

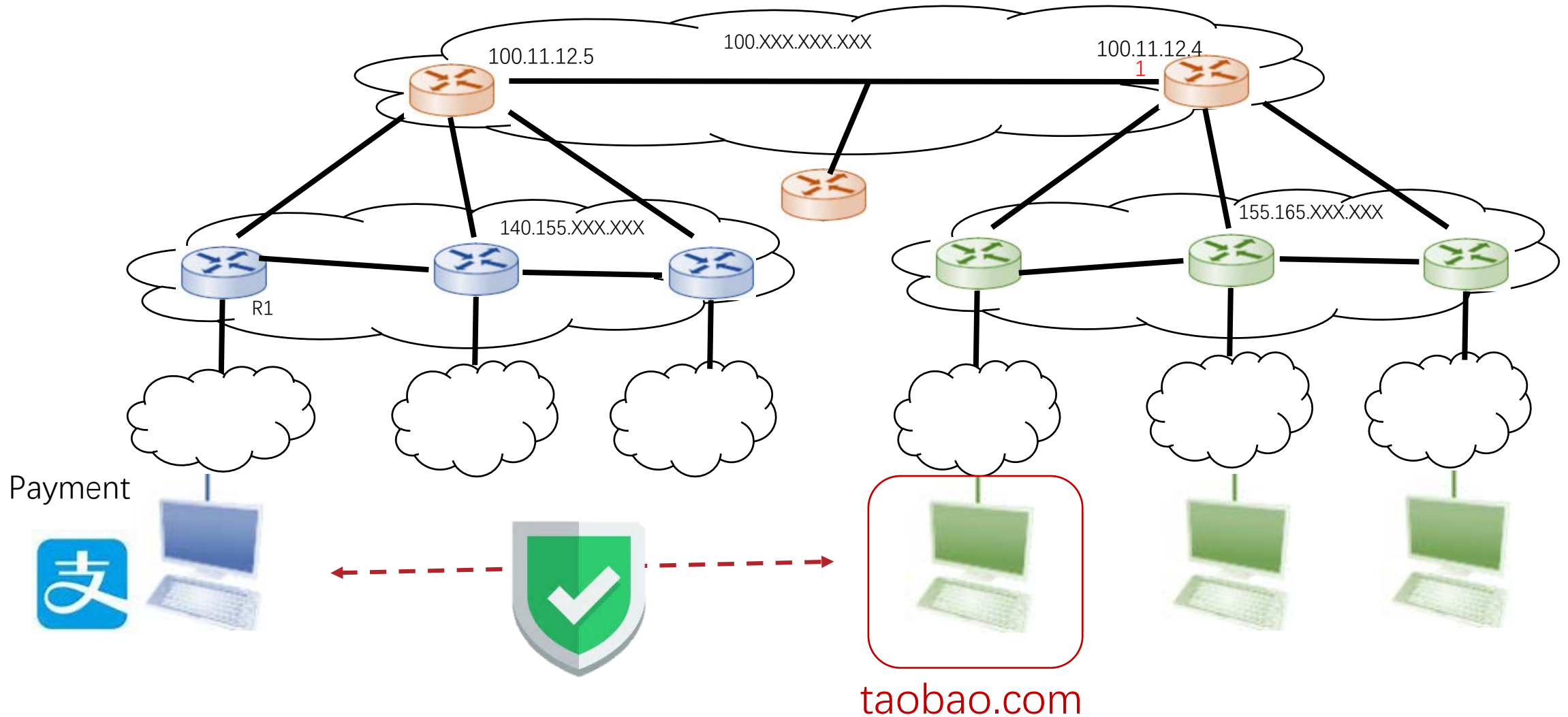


CS120: Computer Networks

Lecture 27. Network Security 1

Zhice Yang

How to Make Internet Secure ?



What is Network Security

- Confidentiality
 - To encrypt messages so as to prevent an adversary from understanding the message contents
- Integrity
 - To prevent an adversary from modifying the message contents.
- Availability
 - services must be accessible and available to users
- Authentication
 - To confirm identity of each other
- Timeliness
 - To identify delayed messages

Guarantee	Primitive
Confidentiality	Encryption
Integrity	MAC
Authentication	Signatures

Security Risks in Network

- Eavesdrop
- Injection
- 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 (DoS):
 - prevent service from being used by others (e.g., by overloading resources)
- ...

What is Network Security

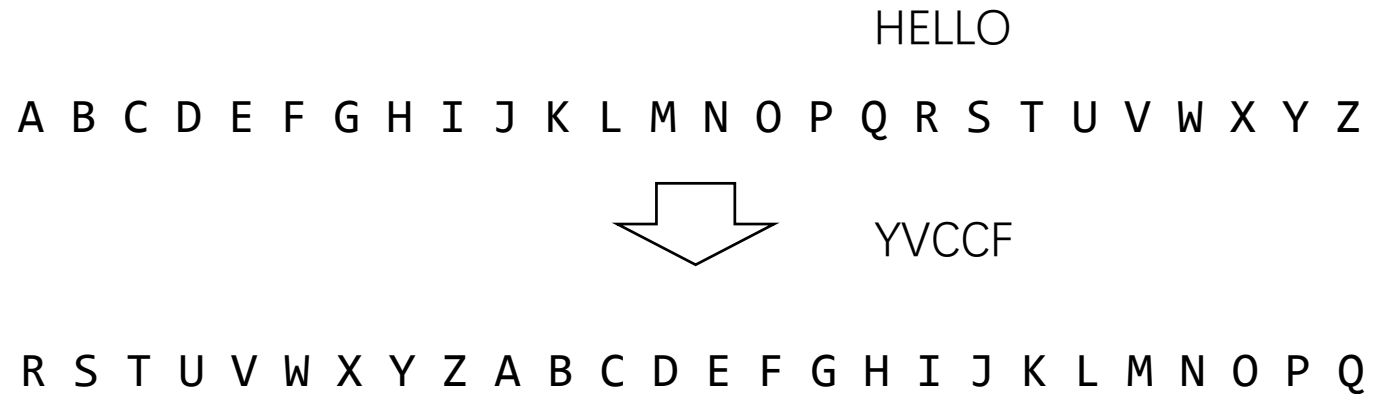
➤ Confidentiality

- To encrypt messages so as to prevent an adversary from understanding the message contents
- Integrity
 - To prevent an adversary from modifying the message contents.
- Availability
 - services must be accessible and available to users
- Authentication
 - To confirm identity of each other
- Timeliness
 - To identify delayed messages

Guarantee	Primitive
Confidentiality	Encryption
Integrity	MAC
Authentication	Signatures

Cipher

- Cipher: the Cryptographic Algorithm for Encryption or Decryption



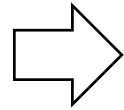
Cipher

- Ciphers are normally parameterized by **keys**
 - Message: x
 - Key: k_1, k_2
 - Encryption function: $y = \text{En}(x, k_1)$
 - Decryption function: $x = \text{De}(y, k_2)$
- Key is the secret
 - The encryption function and decryption function are public known



Cipher as a Secret ?

Obtain the secret by
unlocking the block



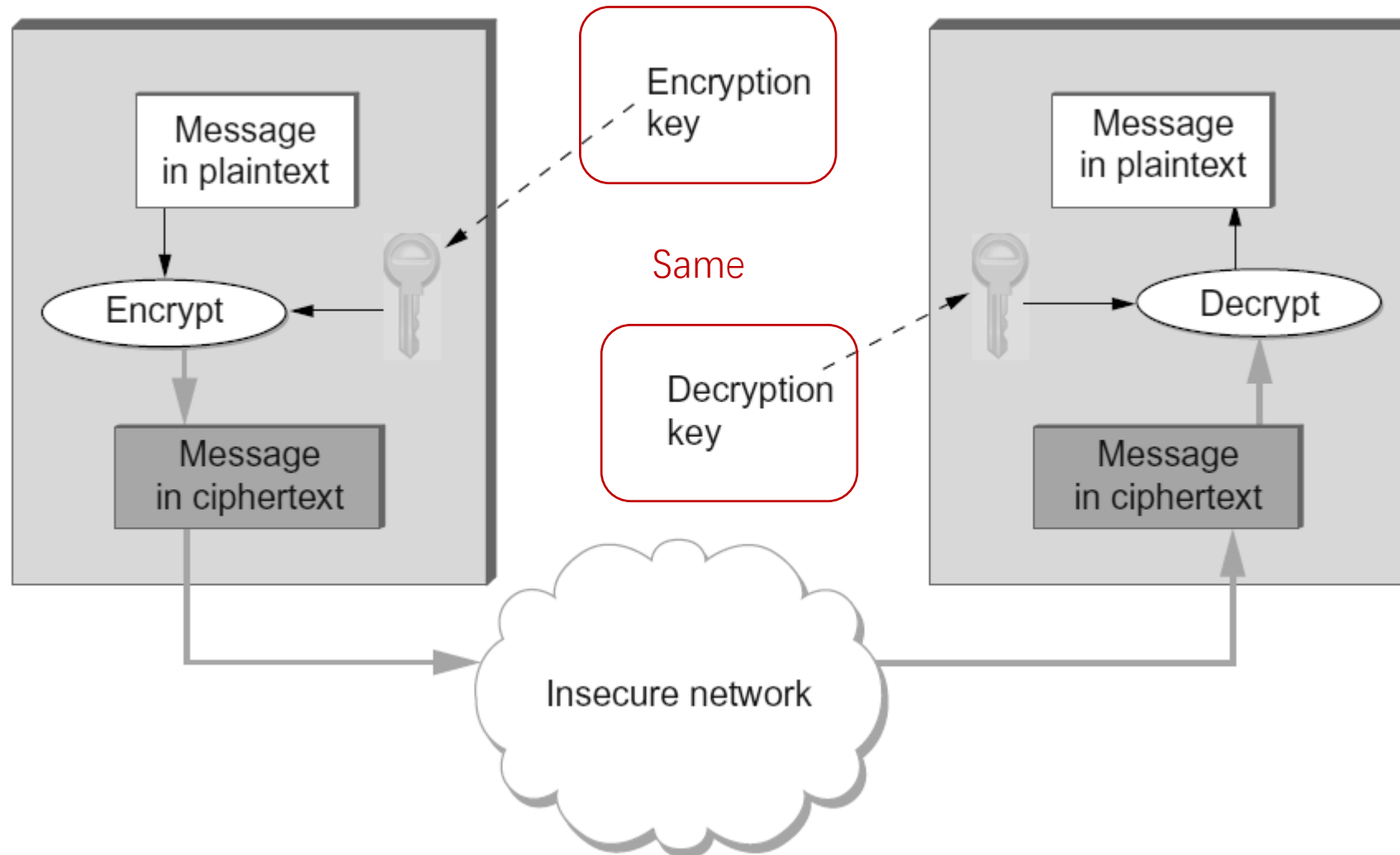
Not Scalable

Not secure after the cipher is cracked

The mechanism of the locker is public known, but the key unknown



Symmetric-Key Cipher

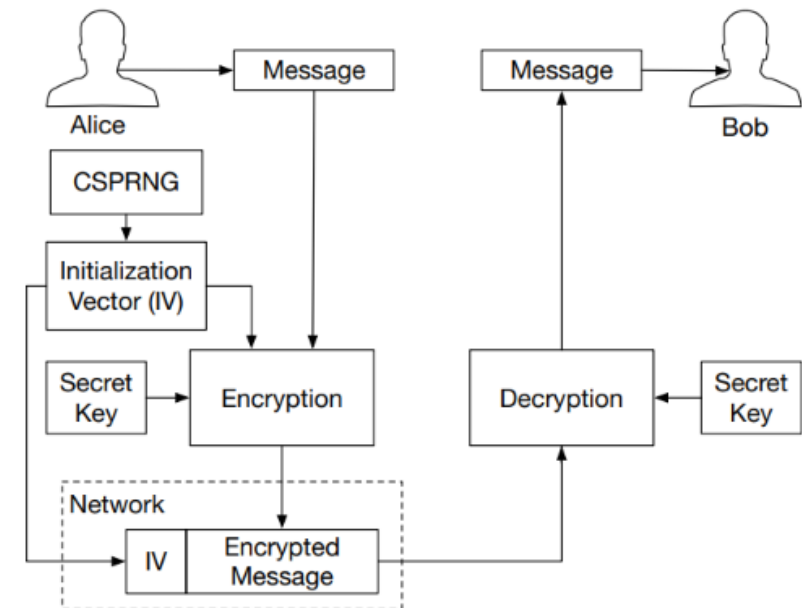
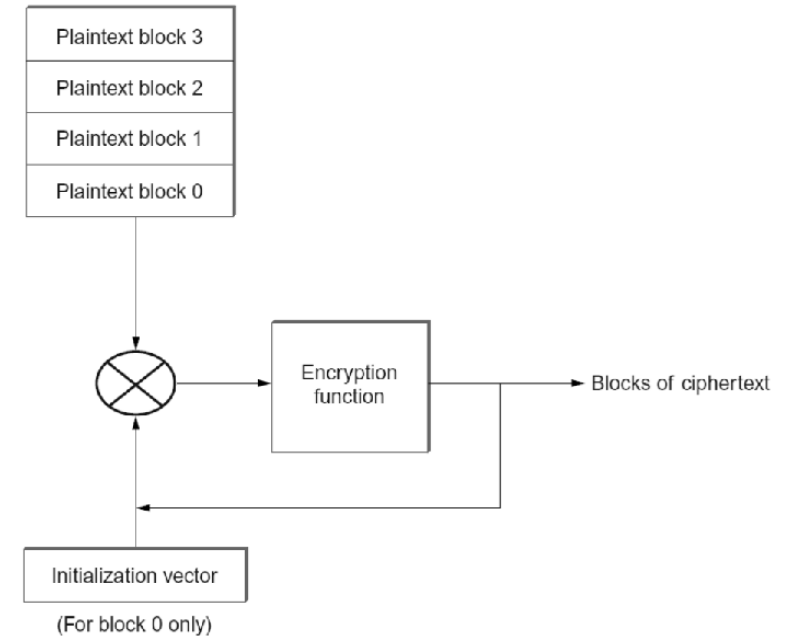


Symmetric-Key Cipher

- Examples:
 - Advanced Encryption Standard (AES)
 - Block size: $4 \times 4 = 16$ Byte (128 bit)
 - Operation: a permutation of the 128 bits according to the key
 - key size: 128, 192, 256 bit
 - <https://aesencryption.net/>

Symmetric-Key Cipher

- Ciphers are under various attacks
 - e.g., word frequency, known plaintext, etc.
- Cipher designs
 - Prevent attackers from knowing key even the attacker knows plaintext
 - Initialization Vector (IV)
 - Cipher Block Chaining to prevent same output under same input



Symmetric-Key Cipher

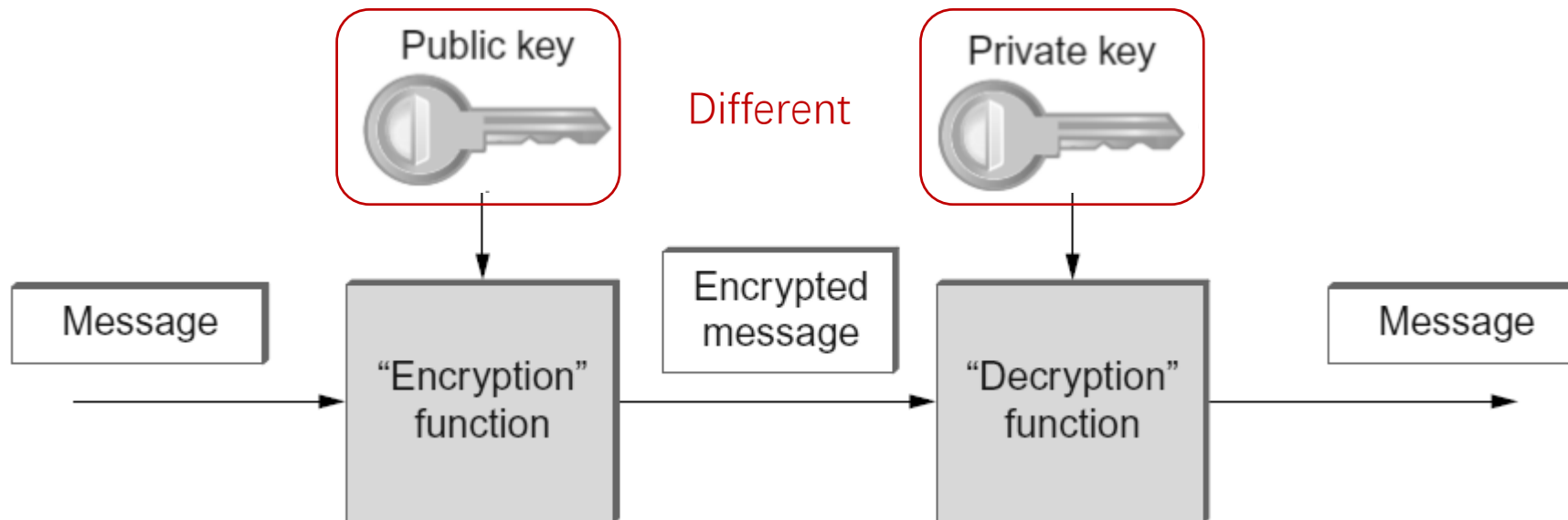
- Examples:
 - Advanced Encryption Standard (AES)
 - Block size: $4 \times 4 = 16$ Byte (128 bit)
 - Operation: a permutation of the 128 bits according to the key
 - key size: 128, 192, 256 bit
 - <https://aesencryption.net/>
 - Operation Mode
 - eg., AES-CTR
 - Initialization Vector (IV)
 - Block chaining
 - eg., Counter (CTR) and Cypher Block Chaining (CBC)

Symmetric-Key Cipher

- Problem
 - Requires sender, receiver know shared secret key
 - Q: how to agree on key in first place (particularly if never “met”)?
- This problem haven't been solved until very recently (70s)
 - -> Public-Key Cipher

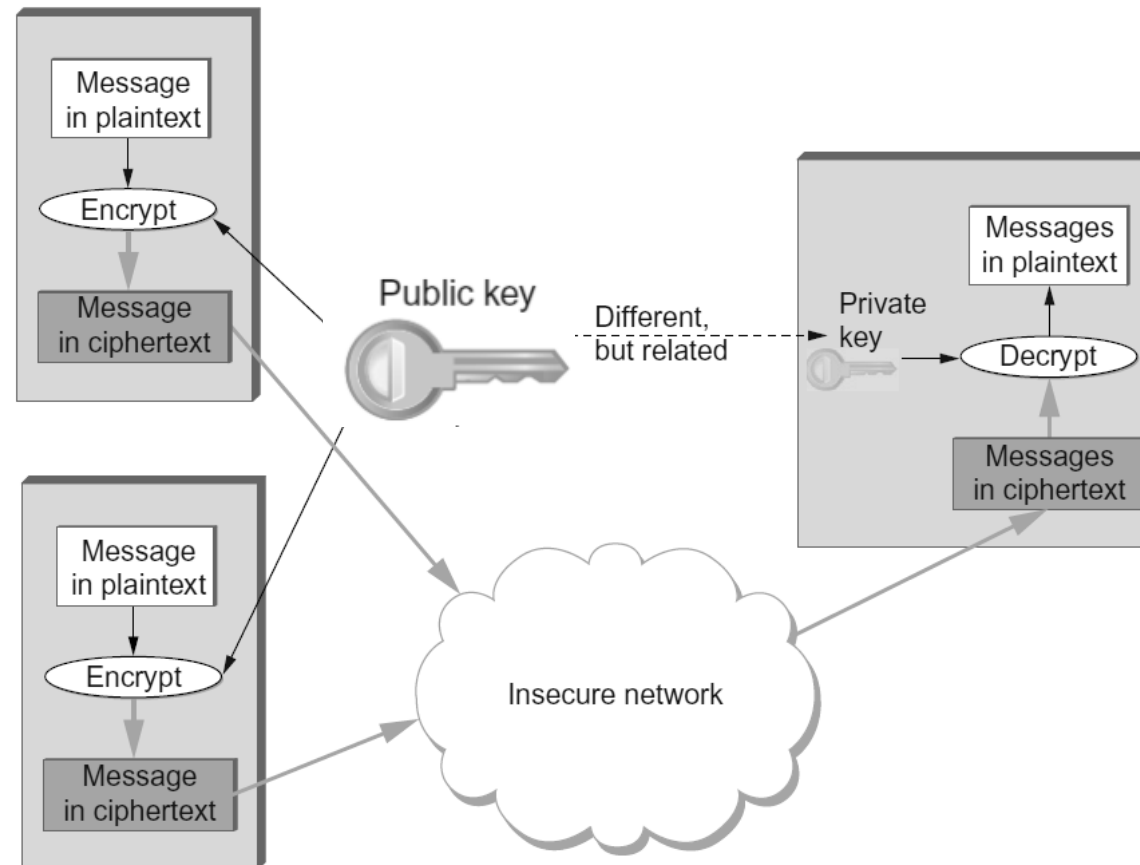
Public-Key Cipher

- If the message is encrypted with the public key
 - The message can only be decrypted with the paired private key

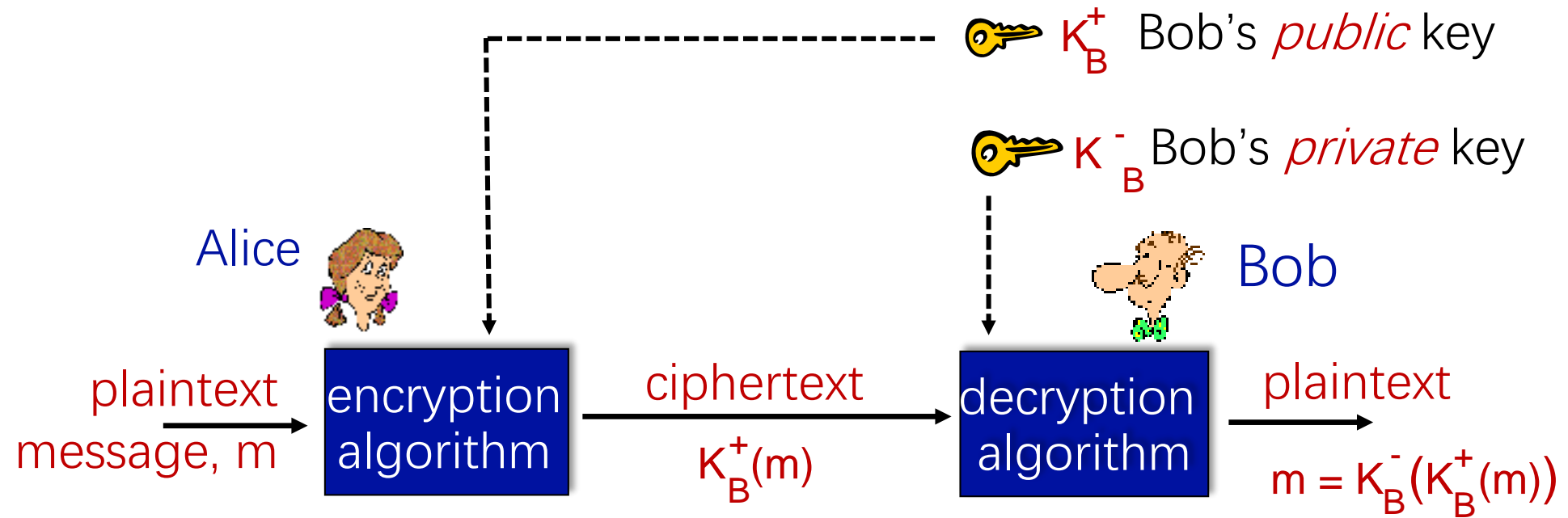


Public-Key Cipher

- For key sharing: the public key can be released to everyone !



Public-Key Cipher



Public-Key Cipher

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^-

Public-Key Cipher

- Example:
 - RSA (Rivest, Shamir, Adelson algorithm)
 - Elliptic Curve Cryptography

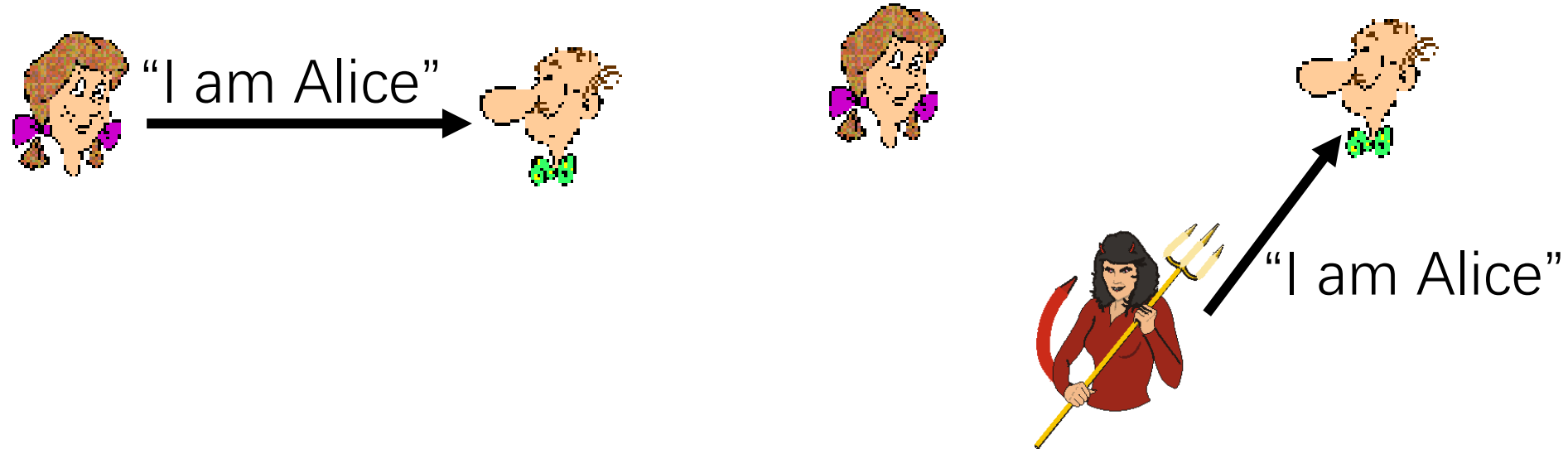
What is Network Security

- Confidentiality
 - To encrypt messages so as to prevent an adversary from understanding the message contents
- Integrity
 - To prevent an adversary from modifying the message contents.
- Availability
 - services must be accessible and available to users
- Authentication
 - To confirm identity of each other
- Timeliness
 - To identify delayed messages

Guarantee	Primitive
Confidentiality	Encryption
Integrity	MAC
Authentication	Signatures

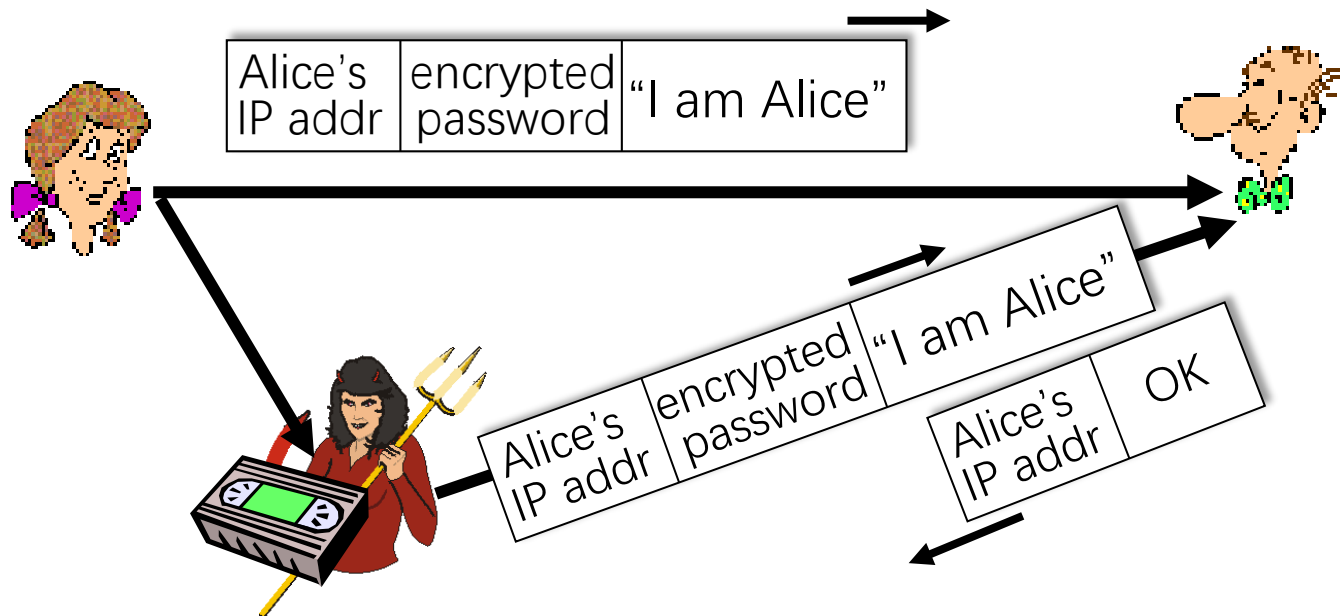
Authentication

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



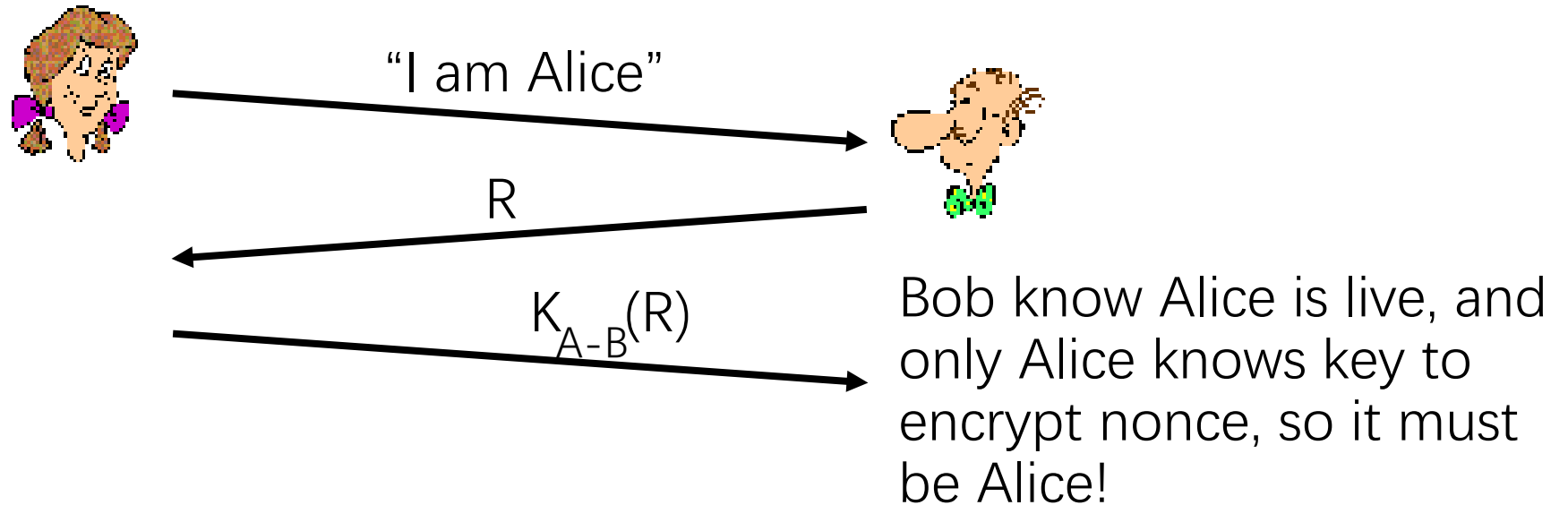
Authentication

- Solution v1
 - Alice says “I am Alice” Alice says “I am Alice” and sends her encrypted secret password to “prove” it.
 - Problem: replay



Authentication

- Solution v2
 - + challenge with a nonce
 - Need symmetric key



Authentication

- Solution v3
 - Change to public cypher
 - Fact:

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

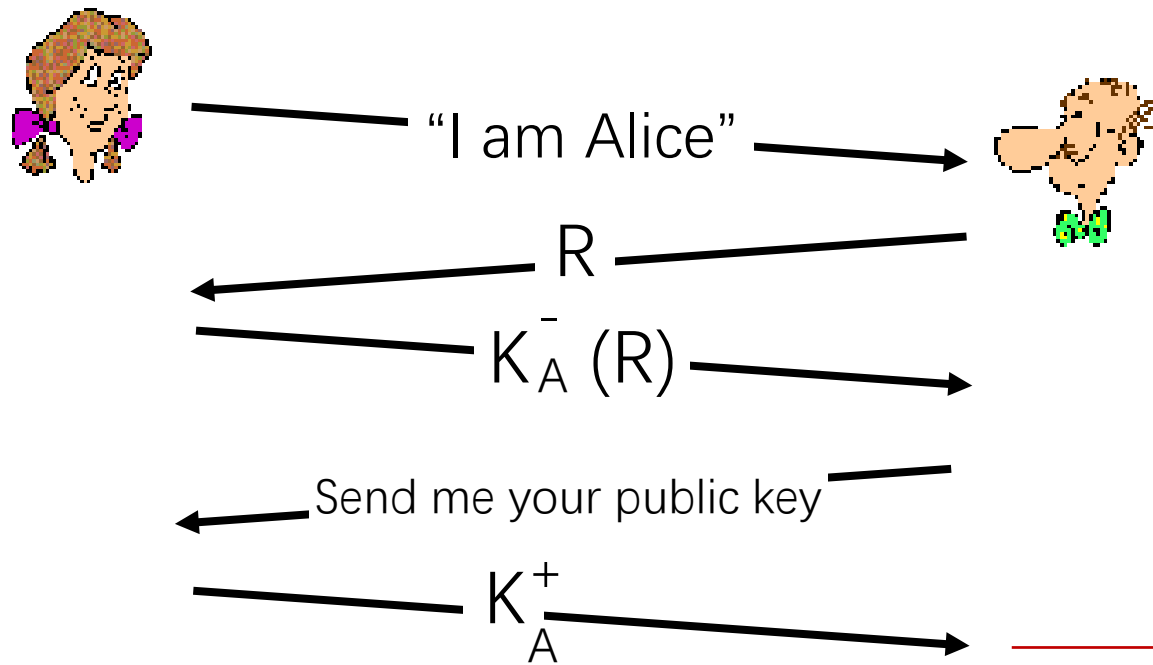
use public key
first, followed
by private key

use private key
first, followed
by public key

result is the same!

Authentication

- Solution v3
 - Change to public cypher



Bob computes

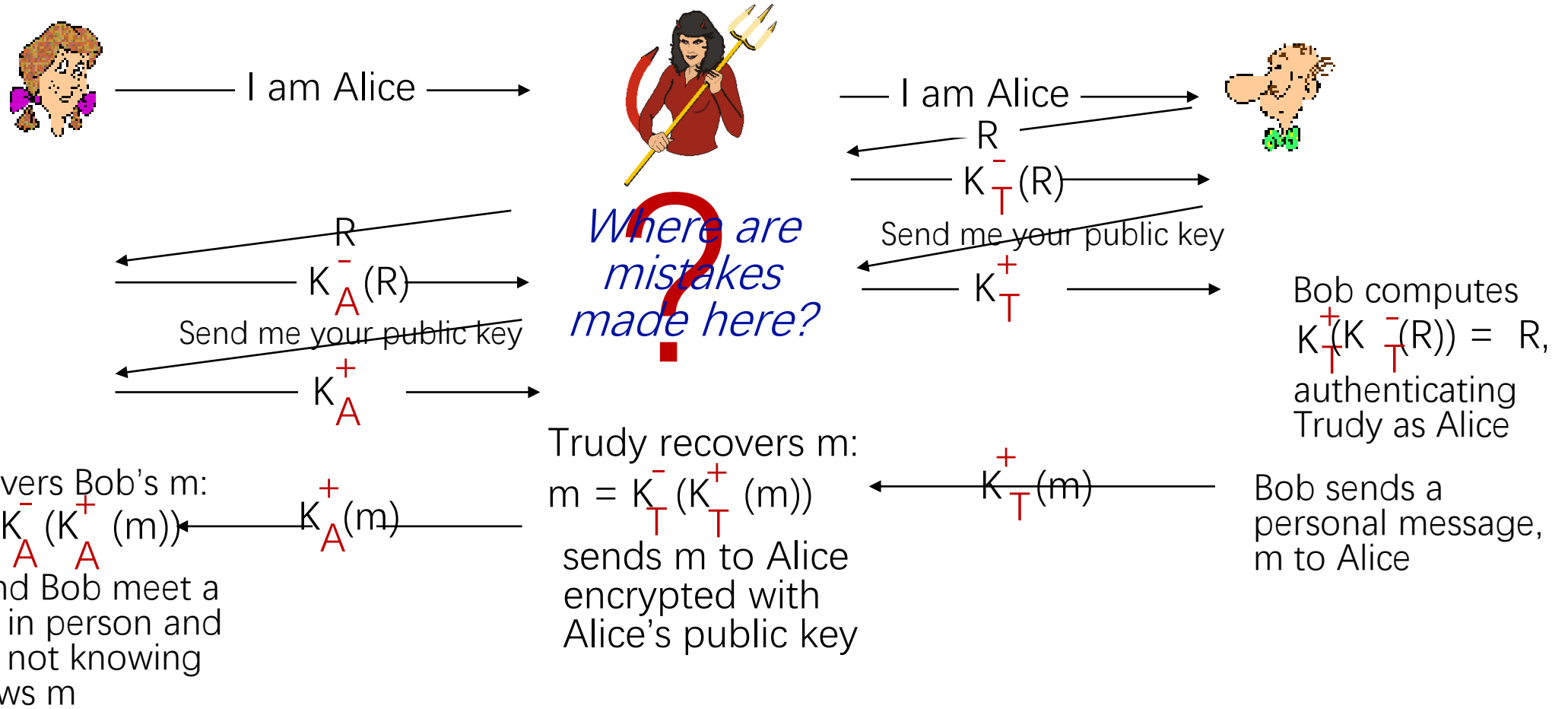
$$K_A^+(K_A^-(R)) = R$$

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

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

Authentication

- Solution v3
 - Still has a flaw: man in the middle !



Key Predistribution

- Distribute through Offline Channel
 - Not scalable




Public-Key Predistribution

• Endorsement

LinkedIn Account Type: Basic | Upgrade Mehrdad

Home Profile Contacts Groups Jobs Inbox Companies News More People

 SKILLS & EXPERTISE

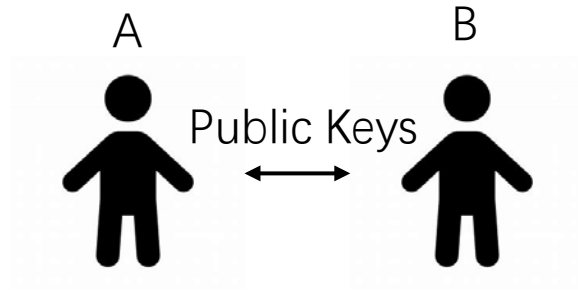
Most endorsed for...

39	Corporate Social...	
25	Sustainability	
21	Environmental Impact...	
13	Sustainability Reporting	
11	Stakeholder Engagement	
6	Capacity Building	
5	Equator Principles	
5	Due Diligence	
5	Social Impact Assessment	
4	Biodiversity	

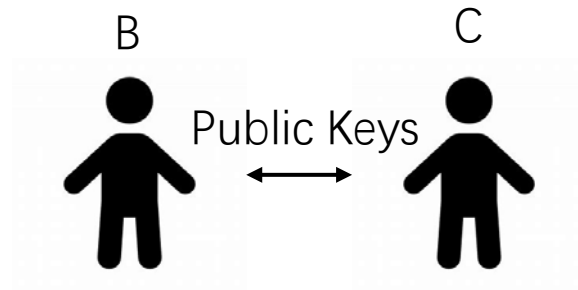
Mehrdad also knows about...



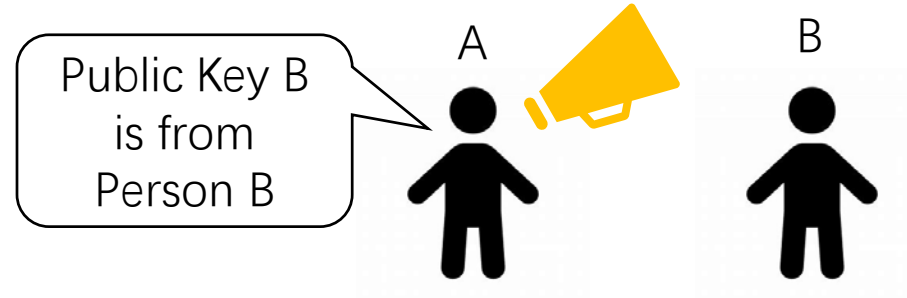
Public-Key Predistribution



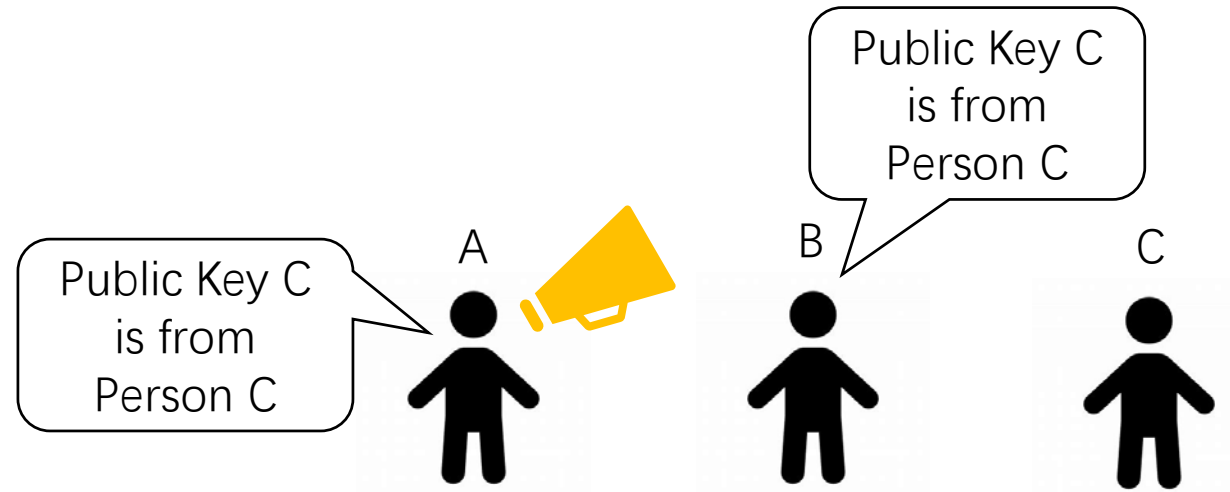
Step 1. Verify Each Other Offline;
Exchange Public Keys



Step 3. Verify Each Other Offline;
Exchange Public Keys



Step 2. Certifies Public Keys



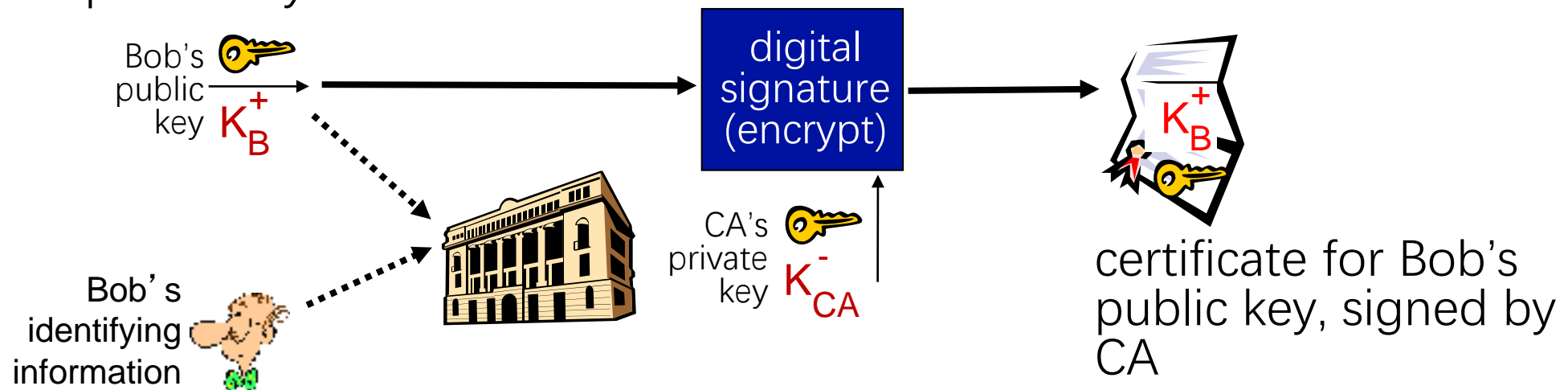
Step 4. Certifies Public Keys from Others

Public-Key Predistribution

- Certificate Authority (CA)
 - Preinstall trusted public keys
- Web of Trust
 - Collect public keys from known people

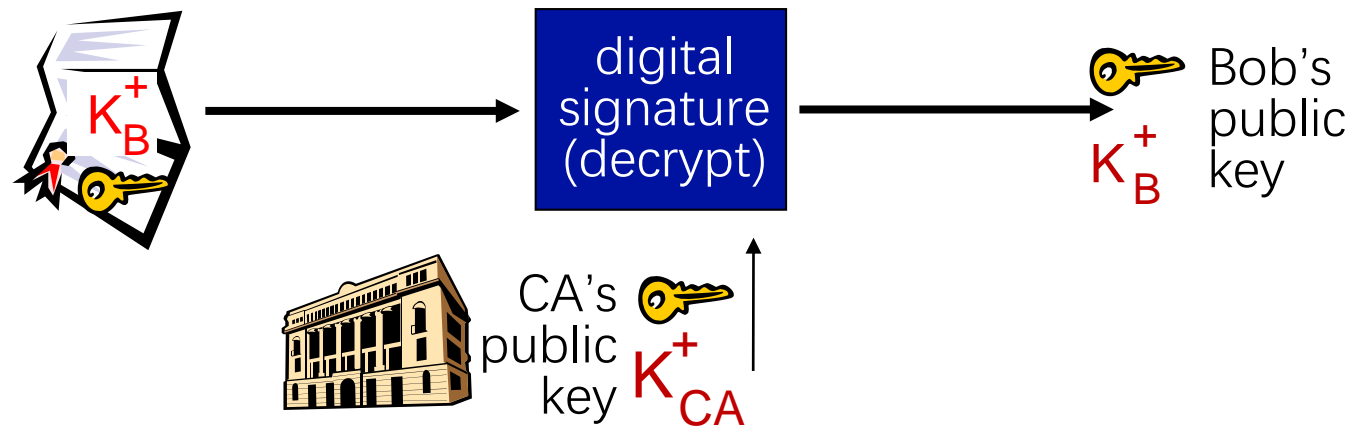
Public-Key Certification Authorities (CA)

- **Certification authority (CA):** binds public key to particular entity, E
- entity (person, website, router) registers its public key, provides “proof of identity” to CA
 - CA creates certificate binding identity E to E’s public key
 - certificate containing E’s public key digitally signed by CA: CA says “this is E’s public key”



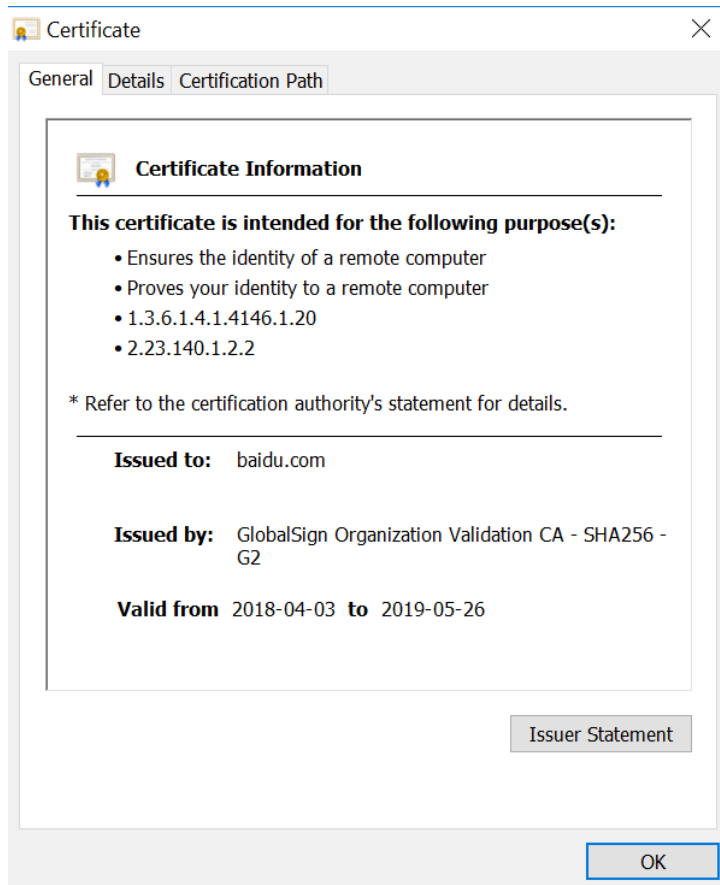
Public-Key Certification Authorities (CA)

- 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



Public-Key Predistribution

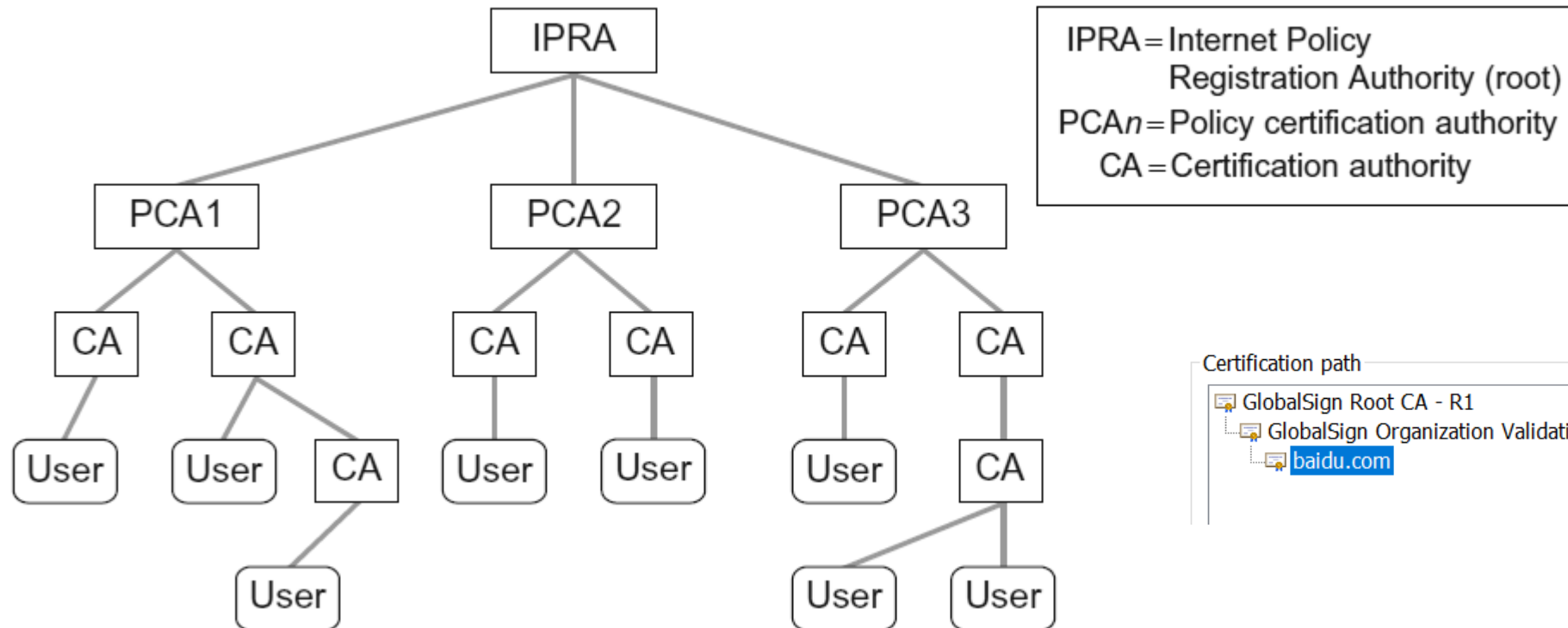
- Certificate



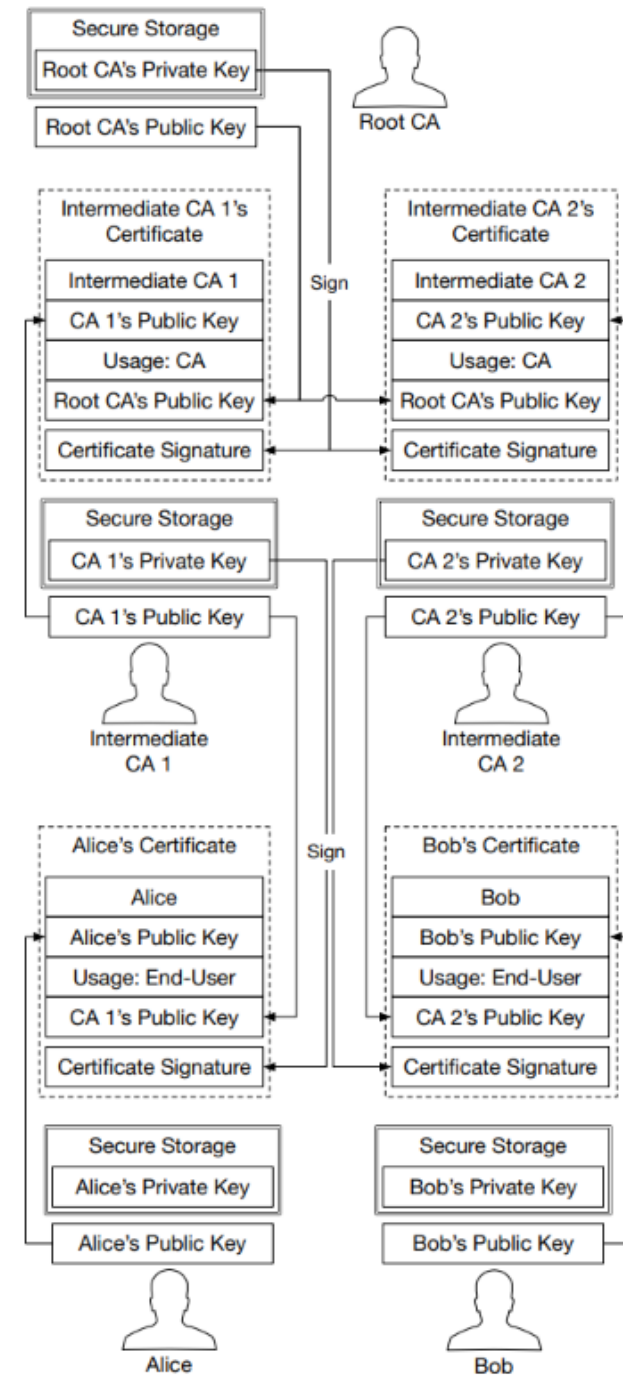
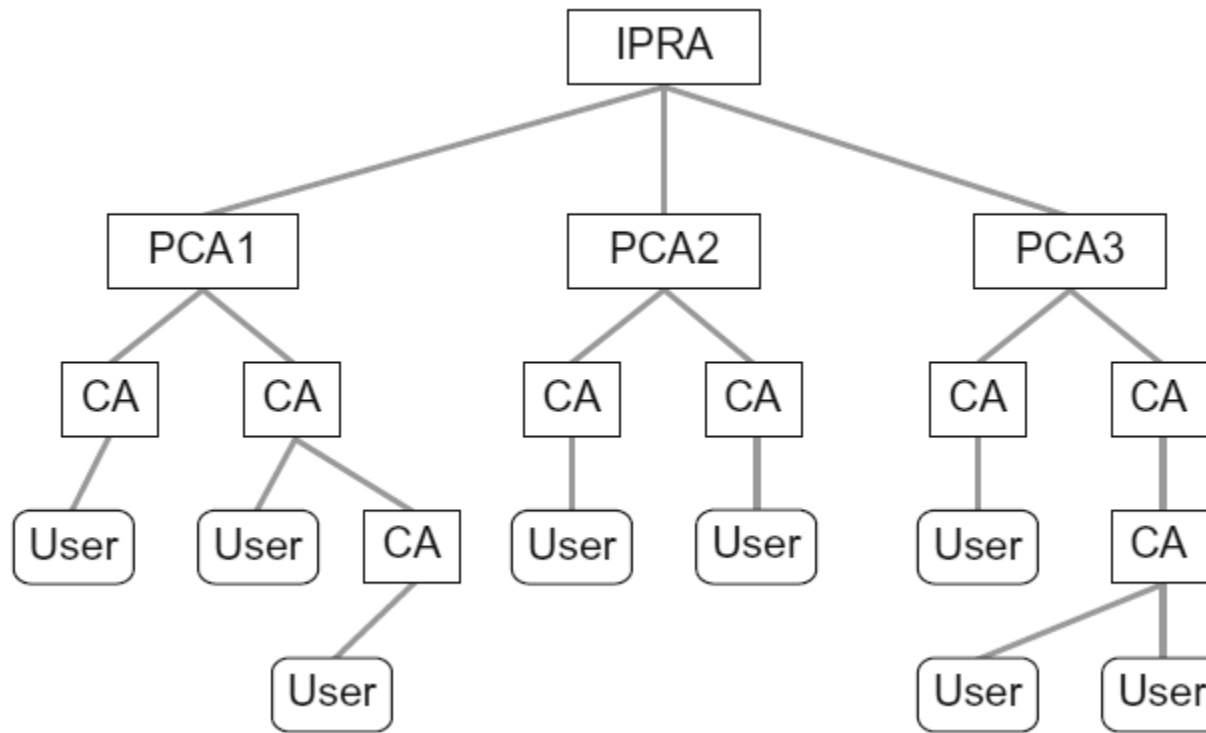
- The identity of the entity being certified
- The public key of the entity being certified
- The identity of the signer
- The digital signature of the signer
- A digital signature algorithm identifier (which cryptographic hash and which cipher)

Public-Key Predistribution

- Certificate Authority (CA)



Public-Key Predistribution



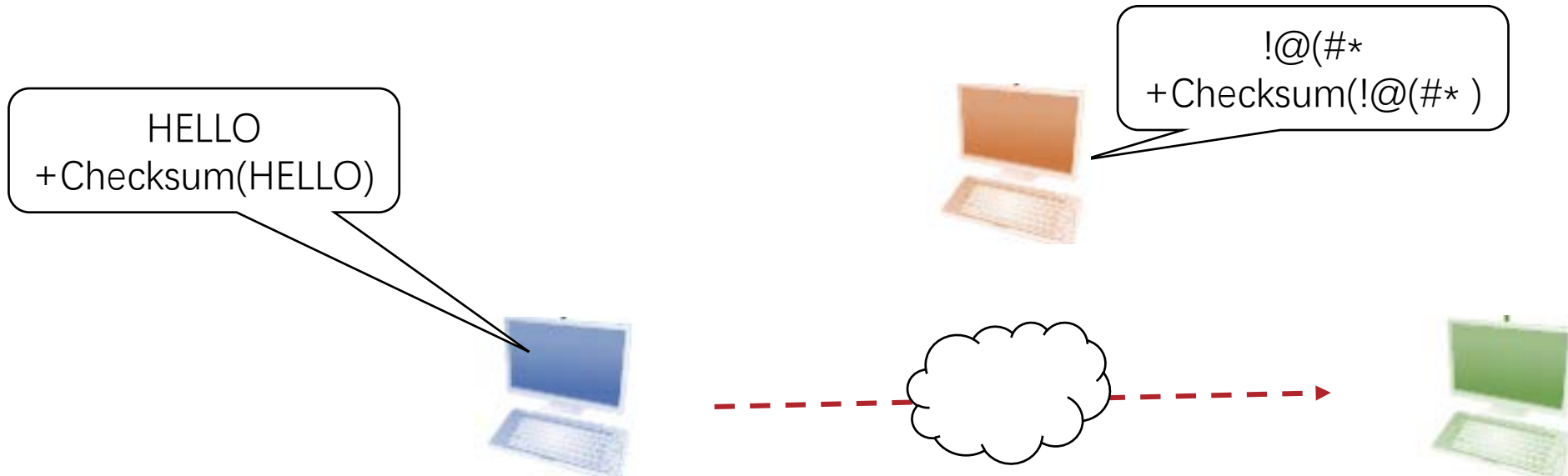
What is Network Security

- Confidentiality
 - To encrypt messages so as to prevent an adversary from understanding the message contents
- Integrity
 - To prevent an adversary from modifying the message contents.
- Availability
 - services must be accessible and available to users
- Authentication
 - To confirm identity of each other
- Timeliness
 - To identify delayed messages

Guarantee	Primitive
Confidentiality	Encryption
Integrity	MAC
Authentication	Signatures

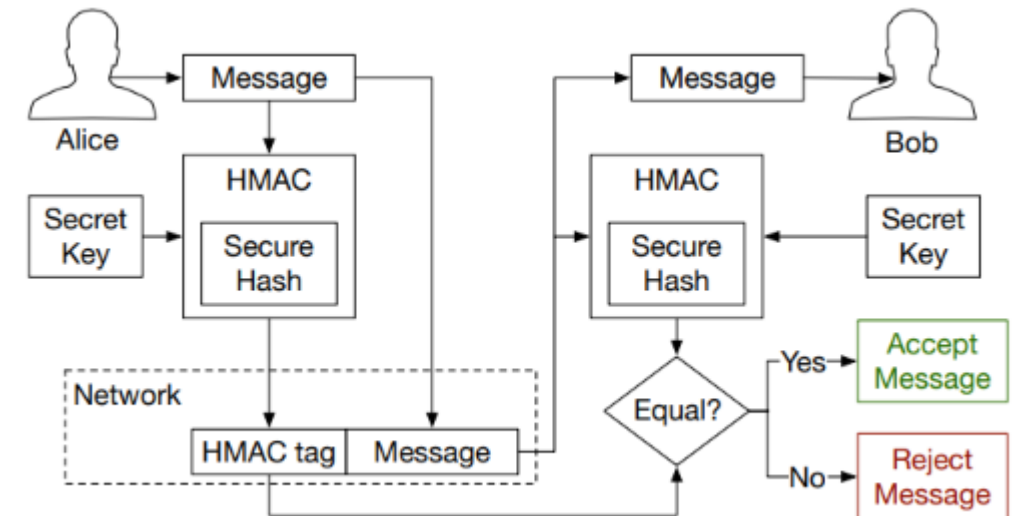
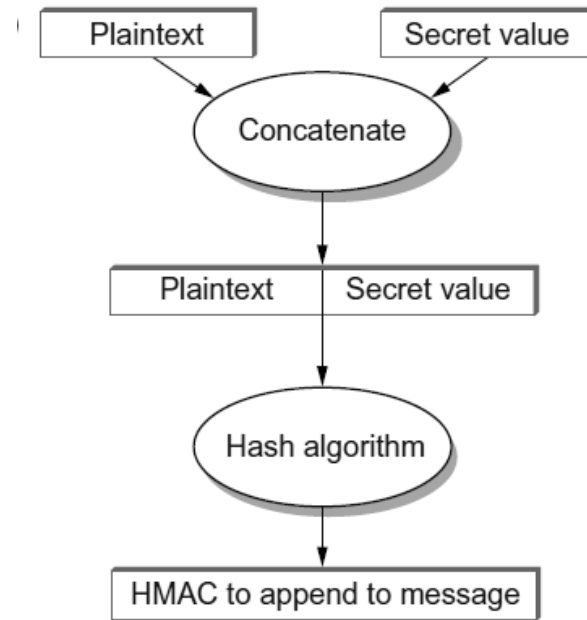
Data Integrity: Checksum

- Checksum can be replicated



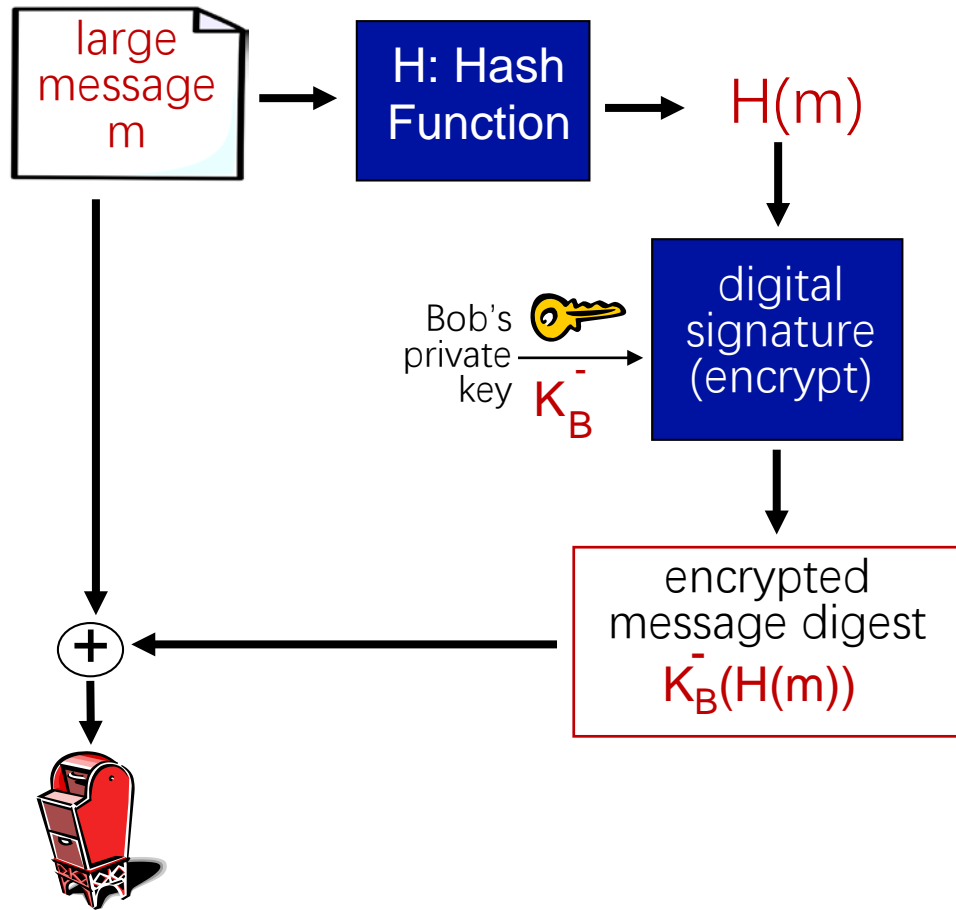
Cryptographic Hash

- Cryptographic Hash
 - Example
 - MD5
 - SHA
- HMAC
 - Hash Message Authentication Code
 - Use Cryptographic Hash Function to generate integrity and authentication check for the message.
- Digital Signature
 - Fixed-length, easy- to-compute digital “fingerprint”
 - Apply hash function H to m , get fixed size message digest, $H(m)$
 - use private key to sign the hash

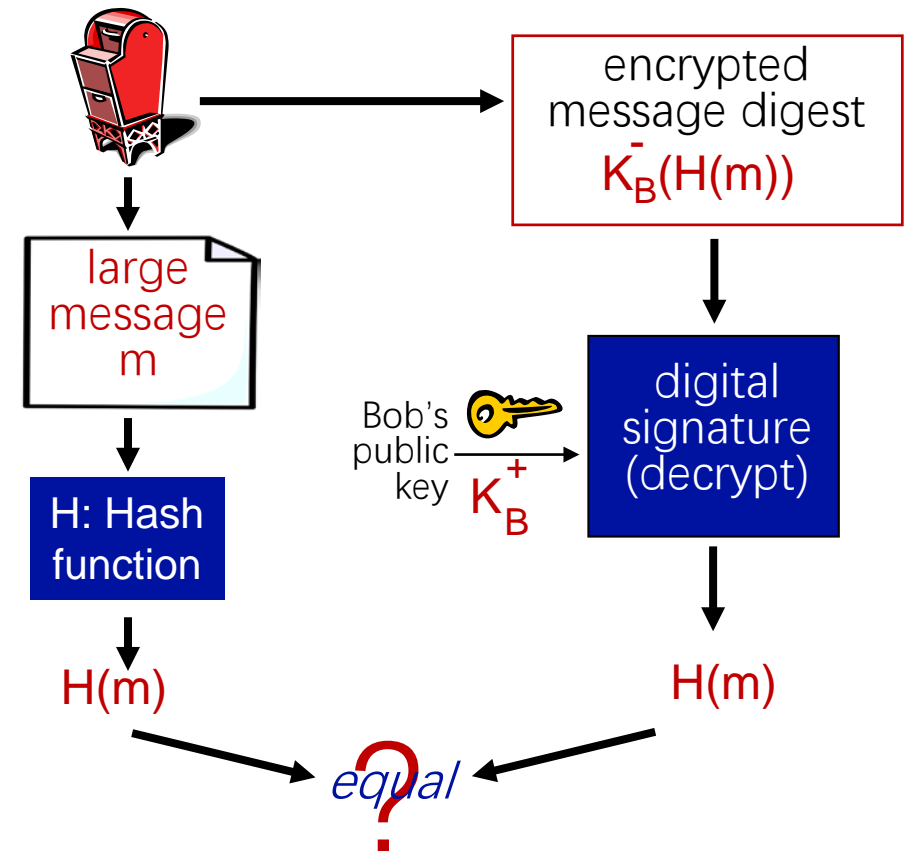


Digital Signature

Bob sends digitally signed message:



Alice verifies signature, integrity of digitally signed message:



Demo

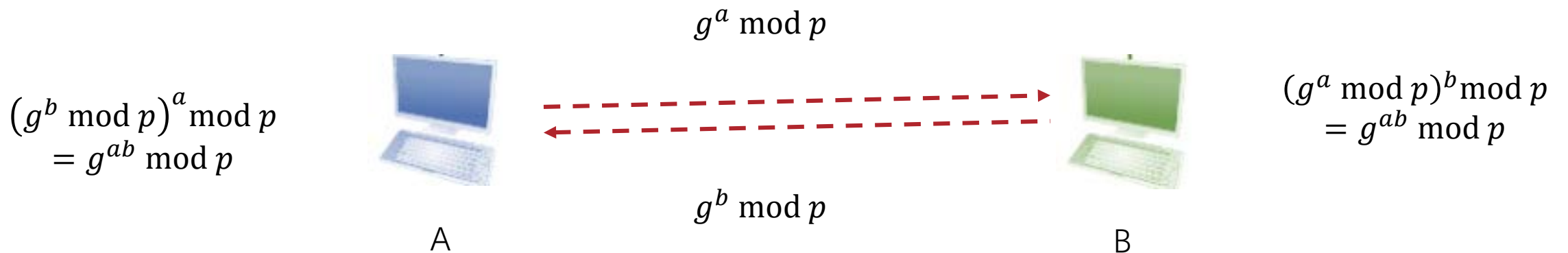
- Certificate Authority (CA)
 - certmgr.msc
 - <https://www.sinorailca.com/>

Symmetric-Key Predistribution

- Through Trust Server
- Through Public-Key Predistribution

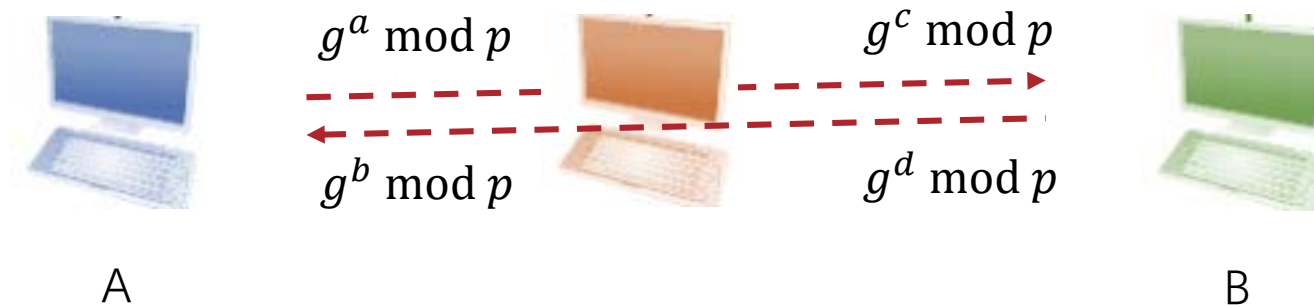
Diffie-Hellman Key Exchange

- Generate shared key without key predistribution
 - a is the secret of A
 - b is the secret of B
 - g and p are public known
 - $g^{ab} \bmod p$ is the shared key



Diffie-Hellman Key Exchange

- Man in the middle attack
 - A cannot authenticate he is talking with B
- Diffie-Hellman Key Exchange is not secure without authentication



Reference

- Textbook 8.1, 8.2, 8.3
- Some slides are adapted from http://www-net.cs.umass.edu/kurose_ross/ppt.htm by Kurose Ross