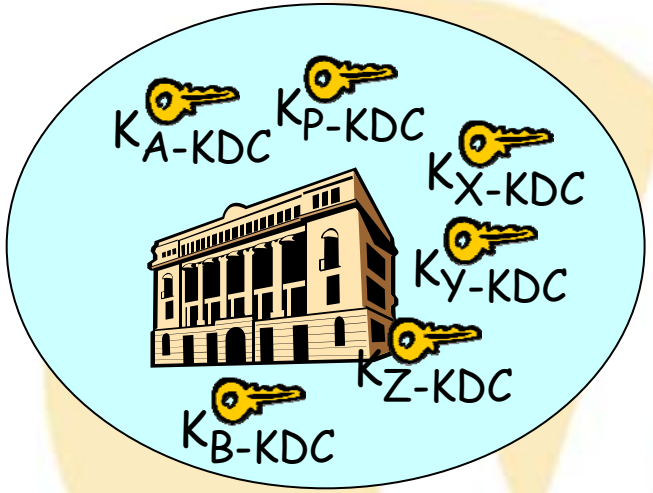
Key Distribution Center

for exchanging shared key

- Alice, Bob need shared symmetric key.
- KDC: server shares different secret key with *each* registered user (many users)
- Alice, Bob know own symmetric keys, KA-KDC KB-KDC , for communicating with KDC.

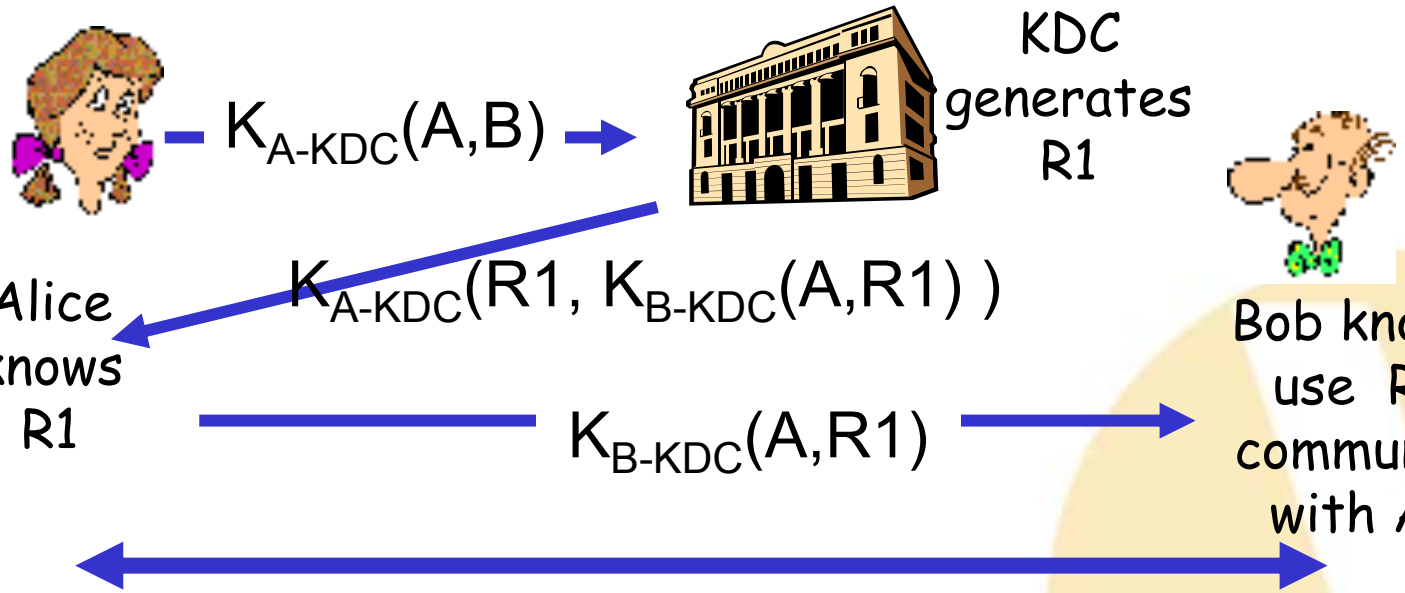






Key Distribution Center (KDC)

Q: How does KDC allow Bob, Alice to determine shared symmetric secret key to communicate with each other?

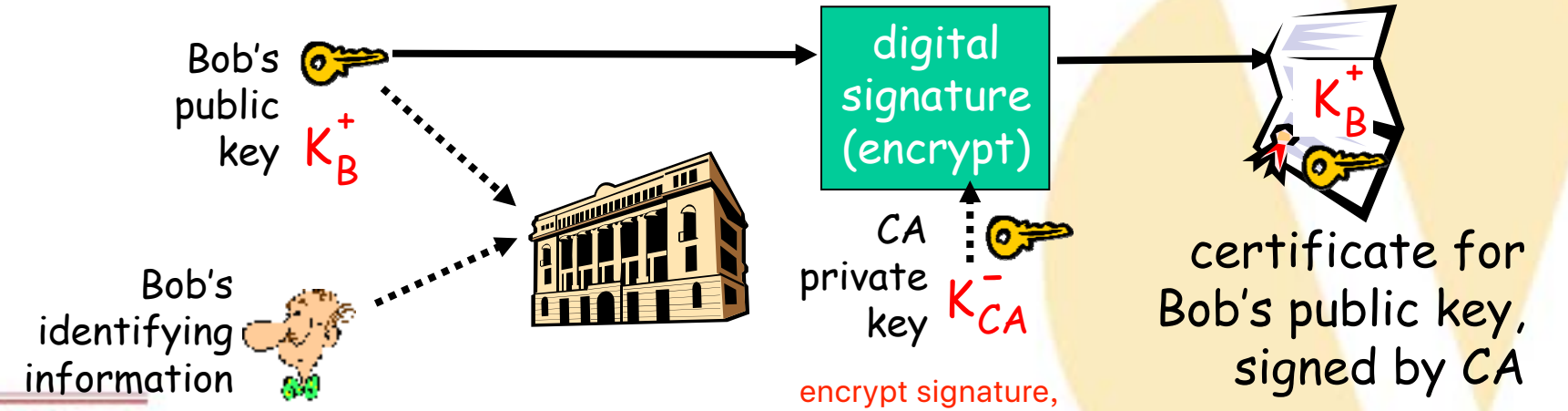


Alice and Bob communicate: using R1 as *session key* for shared symmetric encryption

trusted

Certification Authorities

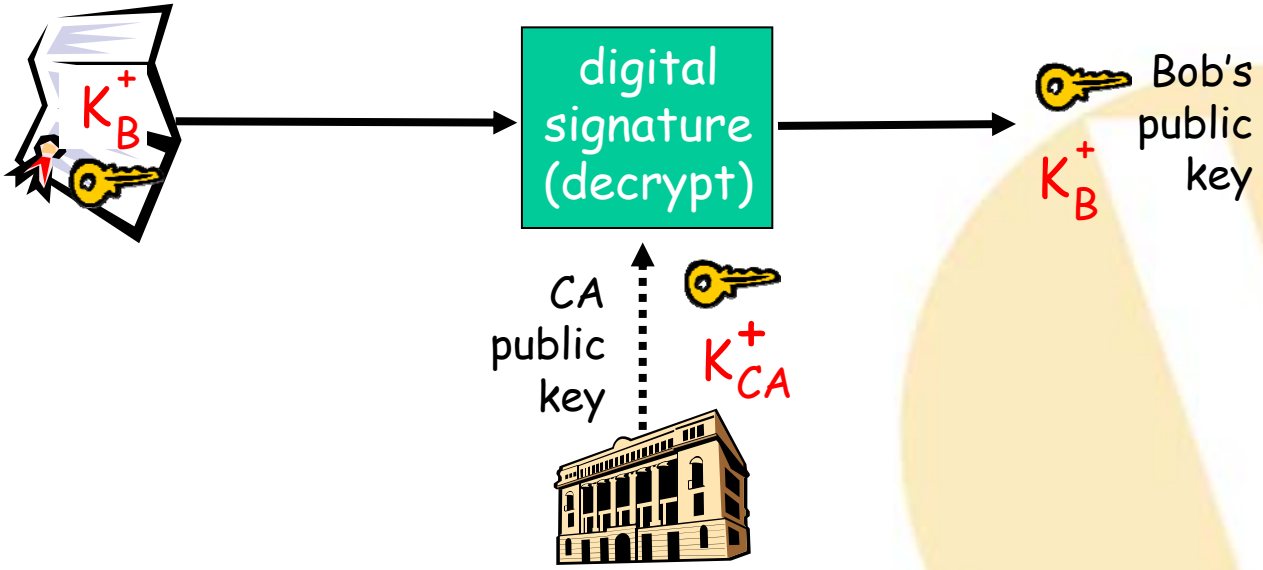
- Certification authority (CA): binds public key to particular entity, E.
- E (person, router) registers its public key with CA.
  - E provides "proof of identity" to CA.
  - CA creates certificate binding E to its public key.
  - certificate containing E's public key digitally signed by CA – CA says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



Certification Authorities (Cont.)

decrypted the signature—>then you will know the certification came from CA

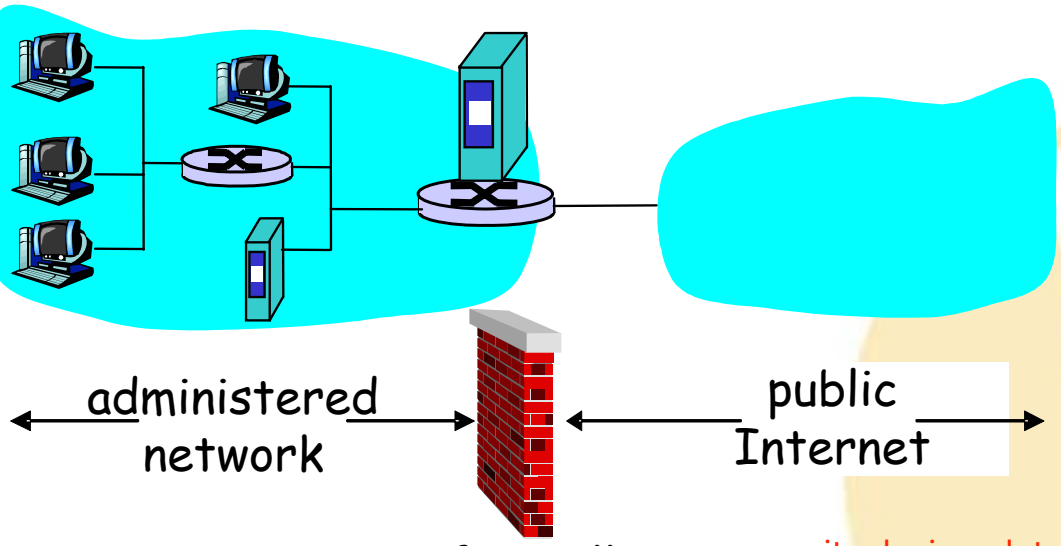
- When Alice wants Bob's public key:
  - gets Bob's certificate (Bob or elsewhere).
  - apply CA's public key to Bob's certificate, get Bob's public key



Access Control: Firewalls

firewall

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



hardware/software device

security device: determine whether you have the right to seprate private and public network

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)
- Two types of firewalls:
  - Packet-Filtering — operated at layer 3 and 4
  - Application-Level Filtering — layer 5

ACL:access control list

Packet Filtering

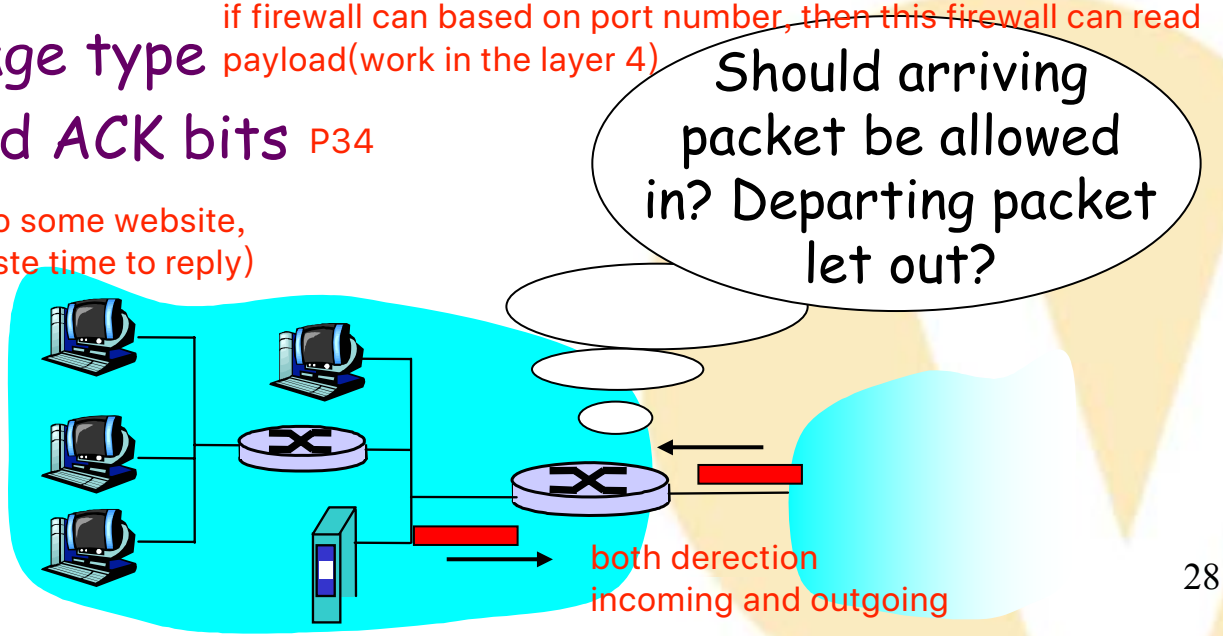
- Internal network connected to Internet via router firewall
- Router filters packet-by-packet, decision to forward/drop packet based on:
  - Source IP address, Destination IP address
  - TCP/UDP Source and Destination Port Numbers
  - ICMP message type
  - TCP SYN and ACK bits P34

if the IP is not in the list(ACL), firewall will drop this packet

if firewall can based on port number, then this firewall can read payload(work in the layer 4)

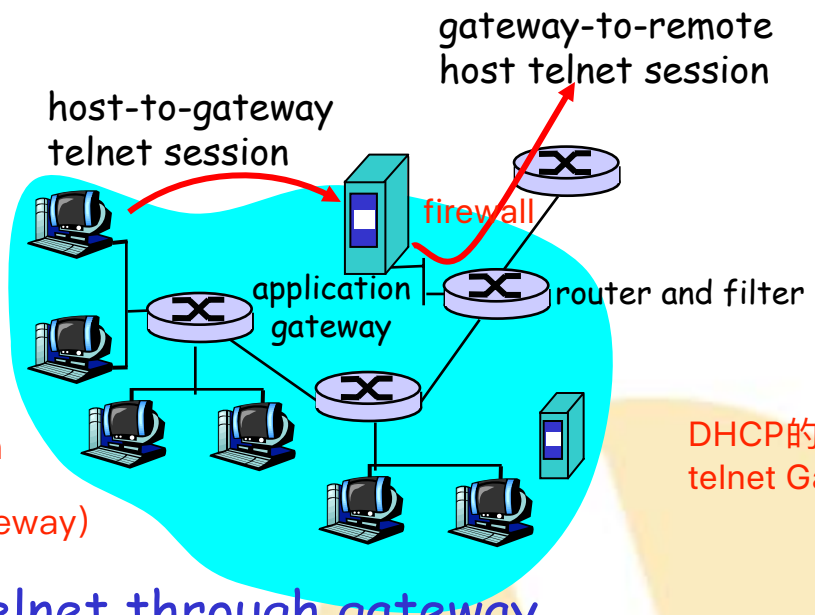
ICMP: internet control message protocol
block ICMP means when you trace root to some website, router will send you ***(don't want to waste time to reply)

@ the network
Or transport layer



Applications Firewalls

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



remote login

不能直接通过红线login
需要经过firewall
first（application gateway）

DHCP的参数需要加上
telnet Gateway

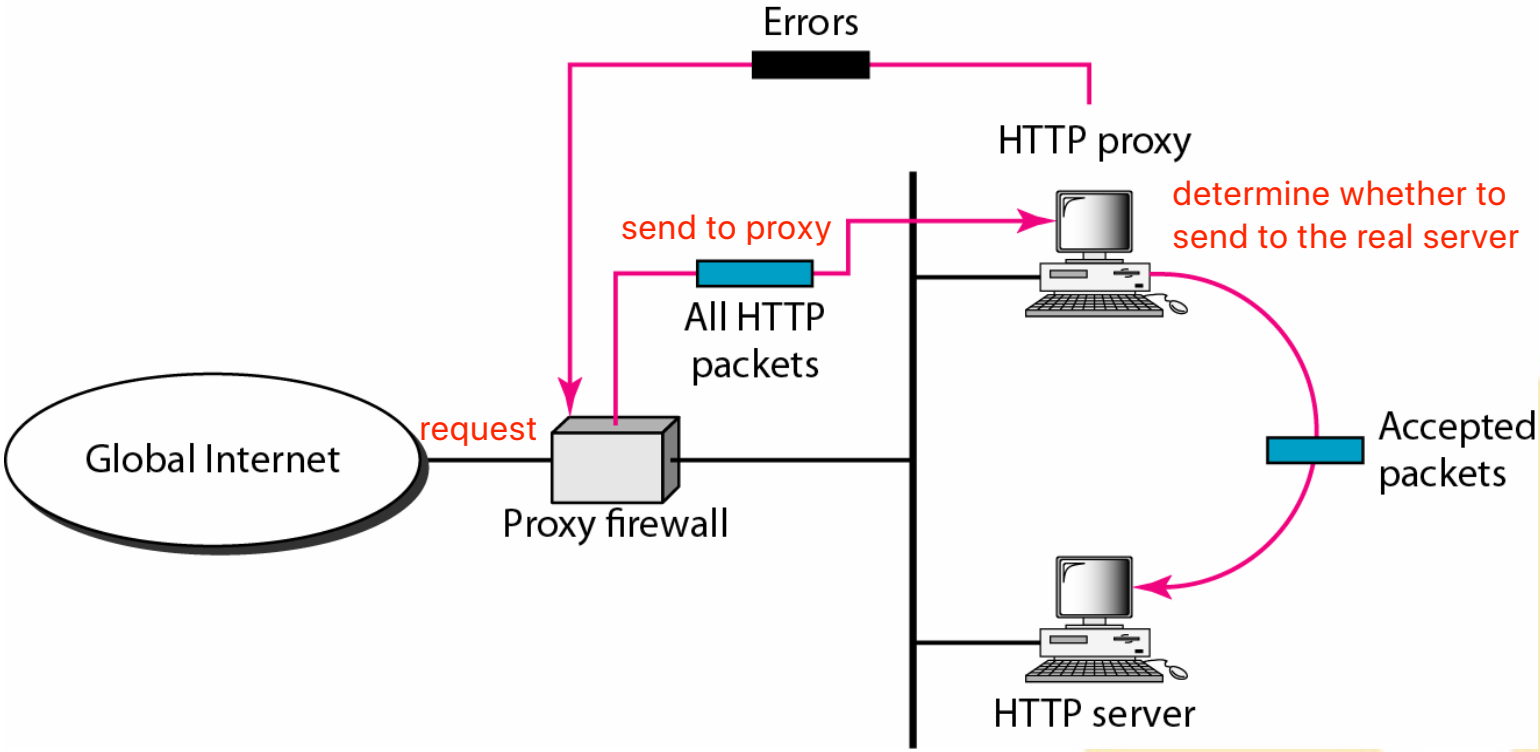
1. Require all telnet users to telnet through gateway.
2. For authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
3. Router filter blocks all telnet connections not originating from gateway.

drop

Proxy Firewall

DNS server

a substitude



real server

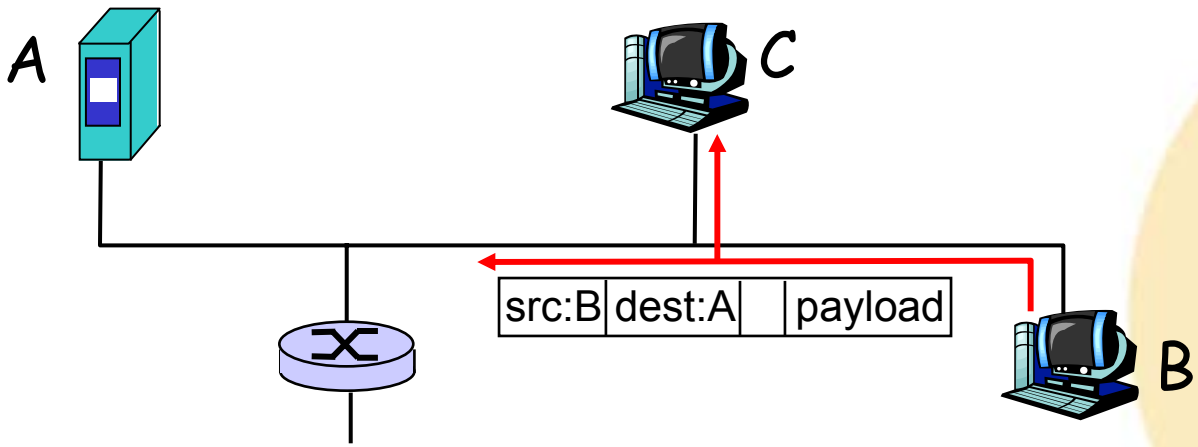
Limitations of Firewalls

- 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.

Security Threats

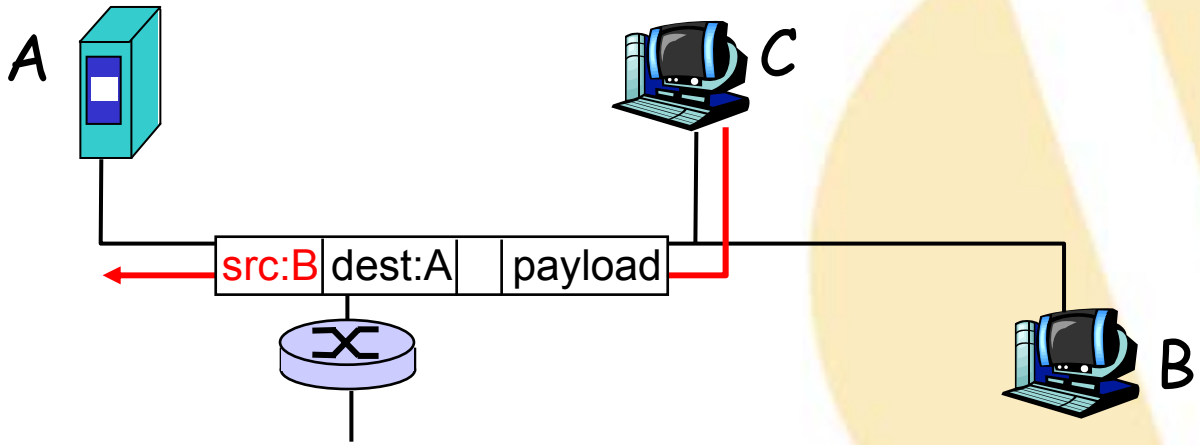
- Packet sniffing: wireshark
  - Broadcast Traffic
  - Promiscuous NIC reads all Packets passing by
  - Can read all unencrypted data (e.g. passwords)
  - e.g.: C sniffs B's packets



Security Threats

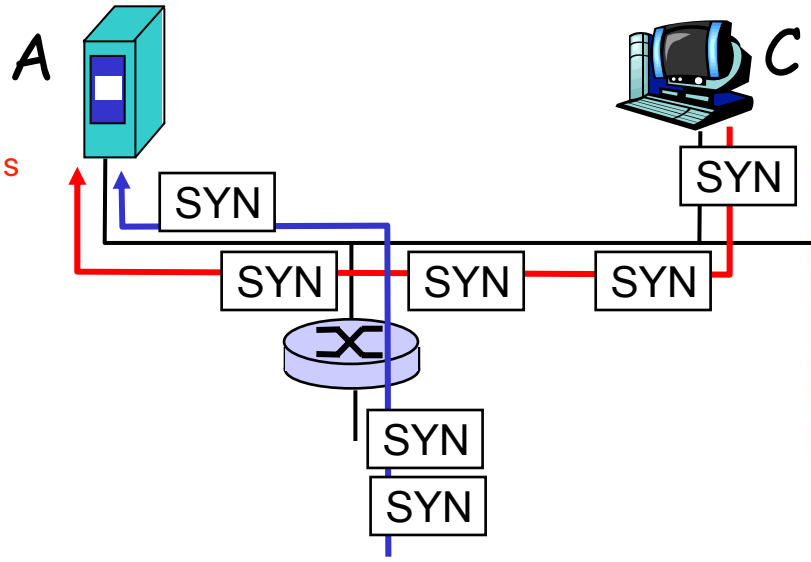
- IP Spoofing:
  - can generate "raw" IP packets directly from application, putting any value into IP source address field
  - receiver can't tell if source is spoofed
  - e.g.: C pretends to be B

he is using B IP
C is pretending to B(spoof)



Security Threats

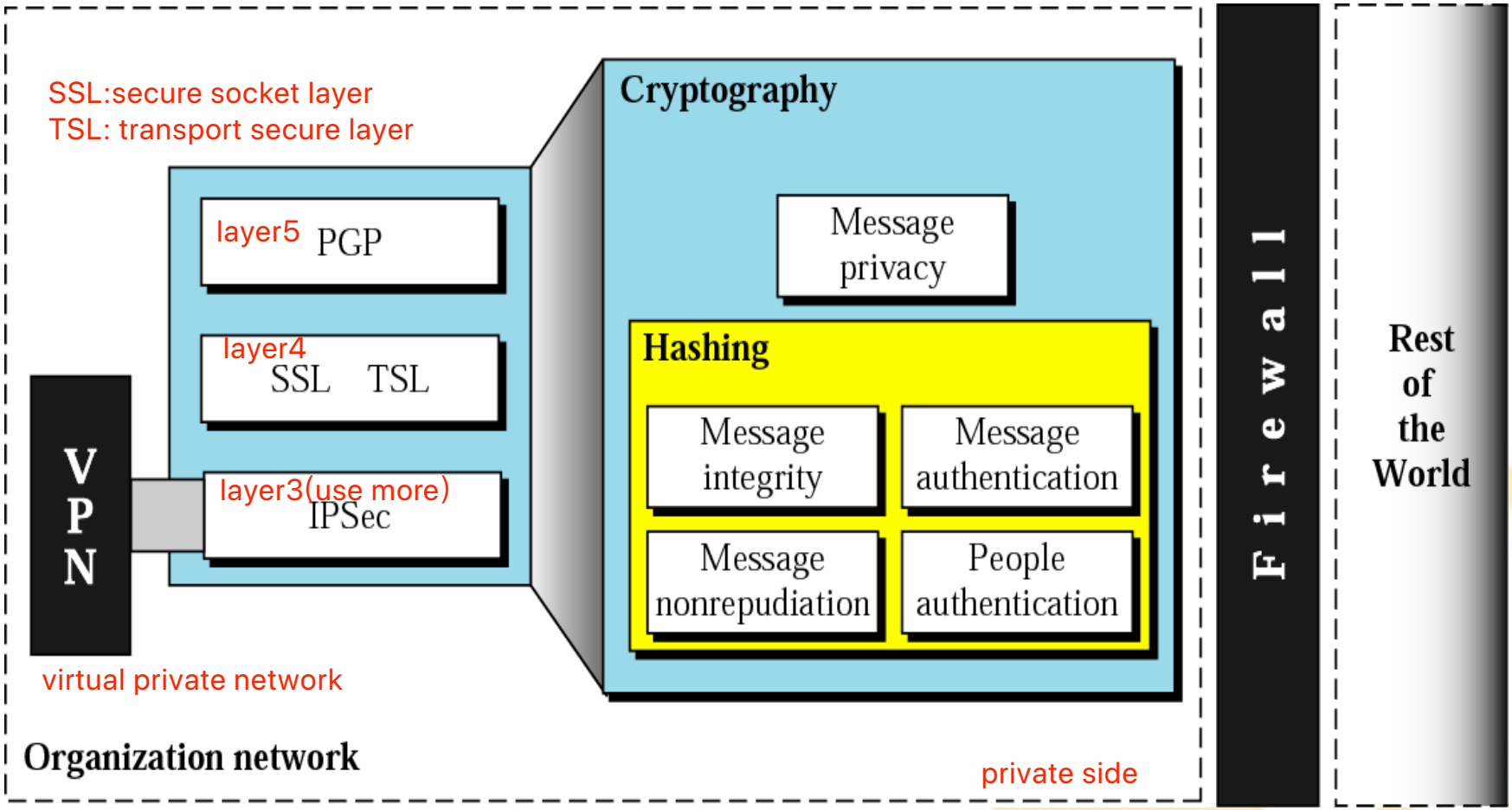
- Denial of service (DOS):
  - Flood of maliciously generated packets "swamp" receiver
  - Distributed DOS (DDOS): multiple coordinated sources swamp receiver
  - e.g., C and remote host SYN-attack A



parent socket shake hands

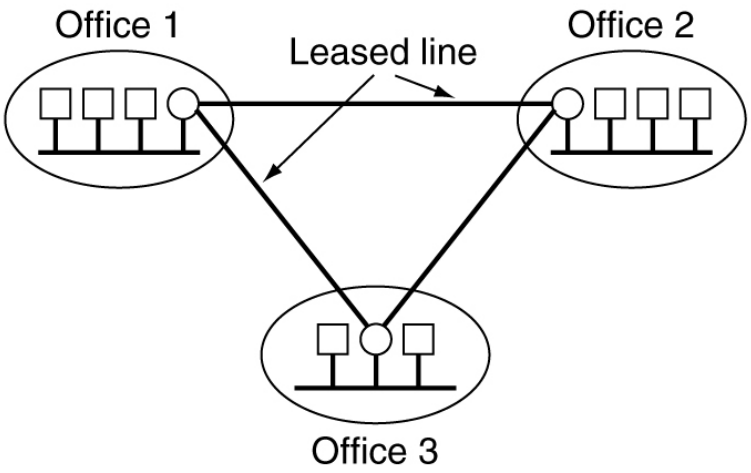
因为serverA一直在shake hand with other，所以B没有办法给serverA发信息

Security Layers

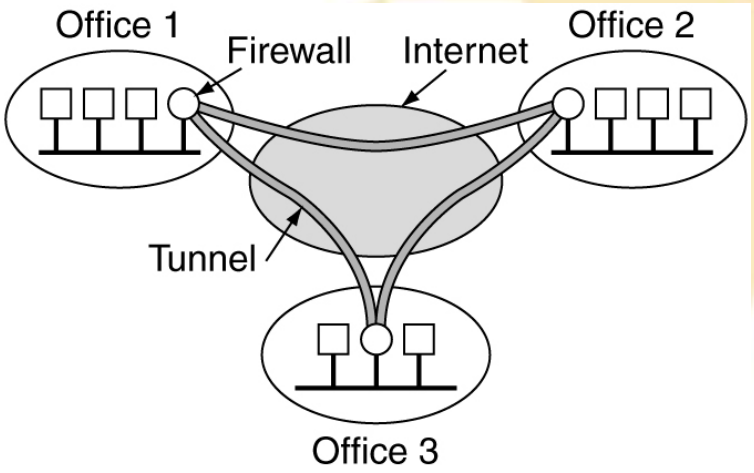


What is a VPN?

- Making a shared network look like a private network
- Why do this?
  - Private networks have all kinds of advantages
  - Building a private network is expensive
    - (cheaper to have shared resources rather than dedicated)



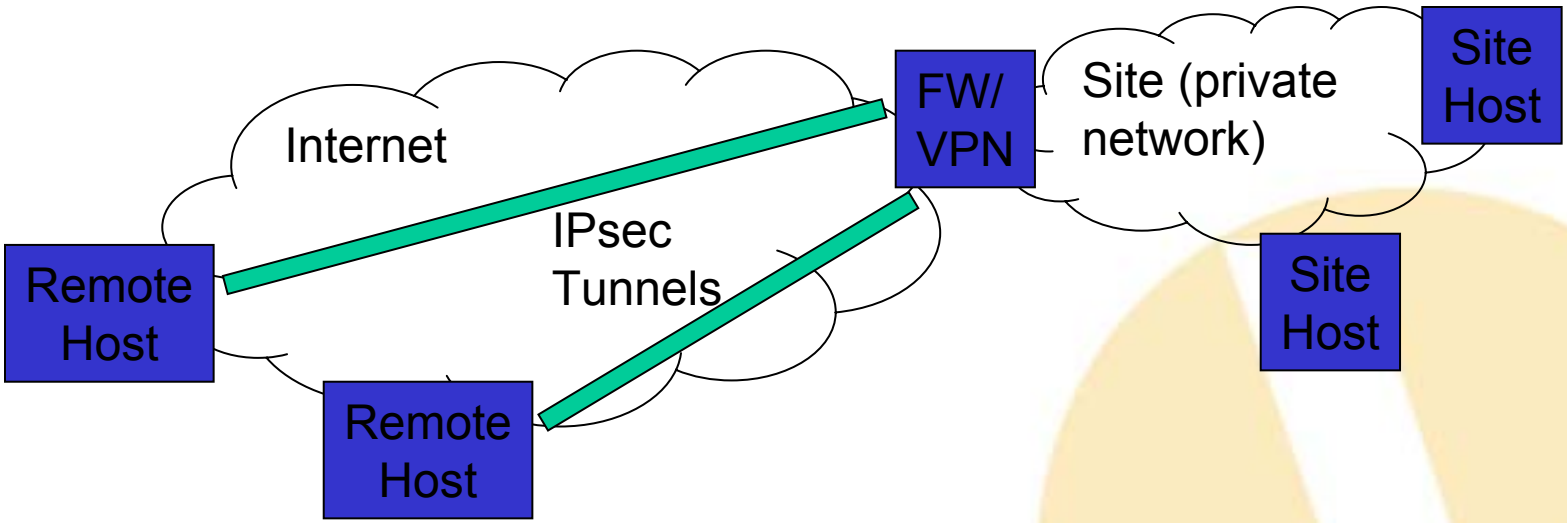
(a)



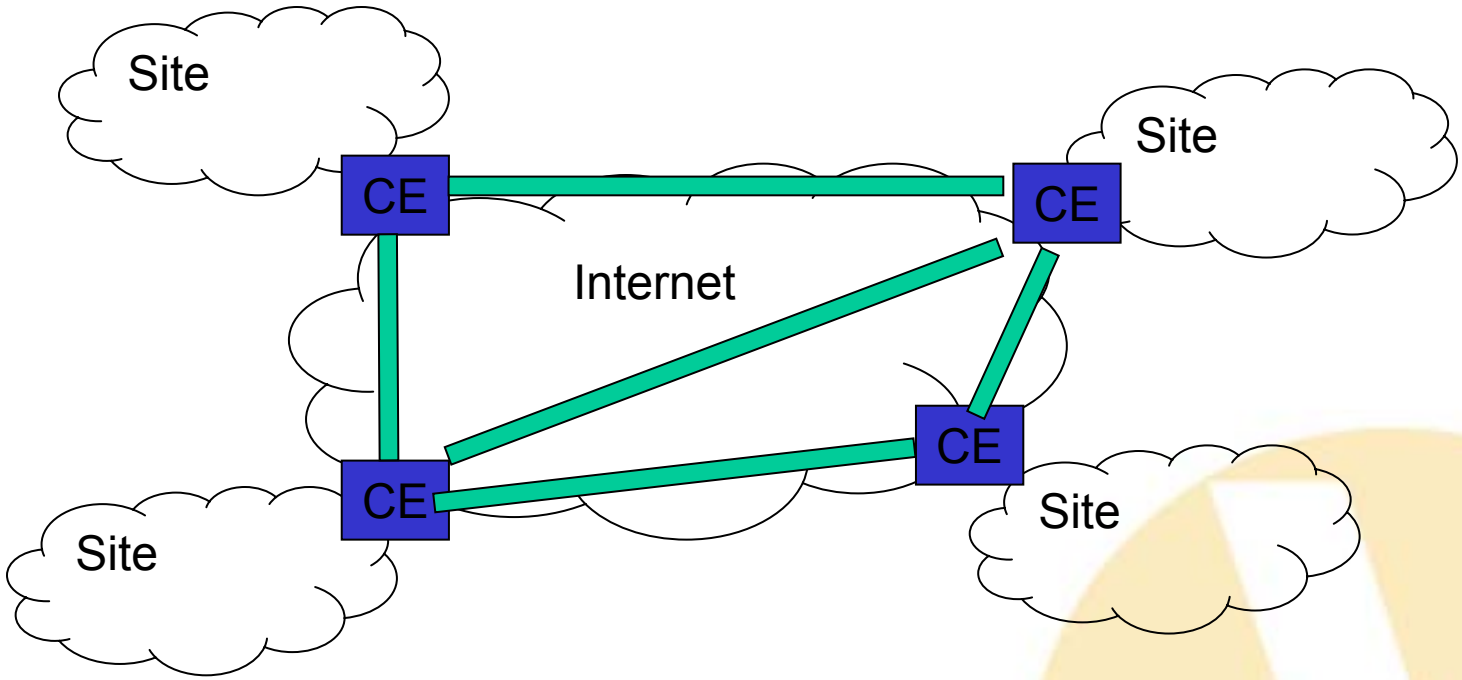
(b)

End-to-End VPNs

- Solves problem of how to connect remote hosts to a firewalled network

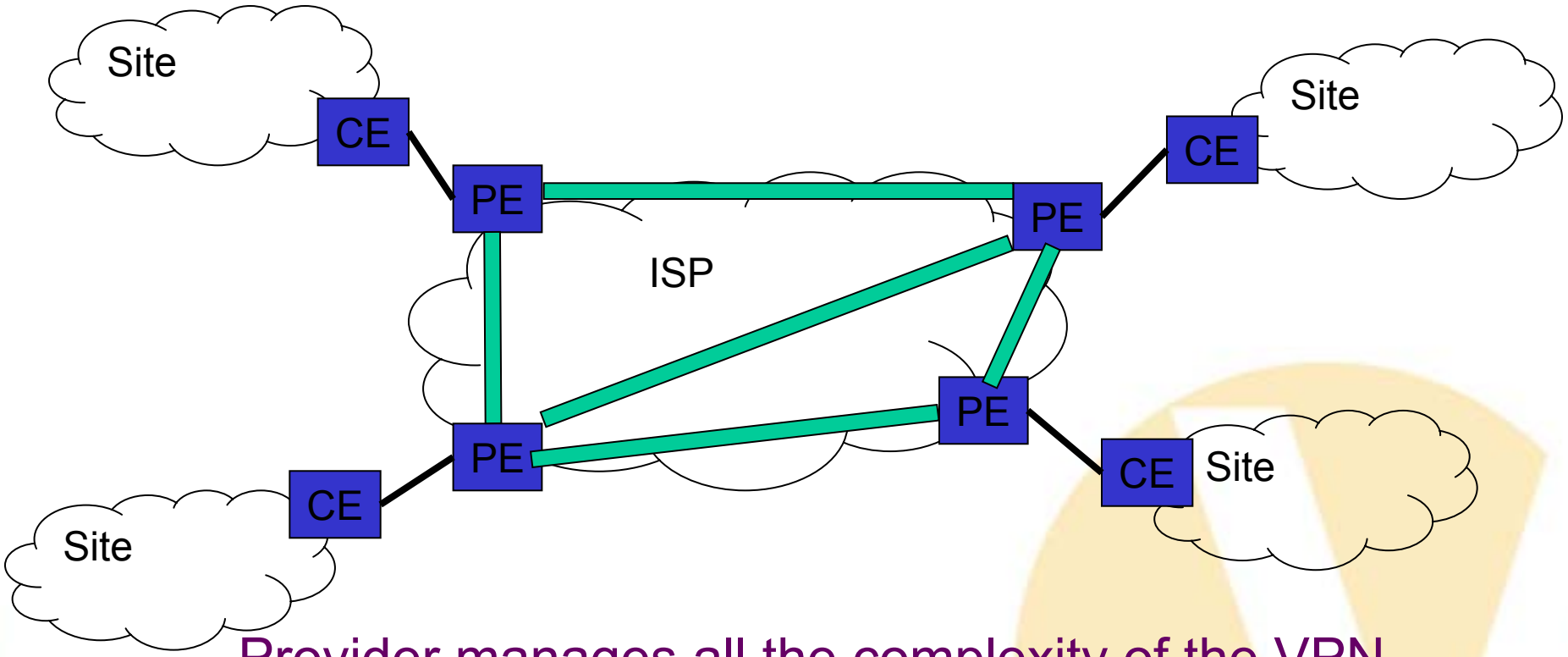


Customer-based Network VPNs



Customer buys own equipment, configures IPsec tunnels over the global internet, manages addressing and routing. ISP plays no role.

Provider-based Network VPNs



Provider manages all the complexity of the VPN.
Customer simply connects to the provider equipment.

End of the Semester

I hope that you learned from
and enjoyed the course
"Good Luck in your finals"