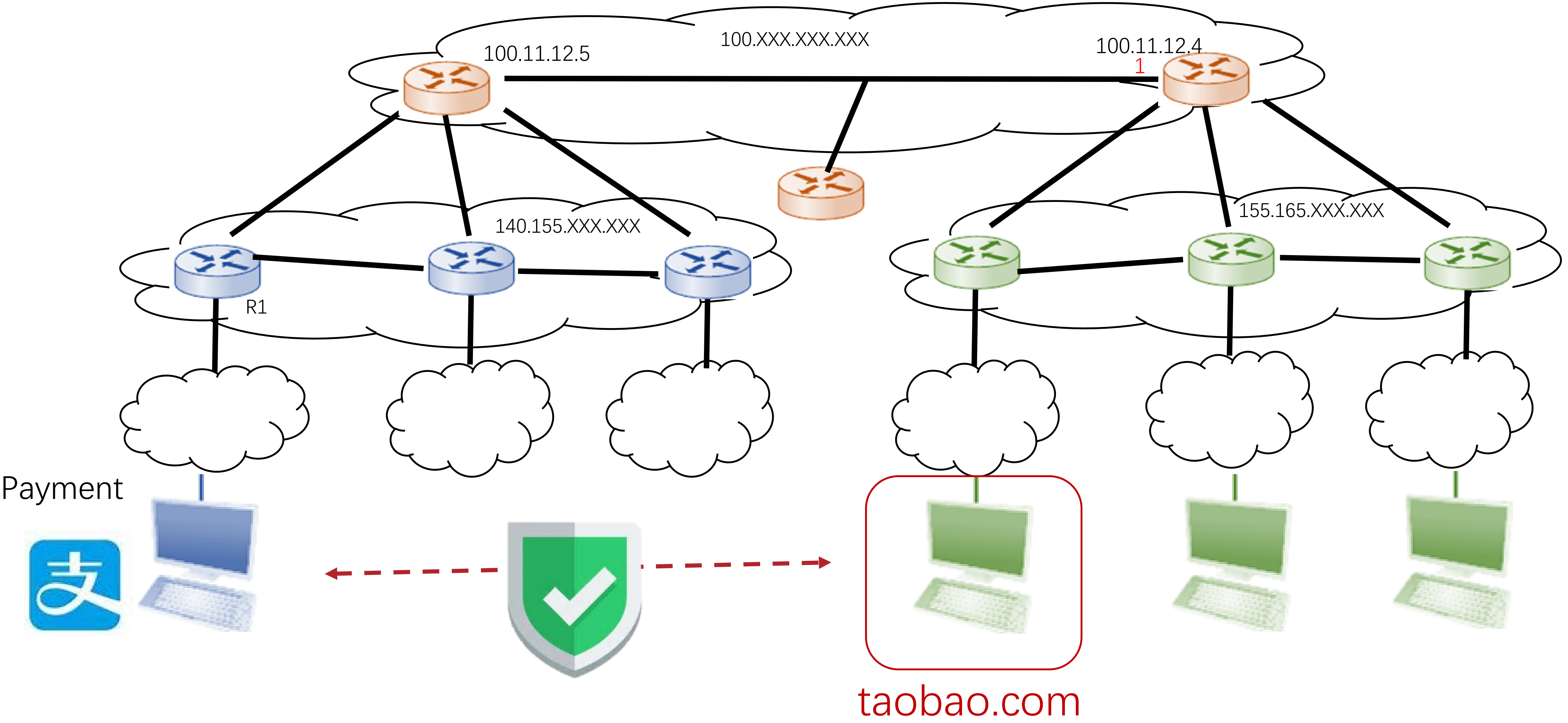
CS120: Computer Networks

Lecture 27. Network Security 1

Zhice Yang

How to Make Internet Secure ?



What is Network Security

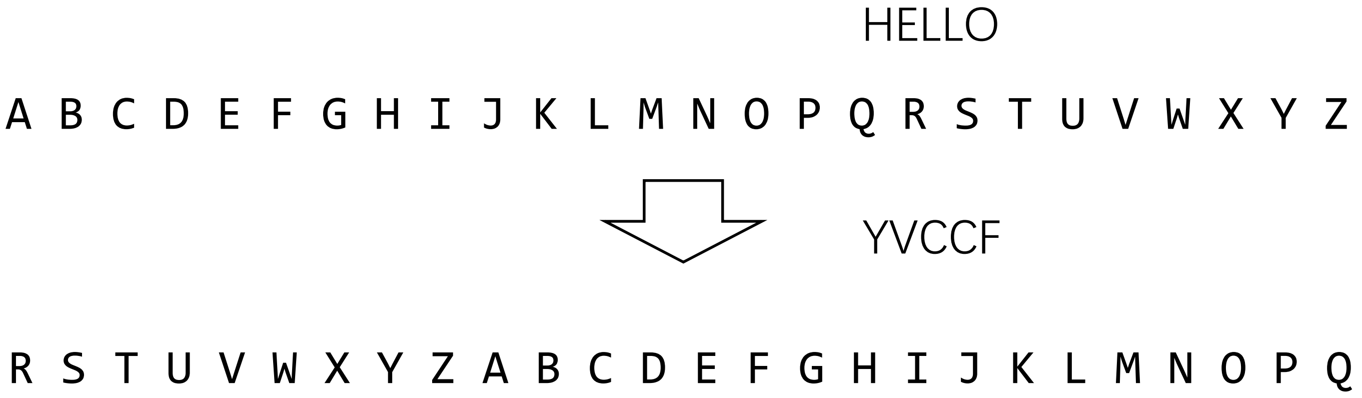
- Confidentiality
  - To encrypt messages so as to prevent an adversary from understanding the message contents
- Integrity
  - To prevent an adversary from modifying the message contents.
- Originality
  - To prevent an adversary from relaying the message
- Timeliness
  - To identify delayed messages

How to Achieve Network Security

- Cryptographic Tools
  - Symmetric-Key Cipher
  - Public-Key Cipher
  - Hash Function
- Key Predistribution Protocols
  - Public-Key Predistribution
  - Symmetric-Key Predistribution
- Authentication Protocols
  - Public-Key Authentication
  - Symmetric-Key Authentication

Cipher

- Cipher: the Cryptographic Algorithm for Encryption or Decryption



HELLO

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

YVCCF

R S T U V W X Y Z A B C D E F G H I J K L M N O P Q

Cipher

- Ciphers are normally parameterized by **keys**
  - Message: x
  - Key: k1, k2
  - Encryption function: y=En(x, k1)
  - Decryption function: x=De(y, k2)
- Key is the secret
  - The encryption function and decryption function are public known

put the valuable in
take the valuable out

CS 120 LEC 27

Cipher as a Secret ?

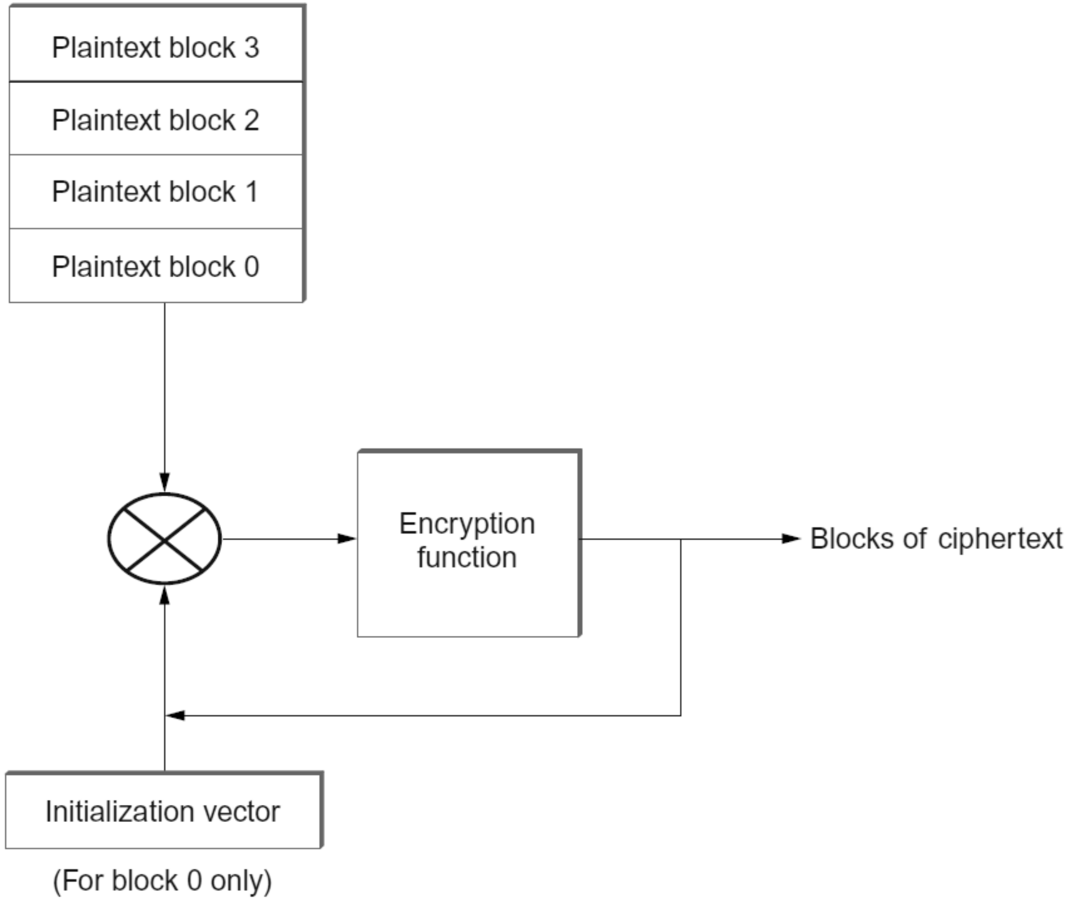
Obtain the secret by unlocking the block

Not Scalable

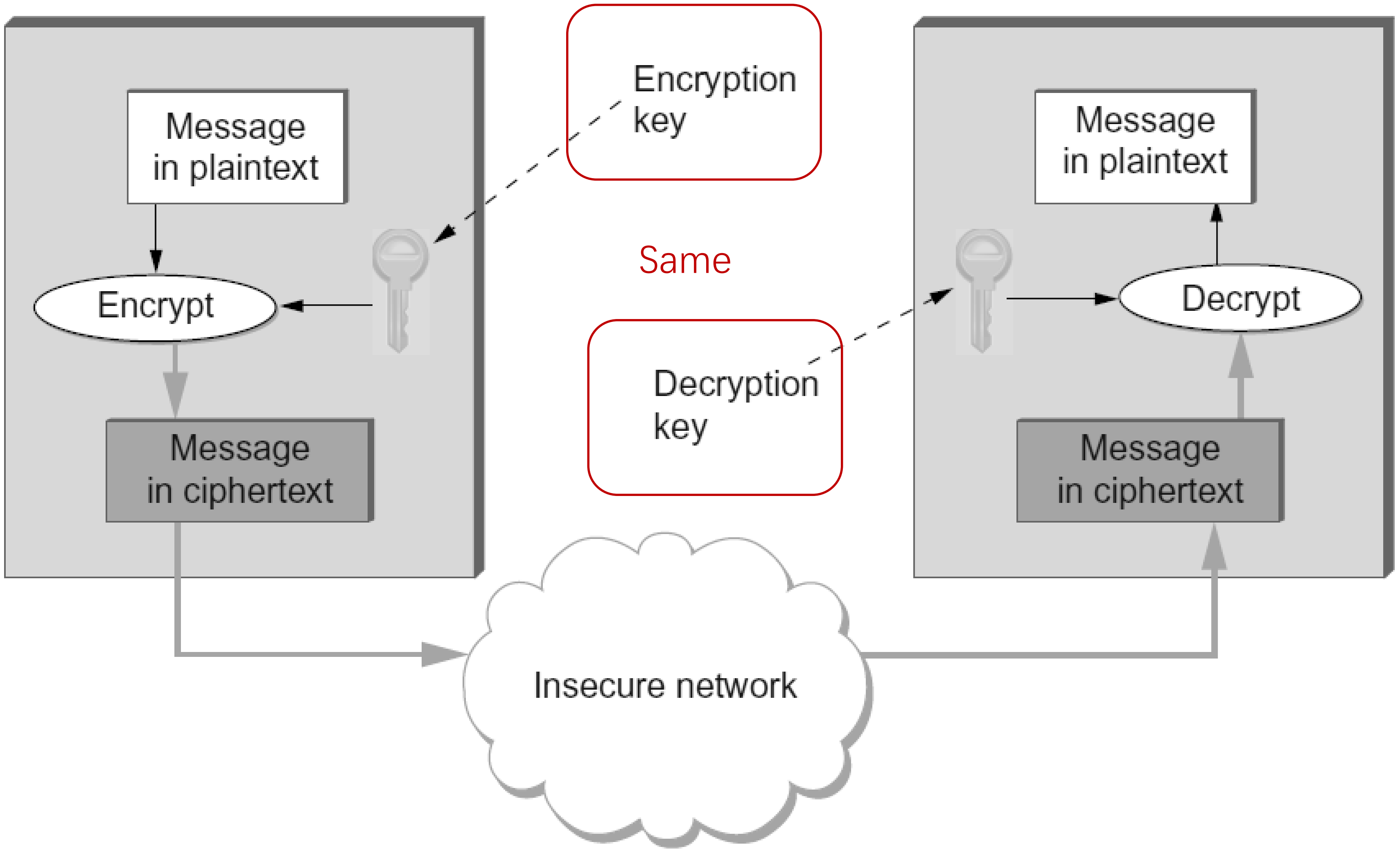
The mechanism of the locker is public known, but the key unknown

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
  - e.g., Cipher Block Chaining to prevent same output under same input



Symmetric-Key Cipher

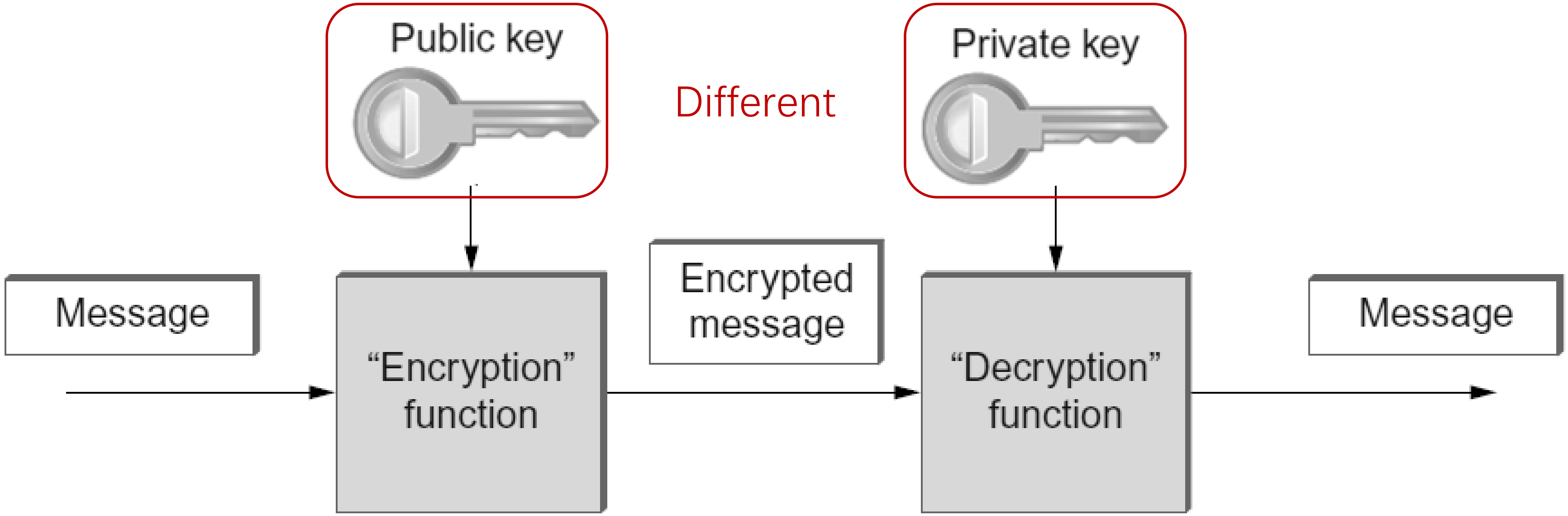


Symmetric-Key Cipher

- Examples:
  - 3DES
  - ASE
    - https://aesencryption.net/

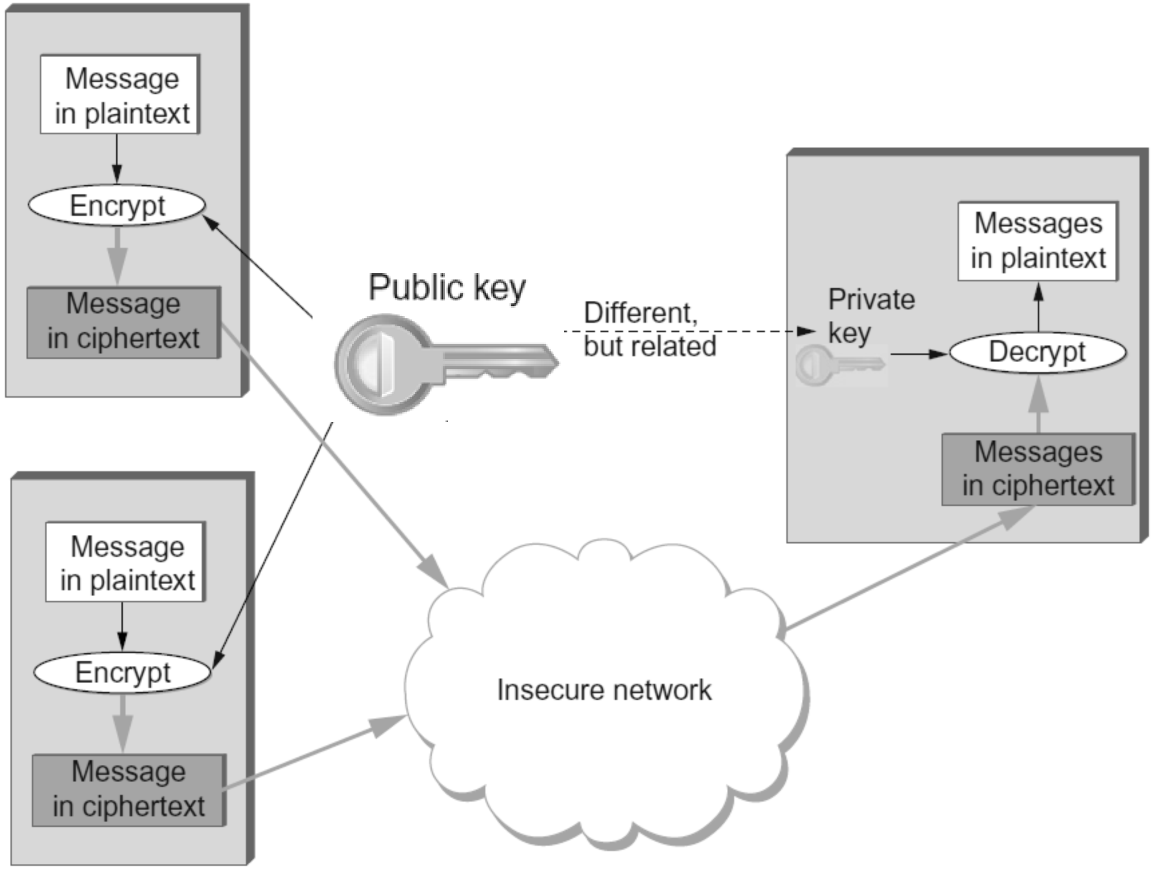
Public-Key Cipher

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



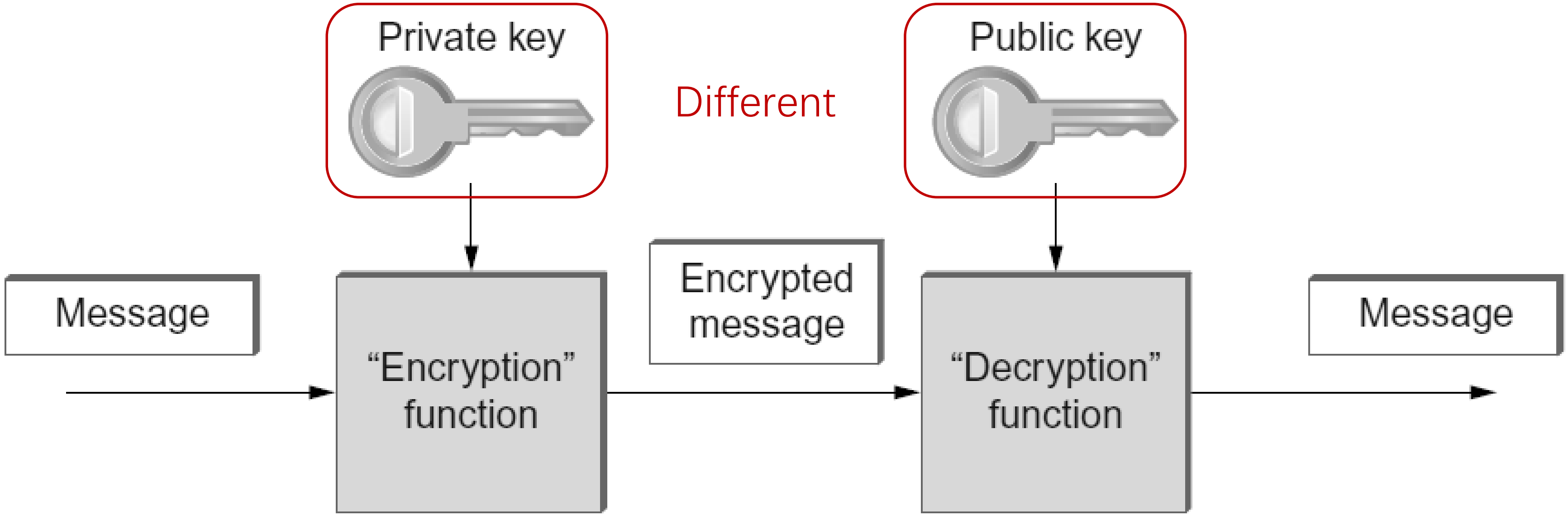
Public-Key Cipher

- For traffic confidentiality: the public key can be released to everyone



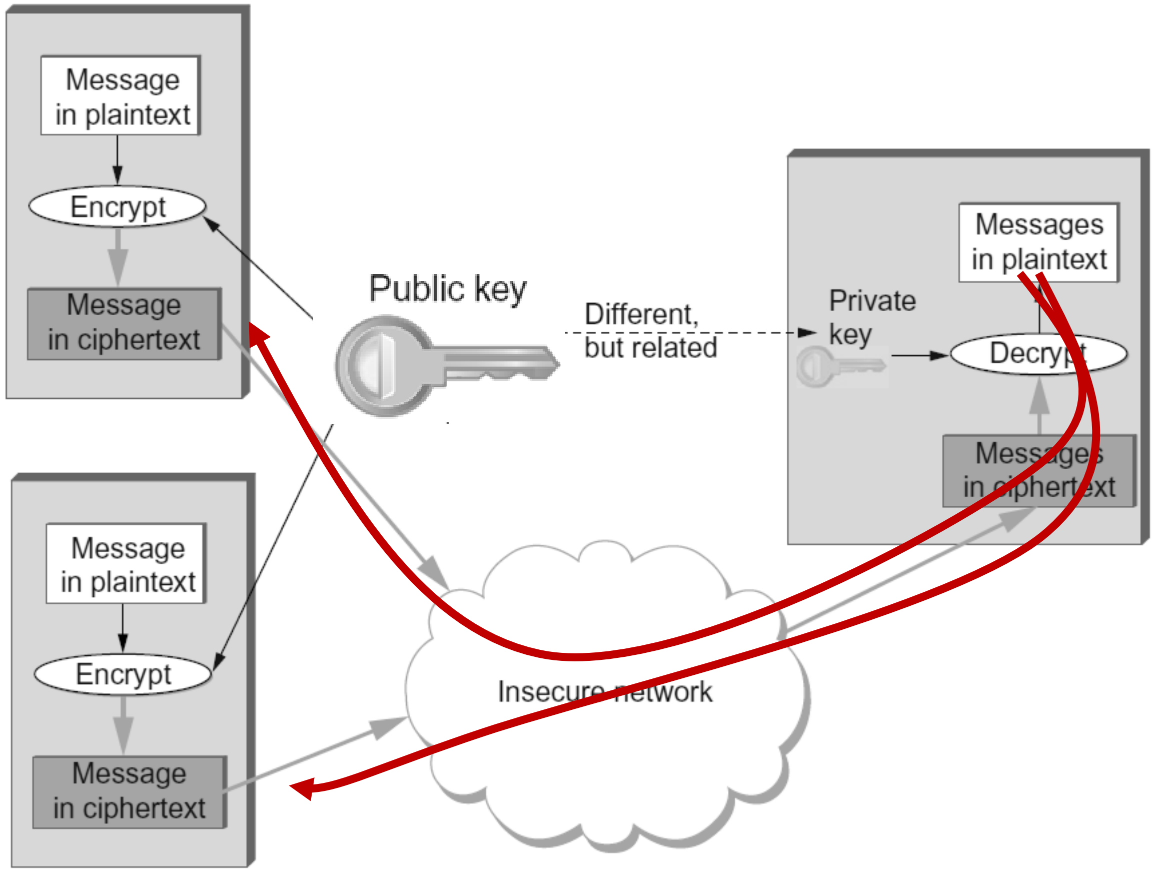
Public-Key Cipher

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



Public-Key Cipher

- For identification: the public key can be used verify if the message sender has the paired private key

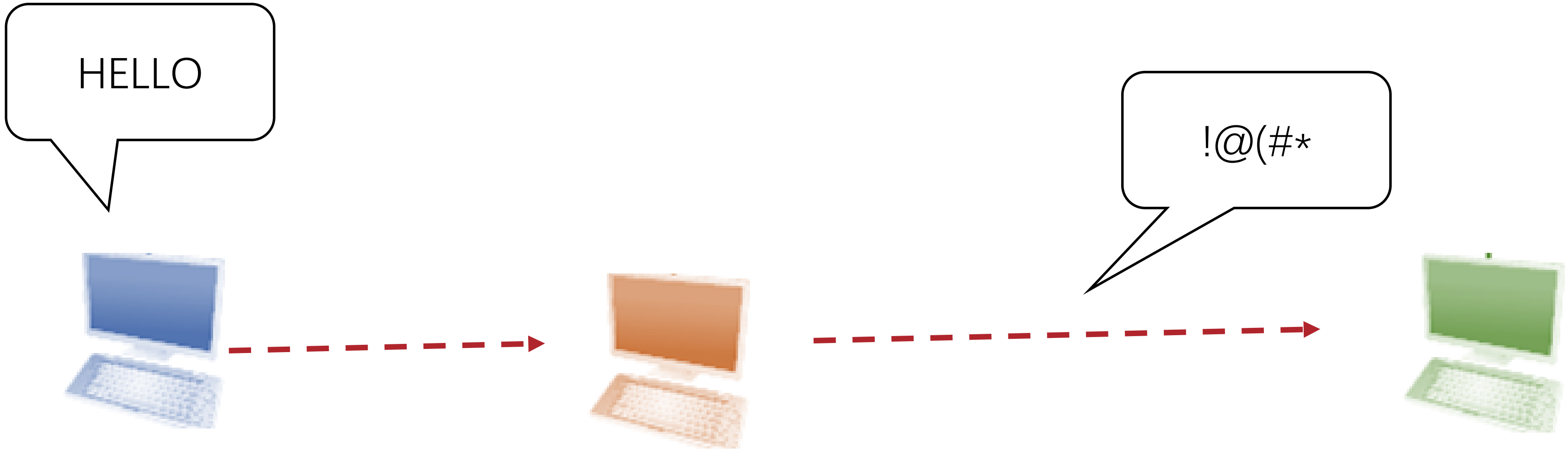


Public-Key Cipher

- Example:
  - RSA
  - Elliptic Curve Cryptography

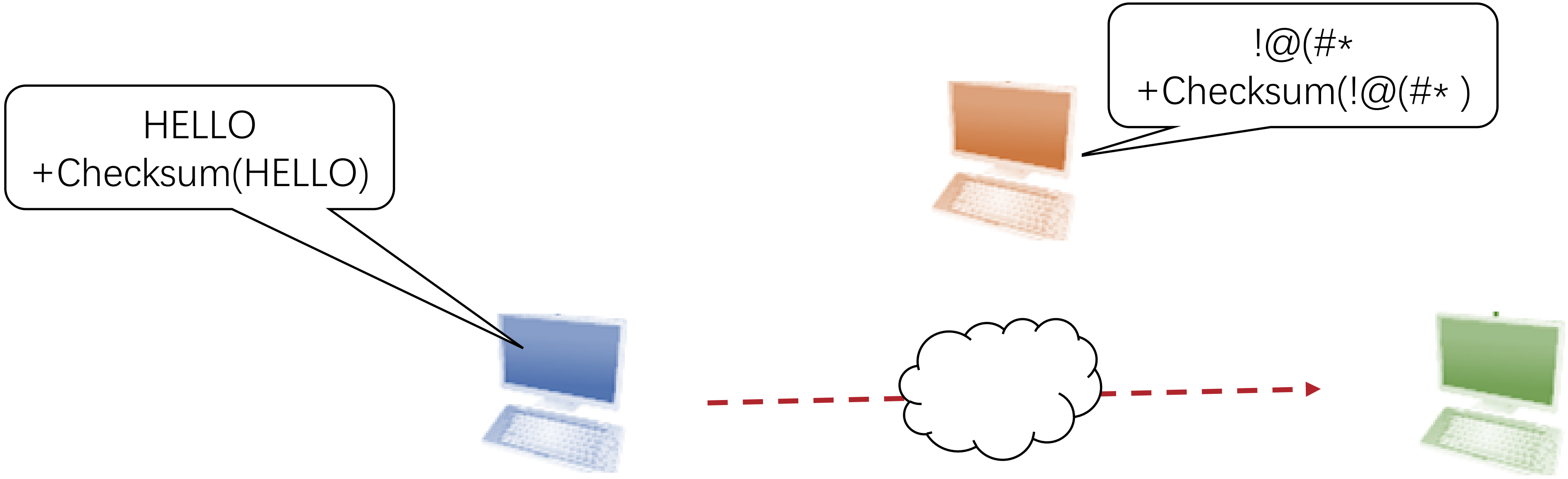
What is Network Security

- Integrity
  - To prevent an adversary from modifying the message contents.



Data Integrity: Checksum

- Checksum can be replicated

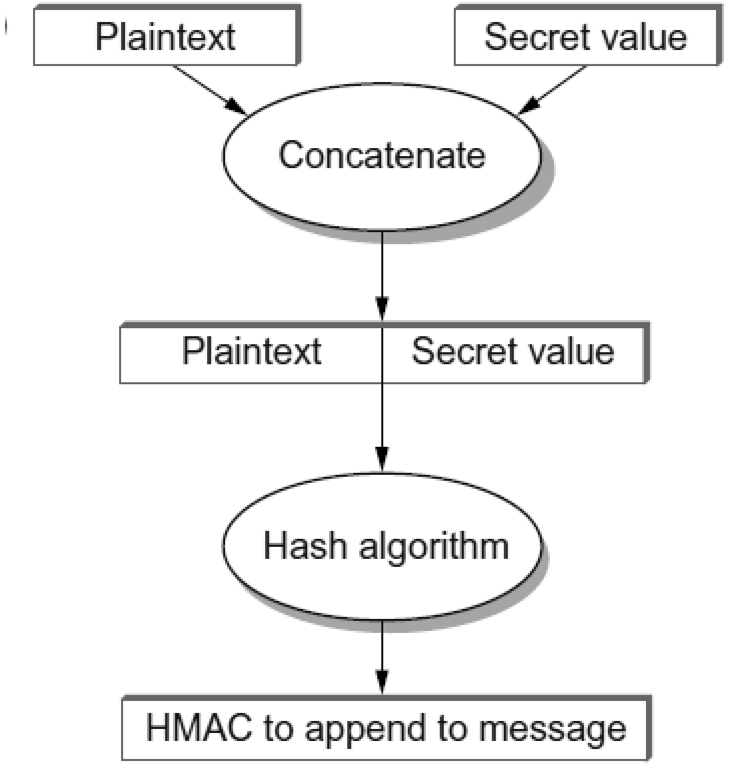


HELLO
+Checksum(HELLO)

!@(#*
+Checksum(!@(#*)

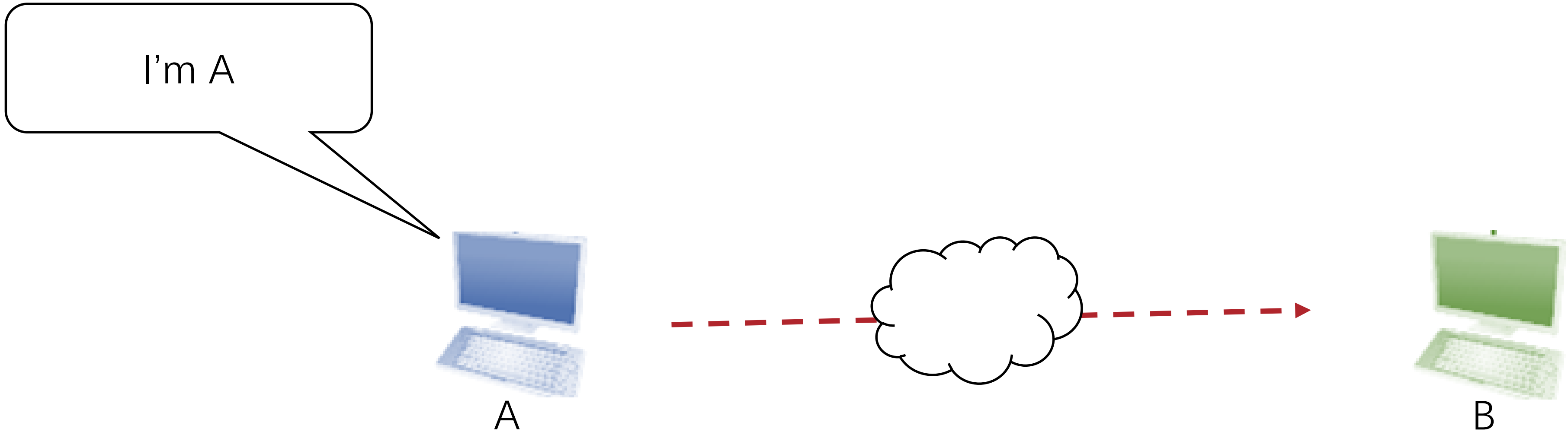
HMAC: Cryptographic Hash + Secret

- Cryptographic Hash
  - Example
    - MD5
    - SHA



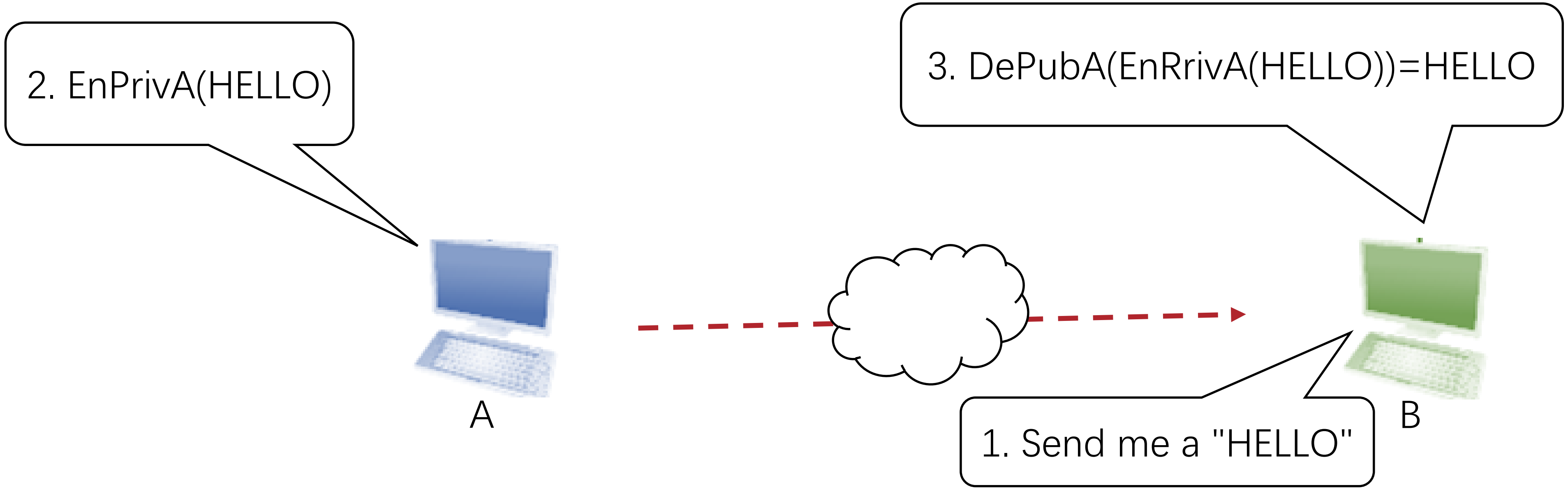
Authenticator

- Digital Signature
  - To authenticate the sender, or to give a recipient reason to believe that the message was created by a known sender

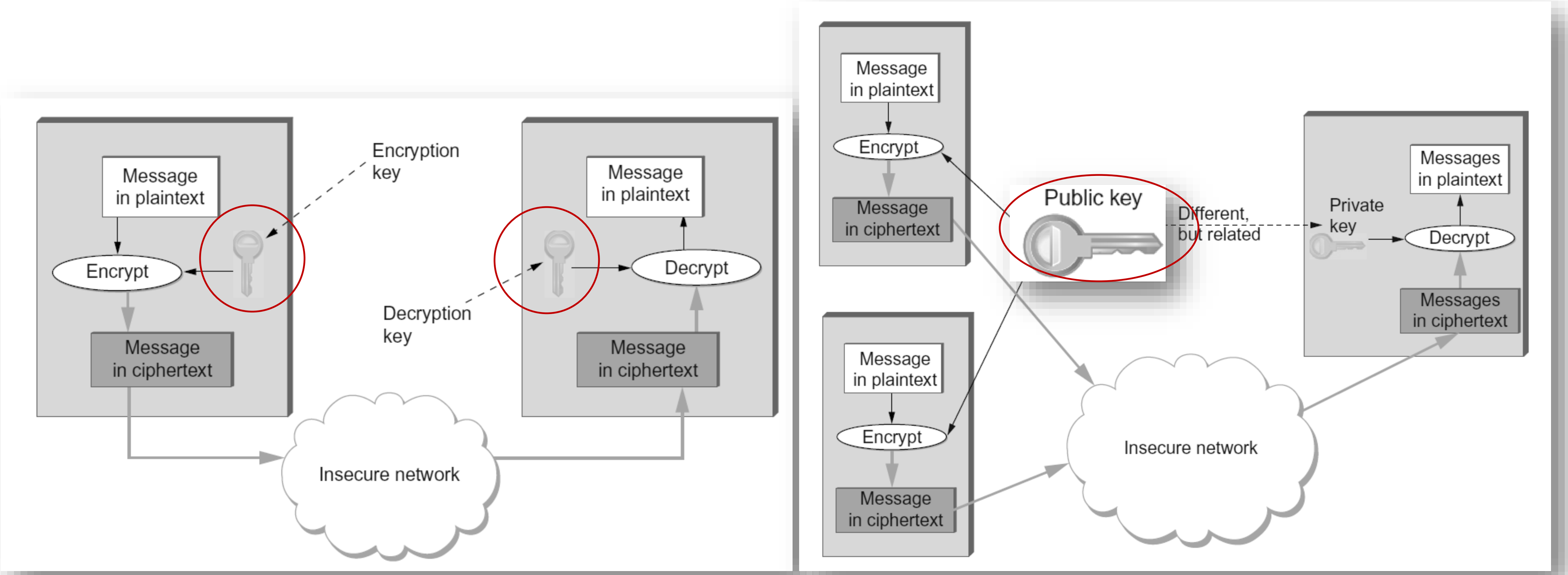


Authenticator

- Digital Signature
  - The message digest can be a signature for the sender, if the message digest is decodable with the public key of the sender
    - Everyone with a public key can challenge the private key holder



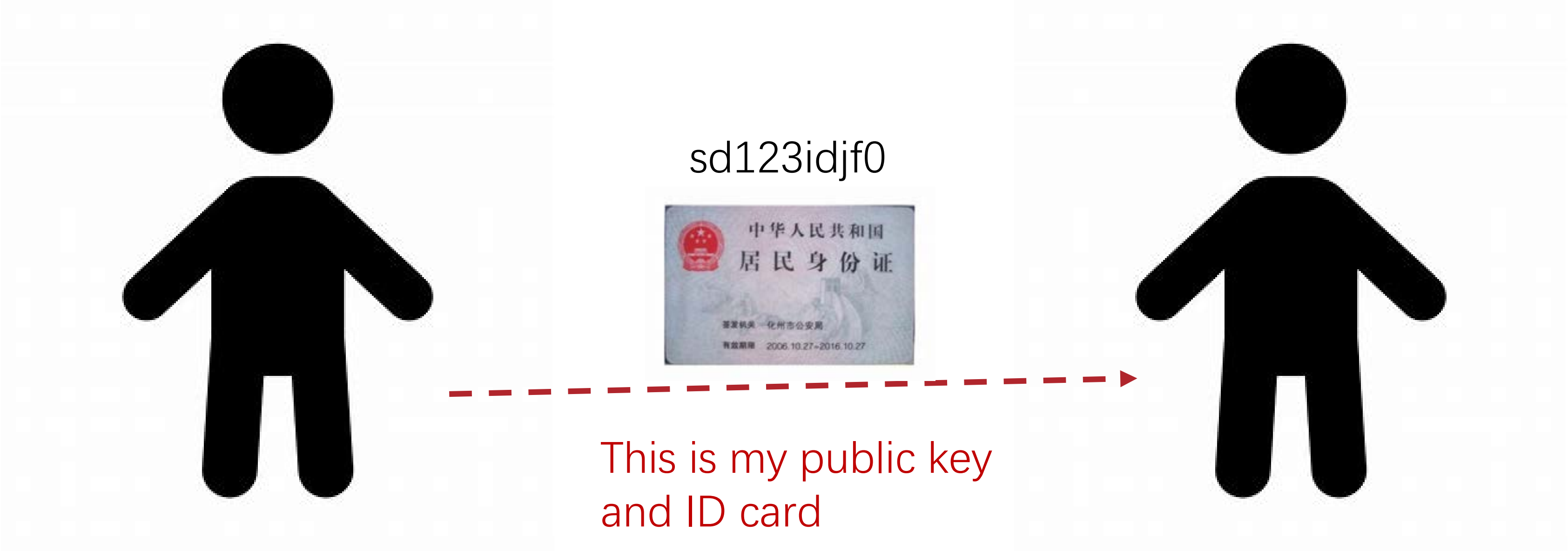
Bootstrap the First Key



How to Predistribute Keys ?

Key Predistribution

- Distribute through Offline Channel
  - Not scalable

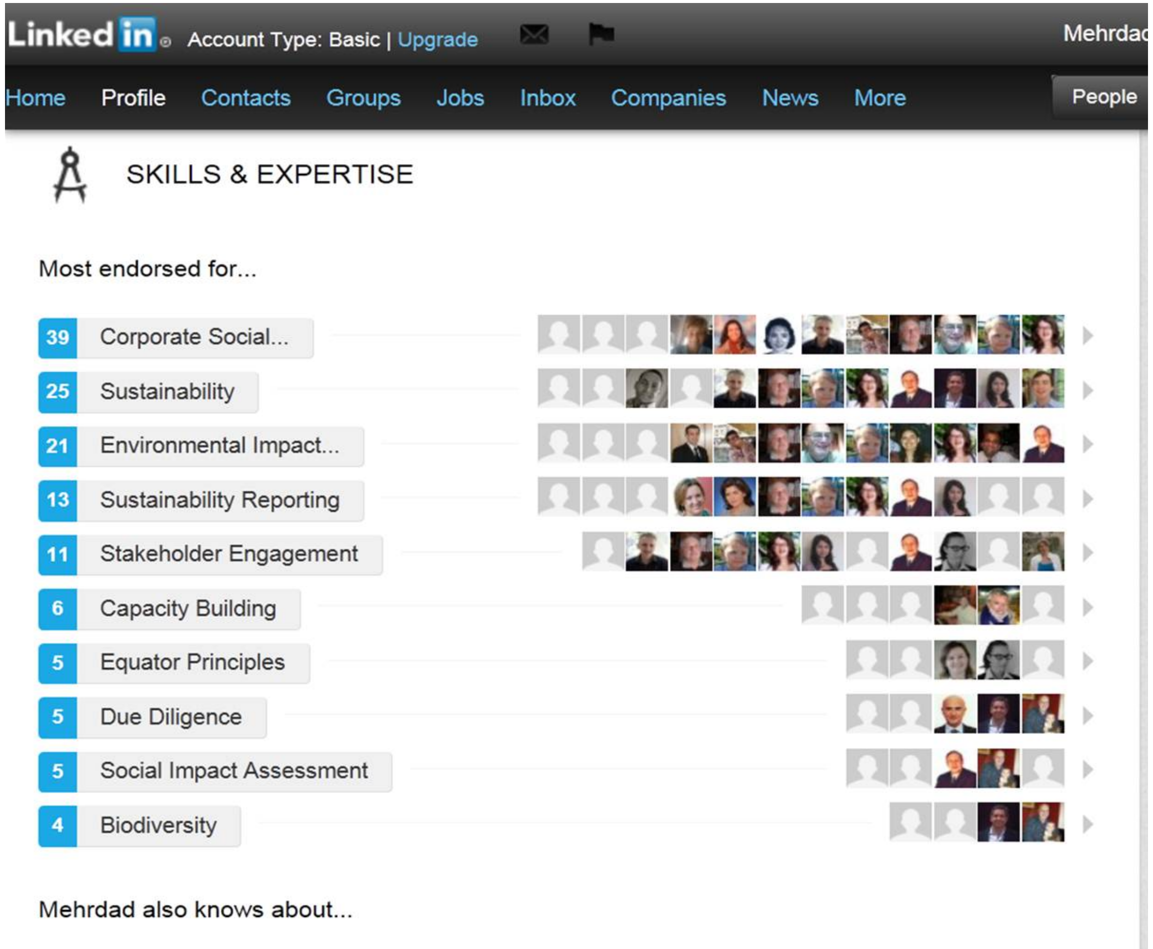


sd123idjf0

This is my public key and ID card

Public-Key Predistribution

- Endorsement



Linked in Account Type: Basic | Upgrade Mehrdac

Home Profile Contacts Groups Jobs Inbox Companies News More People

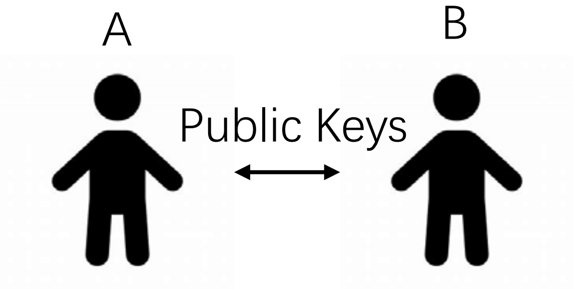
SKILLS & EXPERTISE

Most endorsed for...

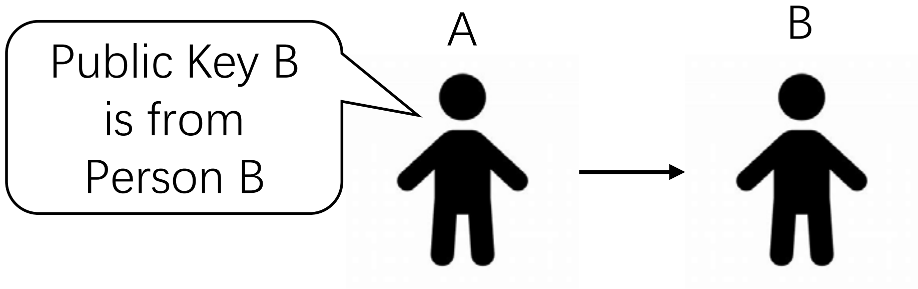
39	Corporate Social...
25	Sustainability
21	Environmental Impact...
13	Sustainability Reporting
11	Stakeholder Engagement
6	Capacity Building
5	Equator Principles
5	Due Diligence
5	Social Impact Assessment
4	Biodiversity

Mehrdad also knows about...

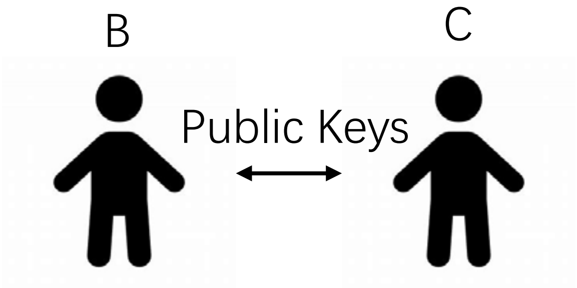
Public-Key Predistribution



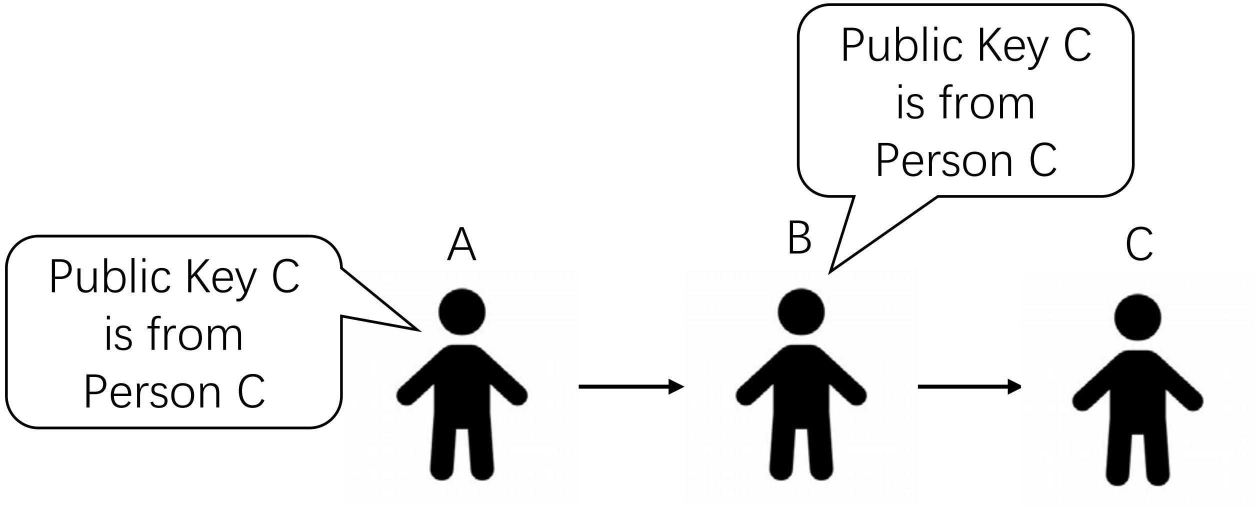
Step 1. Verify Each Other Offline;
Exchange Public Keys



Step 2. Certifies Public Keys



Step 3. Verify Each Other Offline;
Exchange Public Keys



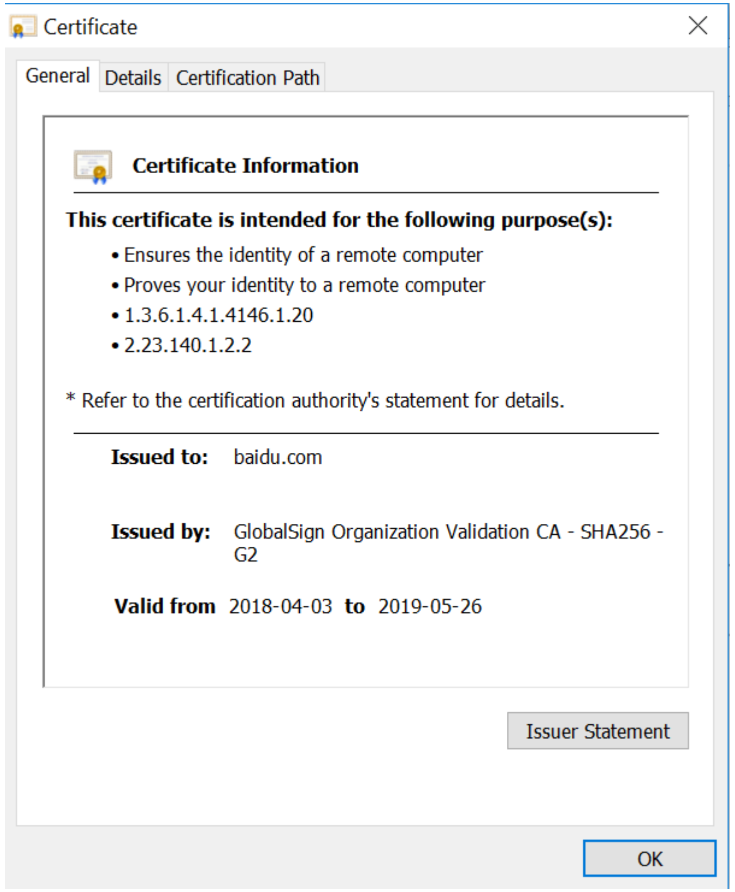
Step 4. Certifies Public Keys from Others

Public-Key Predistribution

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

Public-Key Predistribution

- Certificate



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 1.3.6.1.4.1.4146.1.20
- 2.23.140.1.2.2

* Refer to the certification authority's statement for details.

Issued to: baidu.com

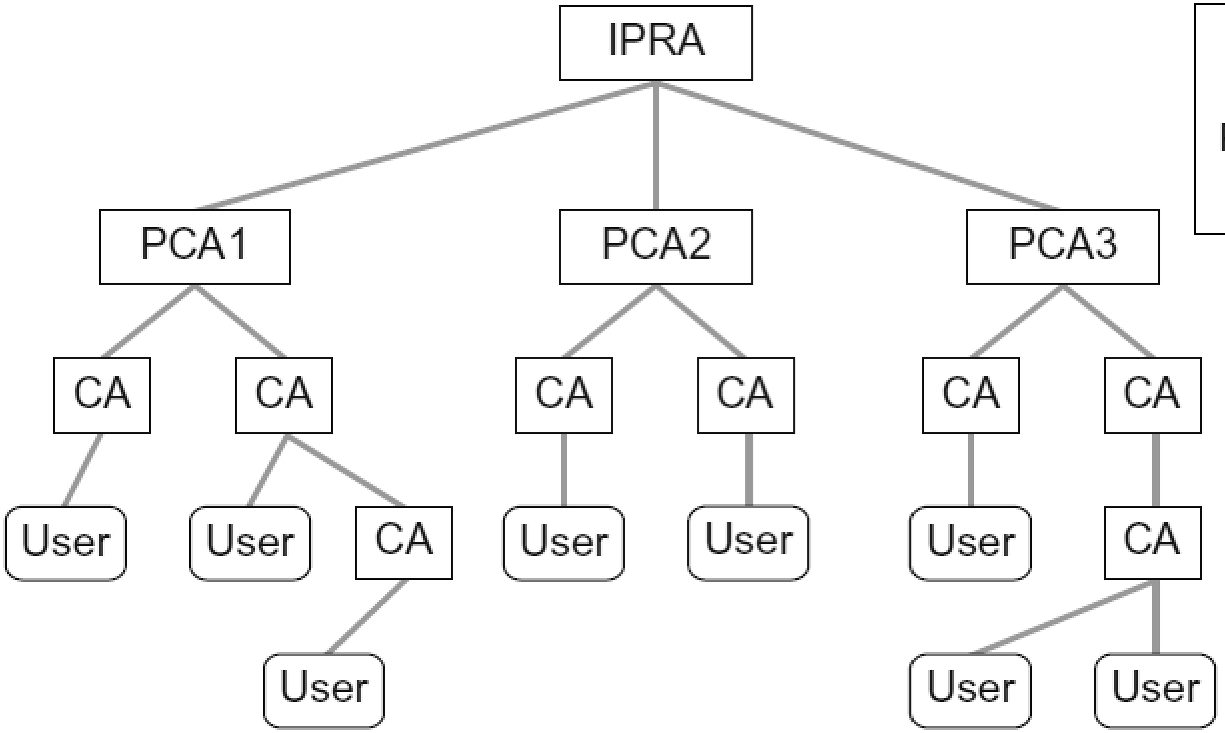
Issued by: GlobalSign Organization Validation CA - SHA256 - G2

Valid from 2018-04-03 **to** 2019-05-26

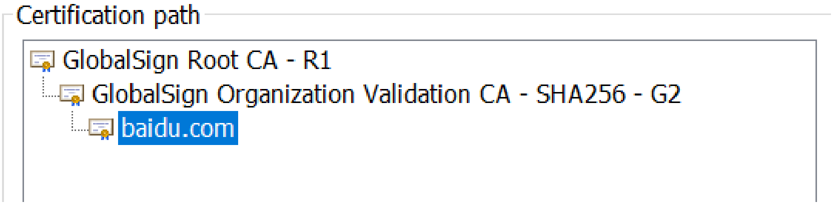
- The identity of the entity being certified
- The public key of the entity being certified
- The identity of the signer
- The digital signature of the signer
- A digital signature algorithm identifier (which cryptographic hash and which cipher)

Public-Key Predistribution

- Certificate Authority (CA)



IPRA = Internet Policy Registration Authority (root)
PCA*n* = Policy certification authority
CA = Certification authority



Certification path

GlobalSign Root CA - R1
GlobalSign Organization Validation CA - SHA256 - G2
baidu.com

Demo

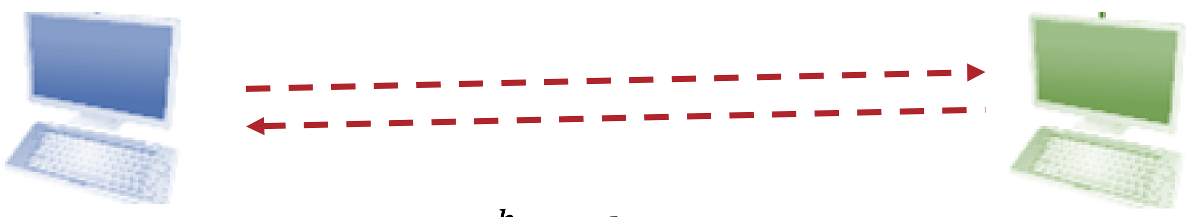
- Certificate Authority (CA)
  - certmgr.msc
  - https://www.sinorailca.com/

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 mod p is the shared key



$g^a \bmod p$

$$(g^a \bmod p)^b \bmod p = g^{ab} \bmod p$$

$$\left(g^b \bmod p\right)^a \bmod p = g^{ab} \bmod p$$

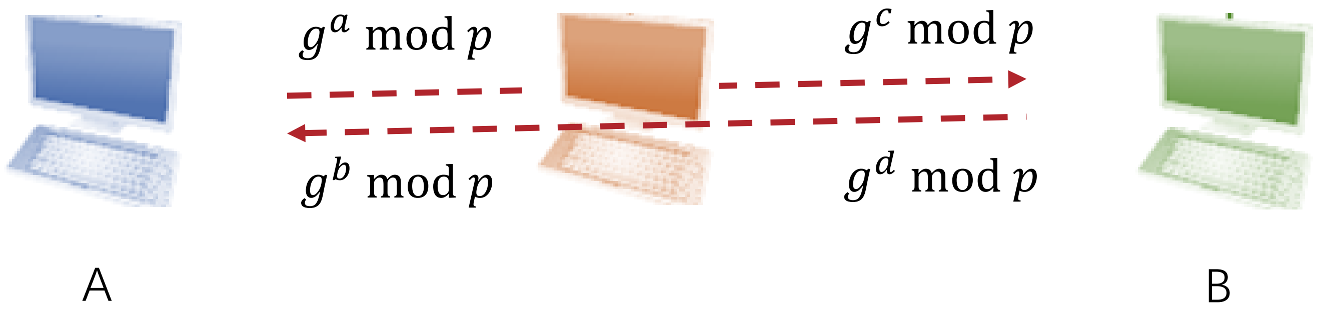
$g^b \bmod p$

A

B

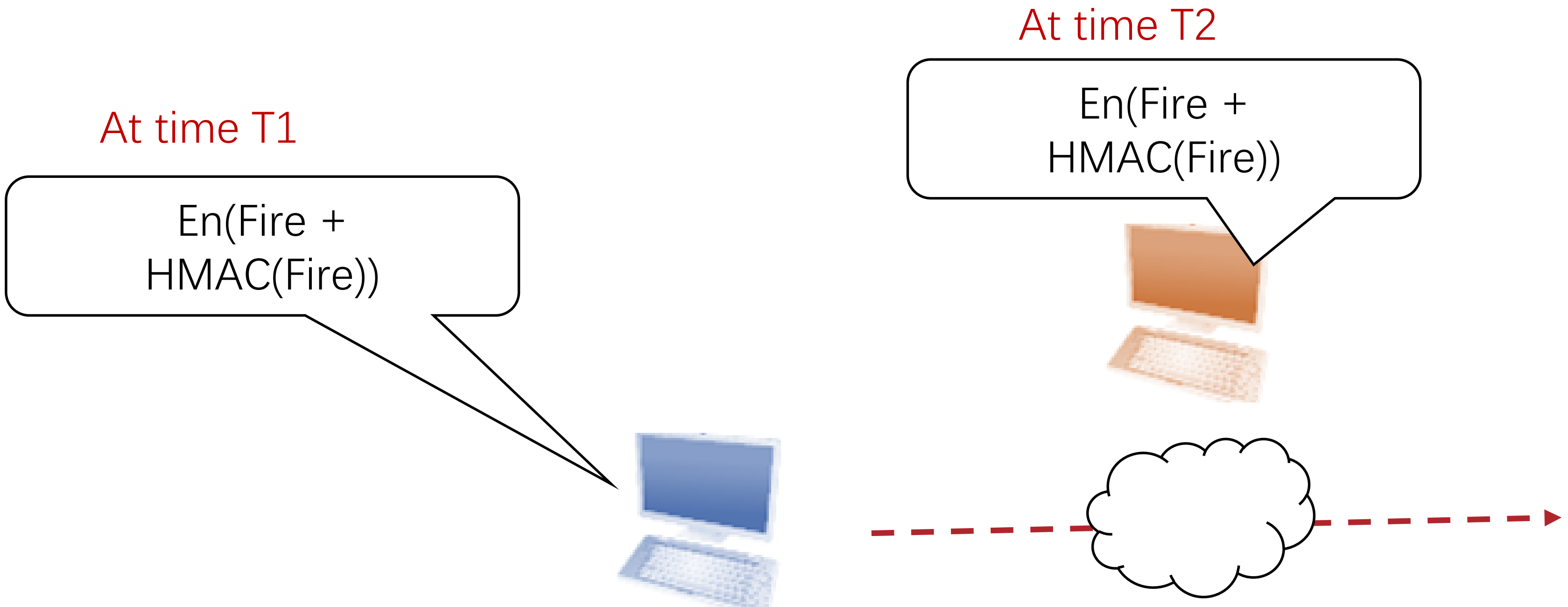
Diffie-Hellman Key Exchange

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



What is Network Security

- Originality
  - To prevent an adversary from replaying the message contents.
- Timeliness
  - To identify delayed messages

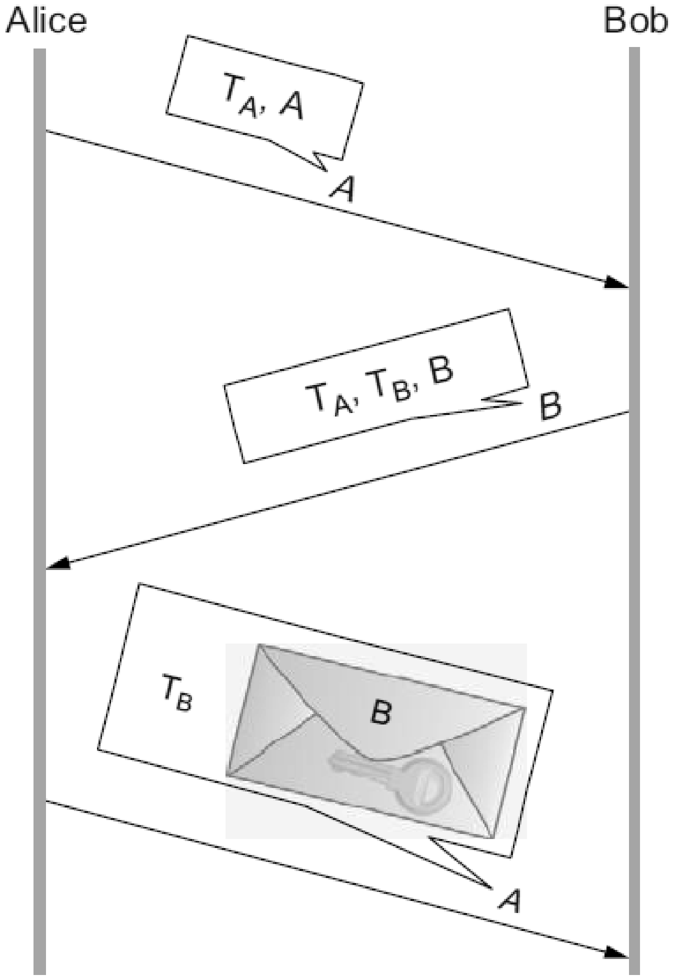


Authentication

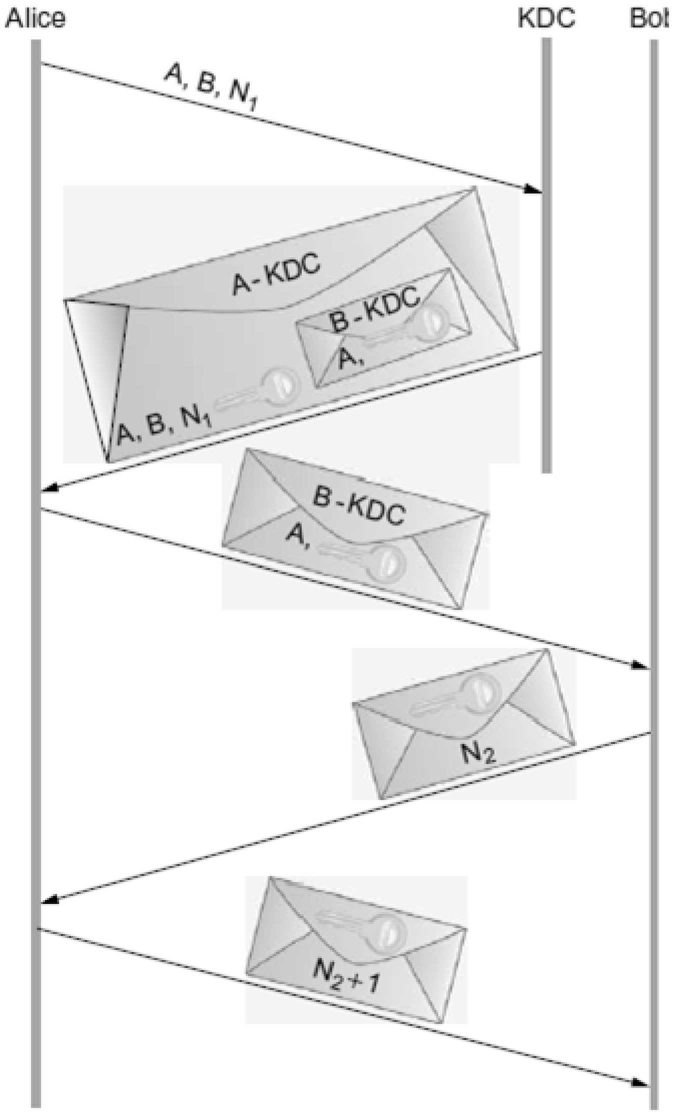
- Messages must be authenticated
    - Timely
        - Timestamp
    - From its original source
        - Authenticate the sender continuously
            - High overhead in using key predistribution methods along
            - Generating new session keys

Public-Key Authentication Protocols

- A sends its certificate and T_A to B
- B verifies A’s certificate
- B sends its certificate, T_A and T_B to A
- A verifies T_A and B’s certificate
- A sends T_B and uses B’s public key to encrypt new session key to B
- B verifies T_B and decrypt the session key

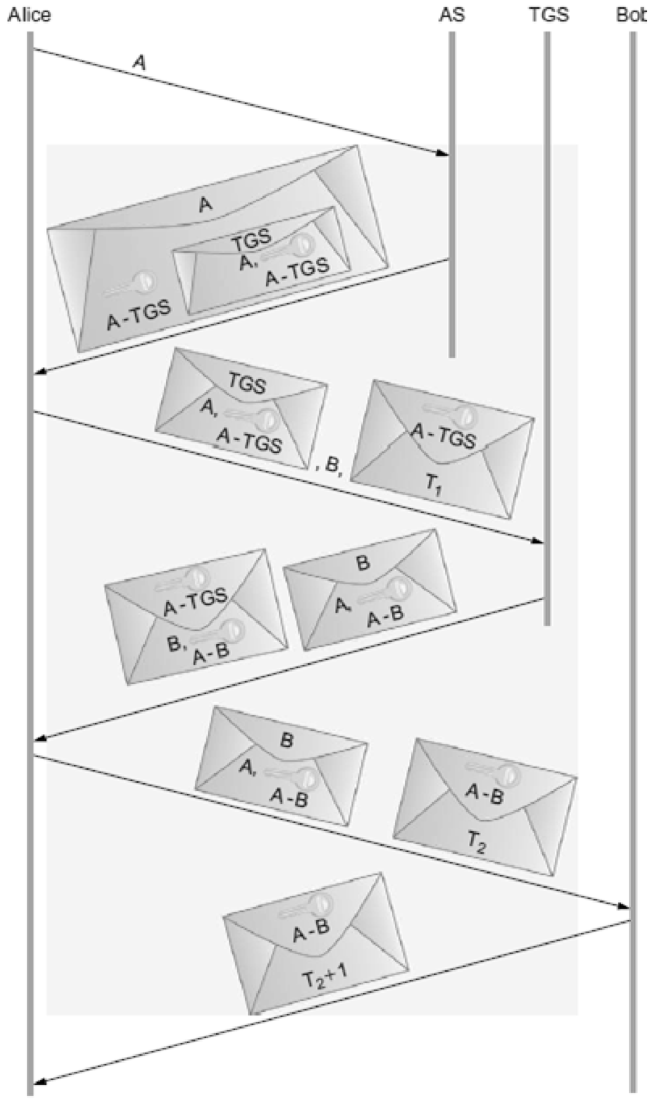


Symmetric-Key Authentication Protocols



Symmetric-Key Authentication Protocols

- Kerberos



Reference

- Textbook 8.1, 8.2, 8.3