1 Introduction

ch1 in textbook

Yanwei Yu

E-mail: ywyu@ustc.edu.cn

Outline

- Introduction to Information security
- X.800 standard
- security attacks, services, mechanisms
- Implementation of Security Services
- models for network (access) security

Background

- Information Security requirements have changed in recent times
- traditionally provided by physical and administrative mechanisms
- computer use requires automated tools to protect files and other stored information
- use of networks and communications links requires measures to protect data during transmission

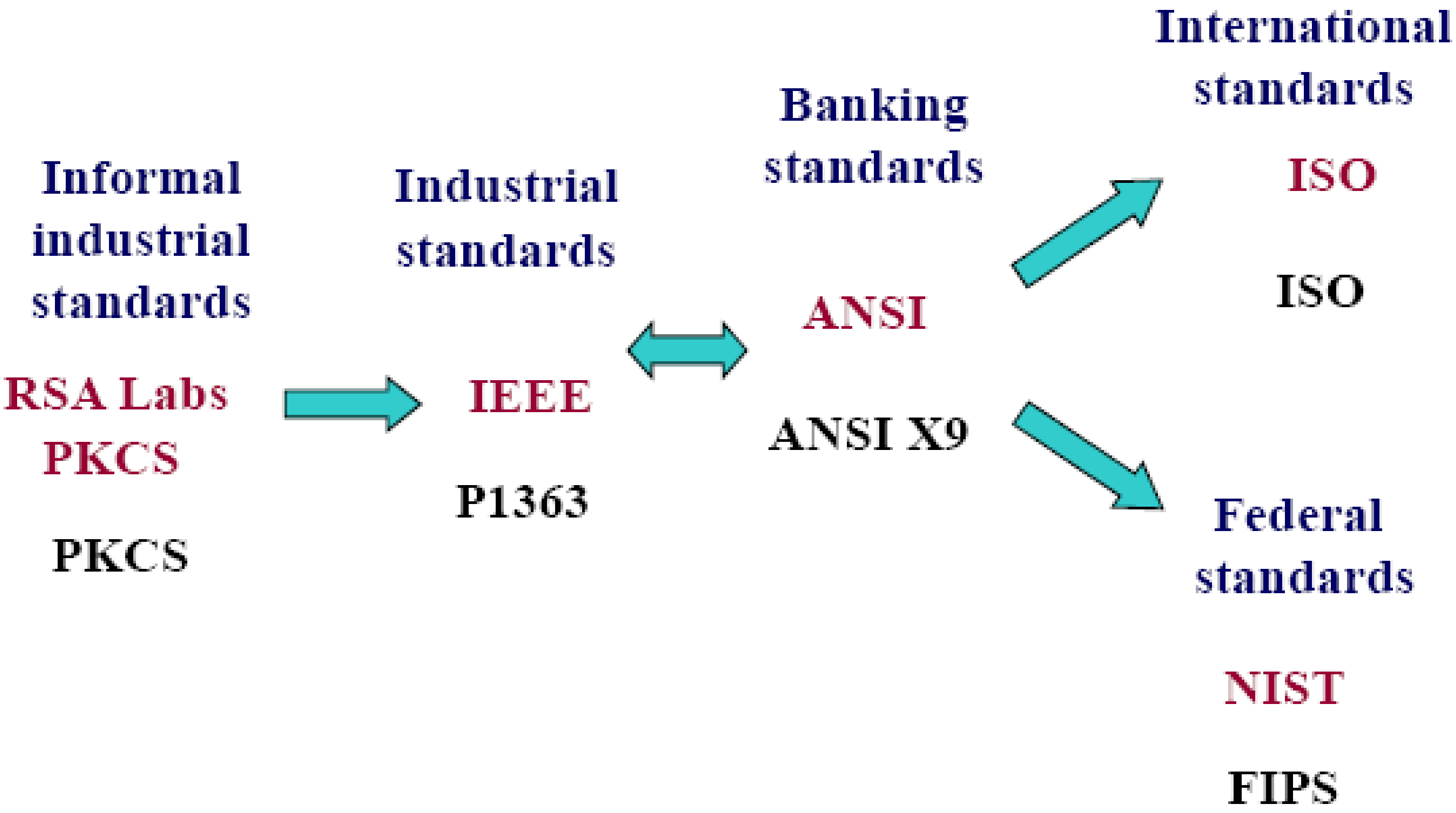
Definitions

- Computer Security
  - to protect data and to prevent hackers
- Network Security
  - to protect data during their transmission
- Internet Security
  - to protect data during their transmission over a collection of interconnected networks

Aim of Course

- our focus is on **Internet Security**
- **Internet Security** consists of methods/techniques to **prevent**, **detect**, and **correct** security attacks that involve the **transmission & storage of information**

American and international standards



Informal industrial standards

RSA Labs PKCS

PKCS

Industrial standards

IEEE

P1363

Banking standards

ANSI

ANSI X9

International standards

ISO

ISO

Federal standards

NIST

FIPS

- **PKCS – Public Key Cryptography Standards**

- **IEEE - Institute of Electrical and Electronics Engineers**

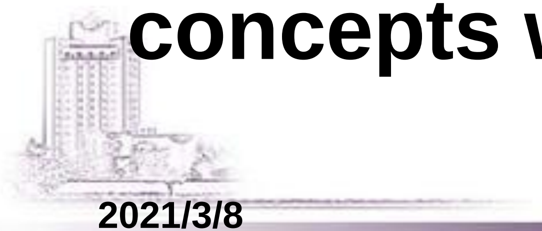
- **ANSI - American National Standards Institute**

- **ISO – International Organization for Standardization**

- **NIST - National Institute of Standards and Technology**
- **FIPS - Federal Information Processing Standards**

OSI Security Architecture

- ITU-T(International Telecommunication Union Telecommunication Standardization Sector) X.800 “Security Architecture for OSI(Open Systems Interconnection)”
- defines a systematic way of defining and providing security requirements
- provides a useful, abstract overview of concepts we will study



Aspects of Security

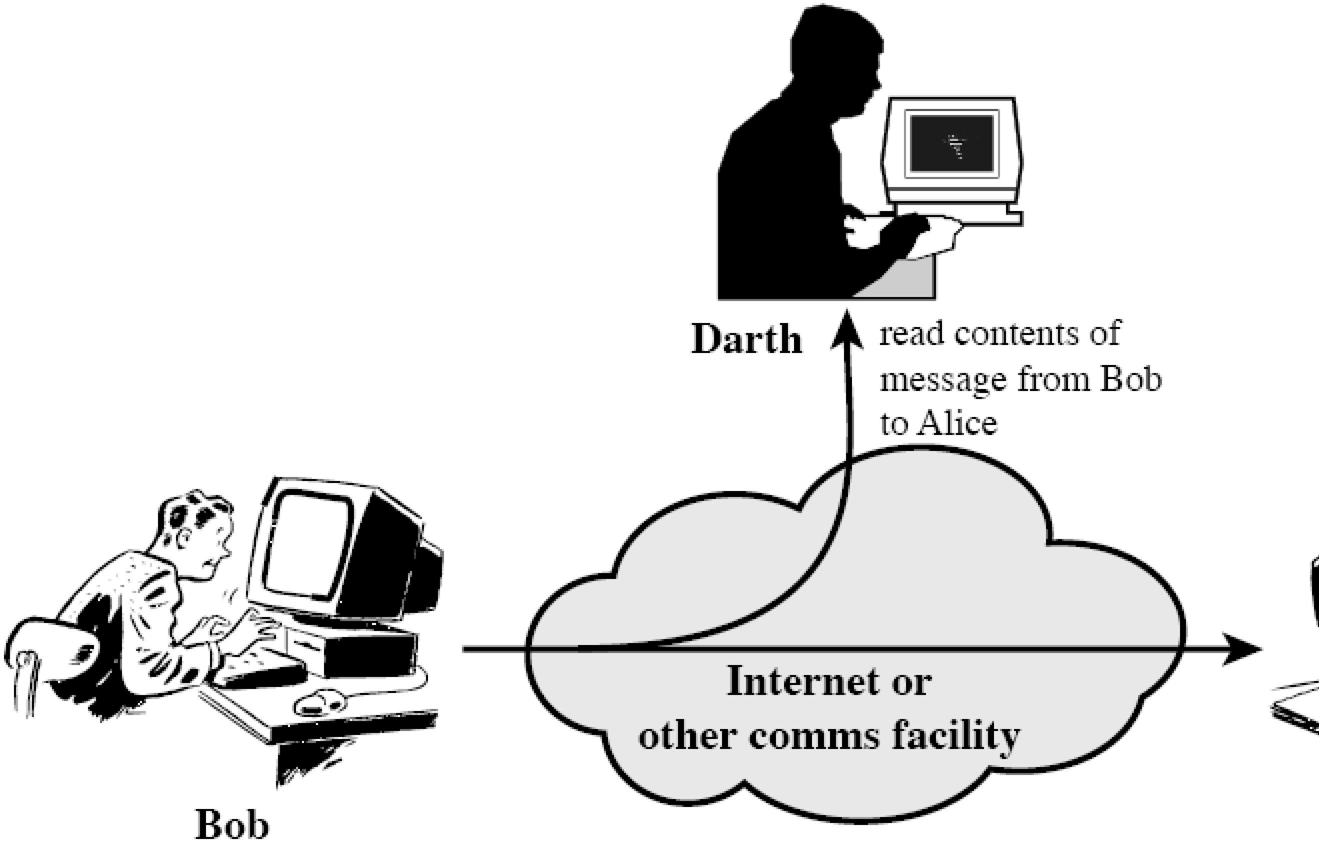
- **consider three aspects of information security:**
  - – security attack
  - – security mechanism/method
  - – security service

Security Attack/threat

- any action that threaten the security of information owned by an organization

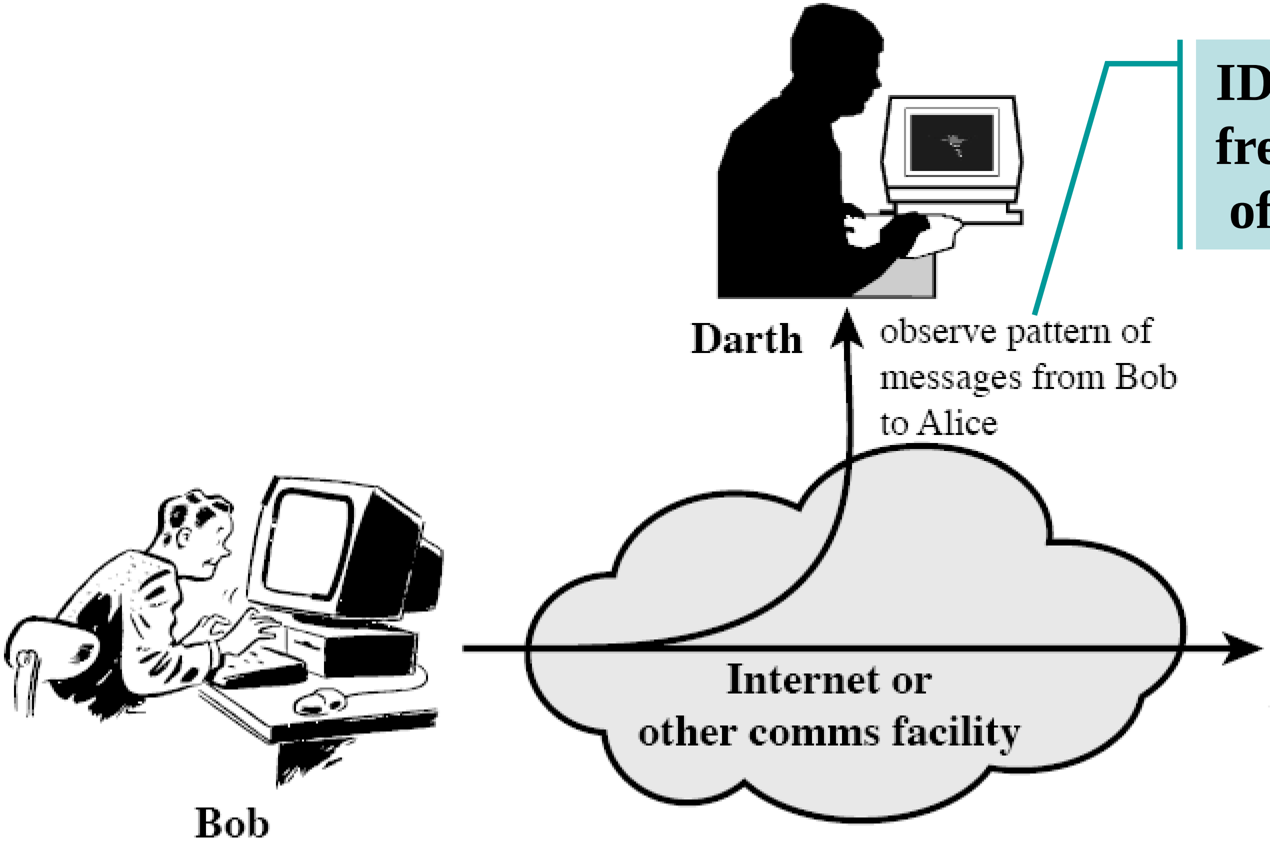
- can focus of generic types of attacks
  - – passive: Prevent
  - – active: Detect, Recover

Passive Attacks


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

(a) Release of message contents

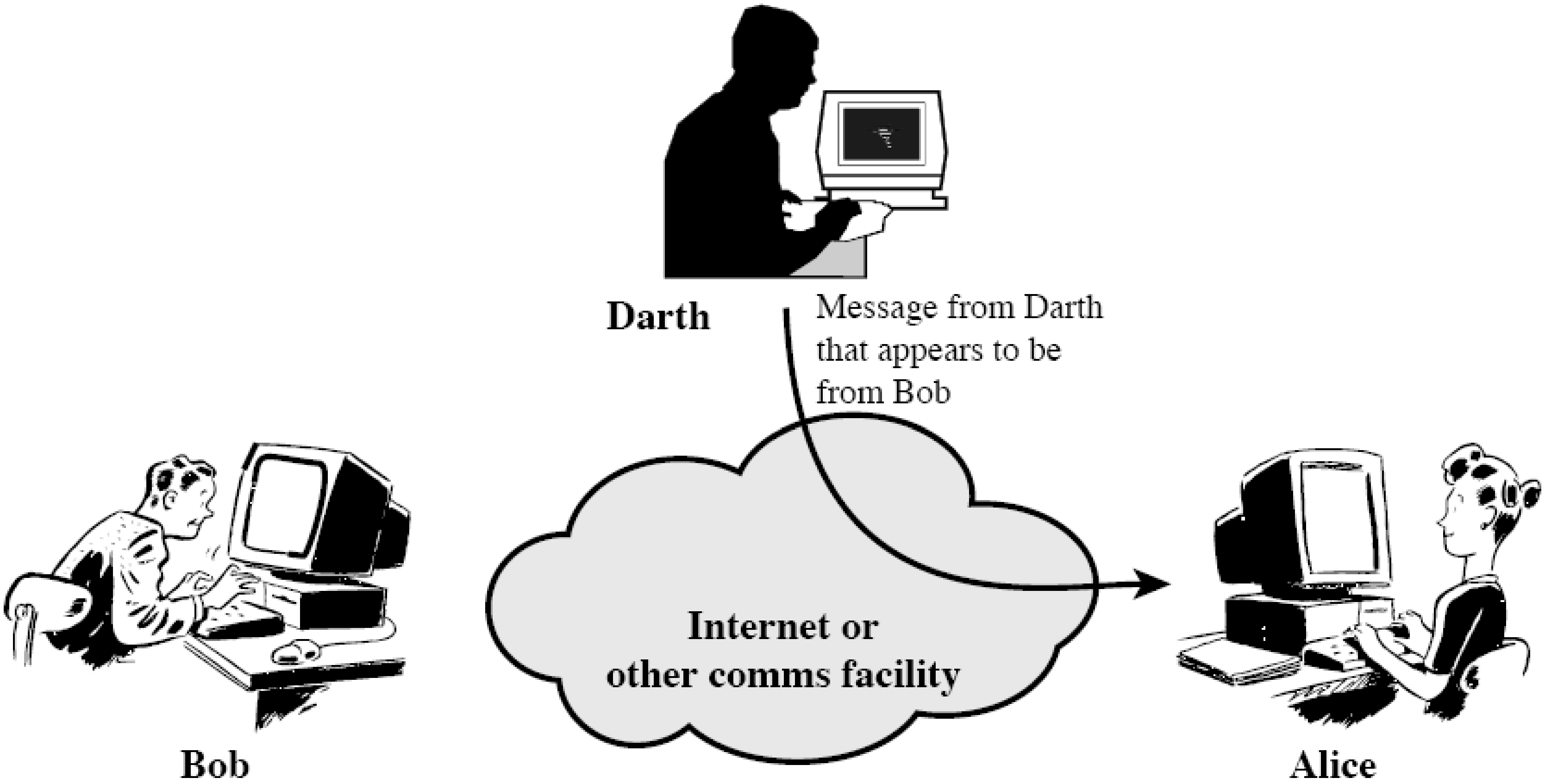
Passive Attacks


Darth
observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

(b) Traffic analysis

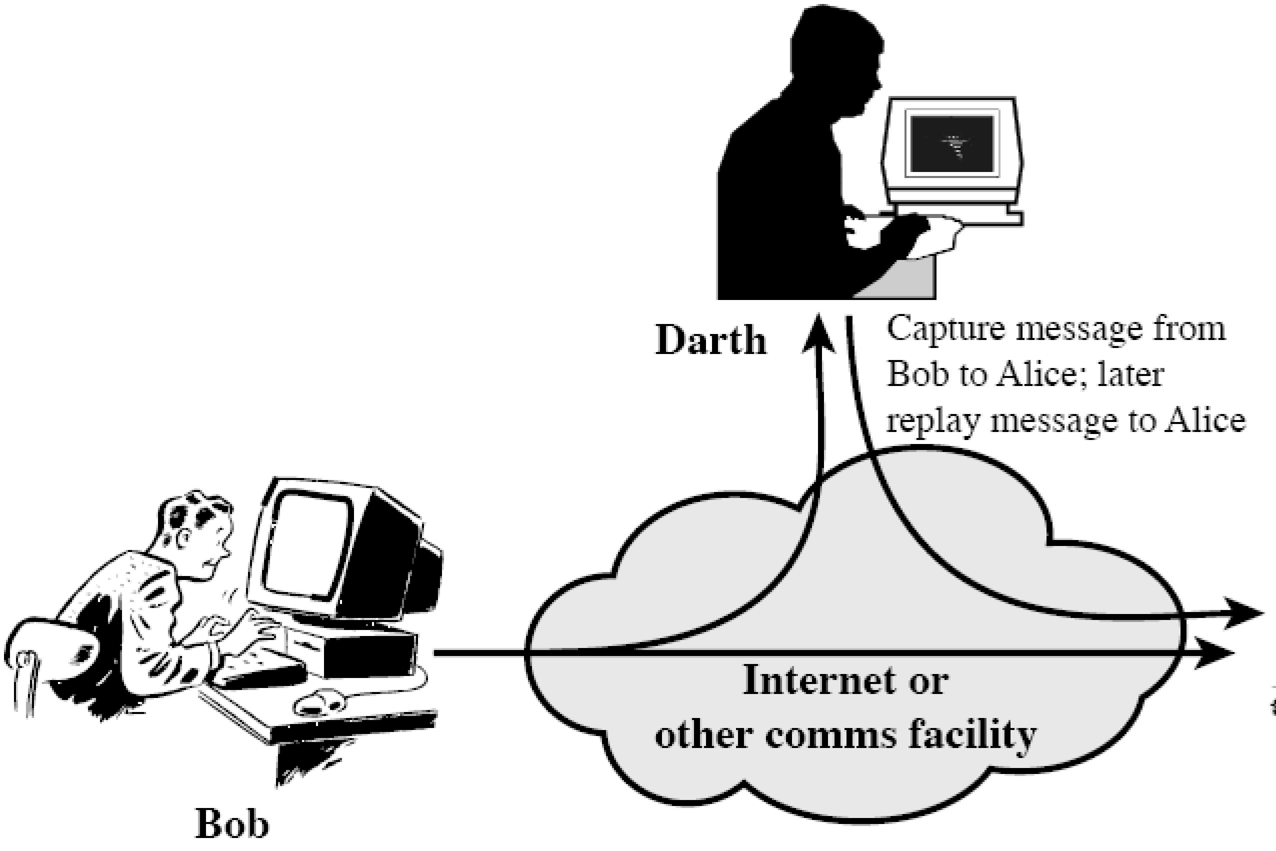
ID and position of Hosts, frequency and length of messages

Active Attacks


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

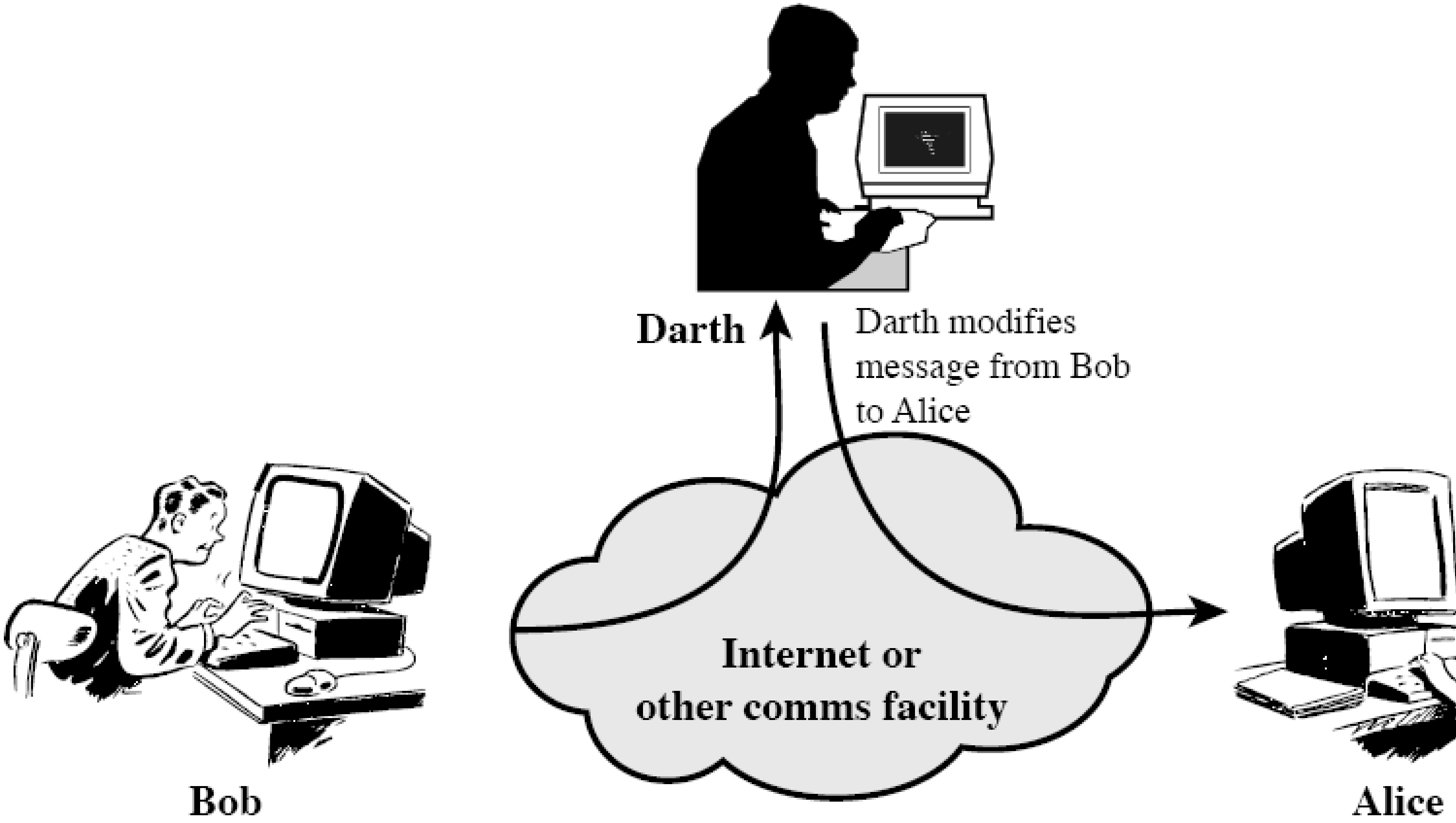
(a) Masquerade (伪装)

Active Attacks



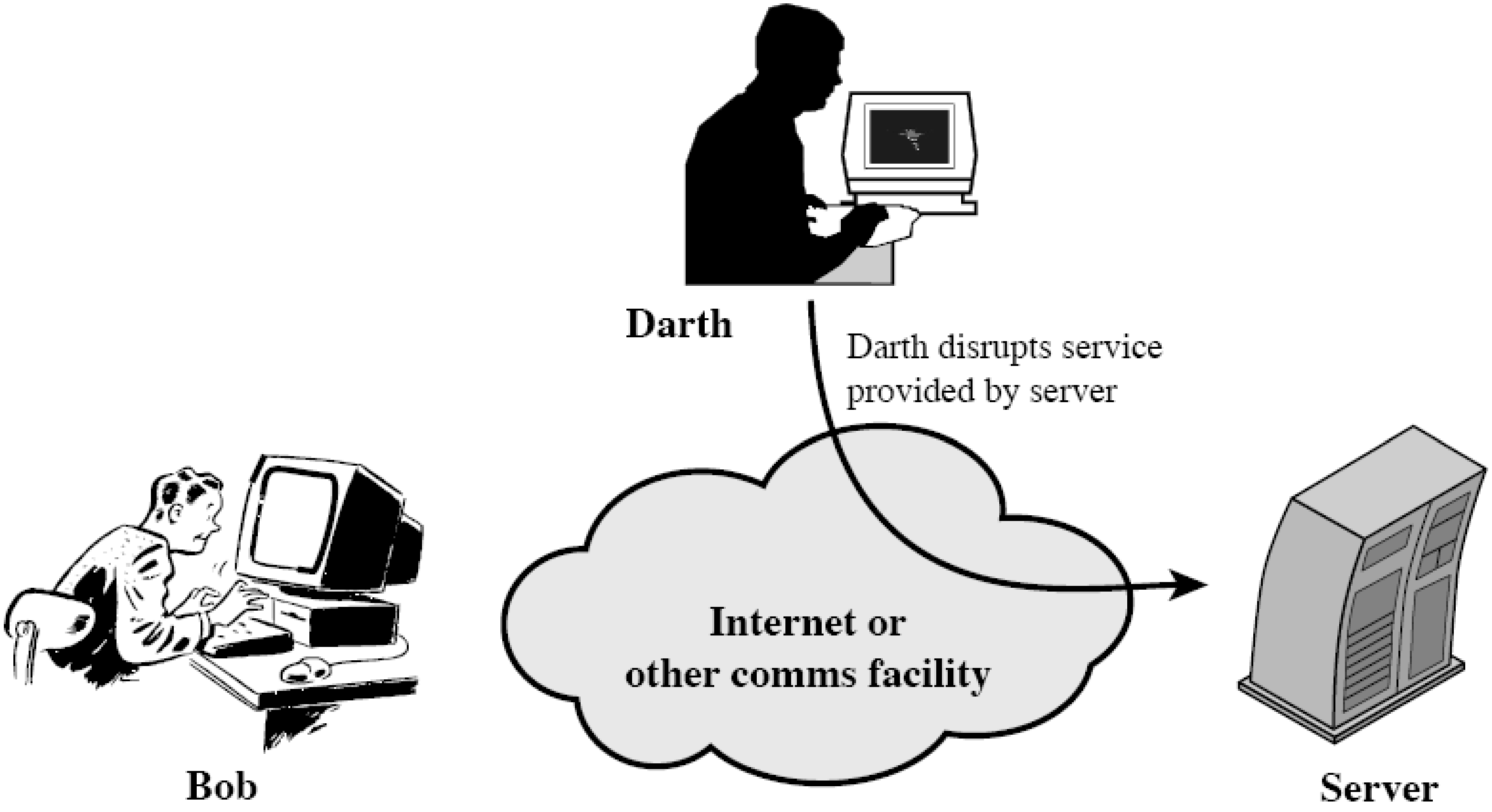
(b) Replay (重放)

Active Attacks


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

(c) Modification of messages

Active Attacks



(d) Denial of service(拒绝服务)

Security Service

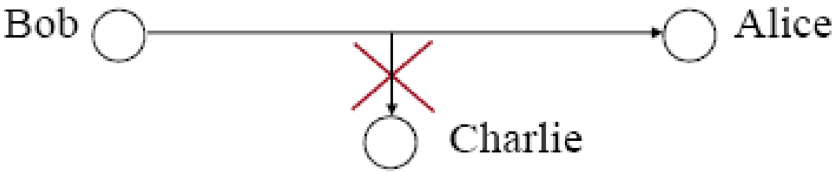
- Used to resolve security attacks
- using one or more security mechanisms
- Provide the similar functions normally associated with physical documents
  - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction, etc.

Security Services

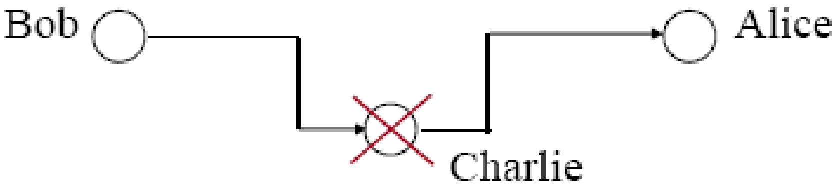
- **X.800:**
  - "a service provided by a protocol layer of communicating open systems, which **ensures** adequate **security of the systems** or **of data transfers**"
- **RFC 2828:**
  - "a processing or communication service provided by a system to give a specific kind of **protection to system resources**"
  - security services implement security policies and are **implemented by security mechanisms.**

Security Services (X.800)

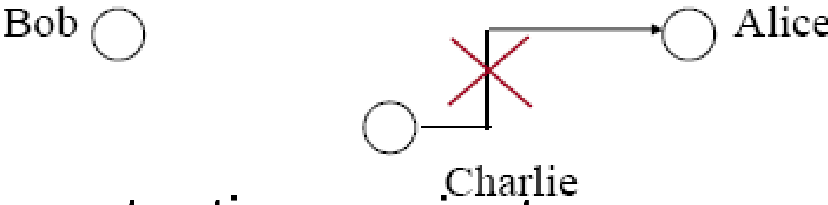
- **Data Confidentiality(机密性)**



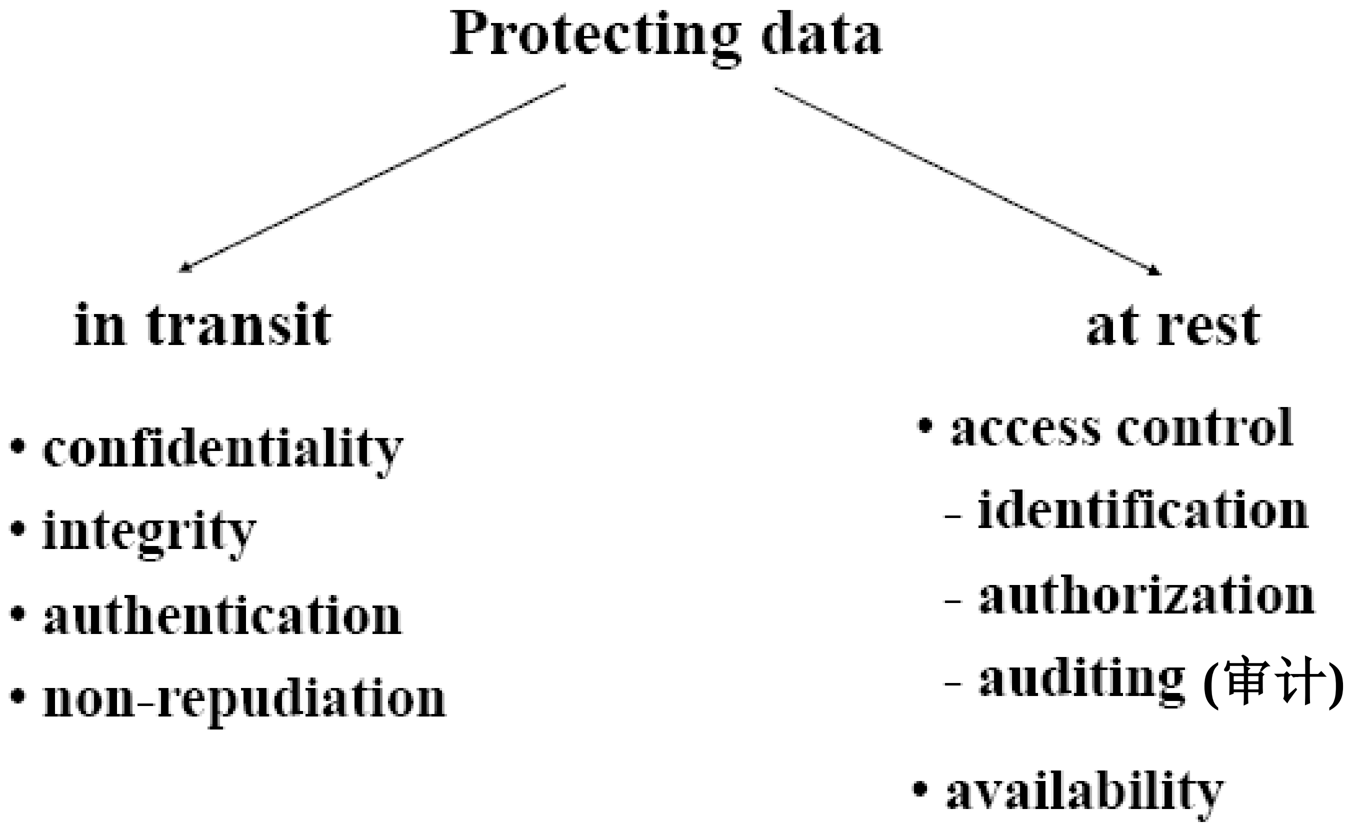
- **Data Integrity**



- **Message Authentication(认证)** & **User Authentication**



- **Non-Repudiation(不可抵赖性)** - protection against denial by one of the parties in a communication
- **Access Control** - prevention of the unauthorized use of a resource
- **Availability**



Protecting data

in transit

- confidentiality
- integrity
- authentication
- non-repudiation

at rest

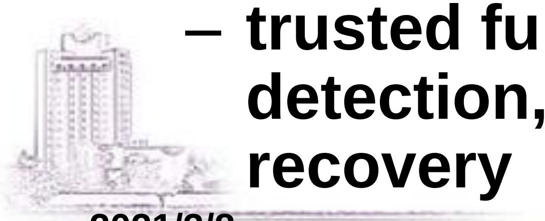
- access control
  - identification
  - authorization
  - auditing (审计)
- availability

Security Mechanism - Our Focus

- designed to detect, prevent, or recover from a security attack
- no single mechanism_that will support all services required
- Consist of cryptographic techniques

Security Mechanisms (X.800)

- specific security mechanisms:
  - realized in some protocol layer
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding(填充), routing(路由) control, notarization(公证)
- pervasive(普遍的) security mechanisms:
  - not limited in any OSI security service or protocol layer
  - trusted functionality(功能), security labels, event detection, security audit trails(跟踪), security recovery



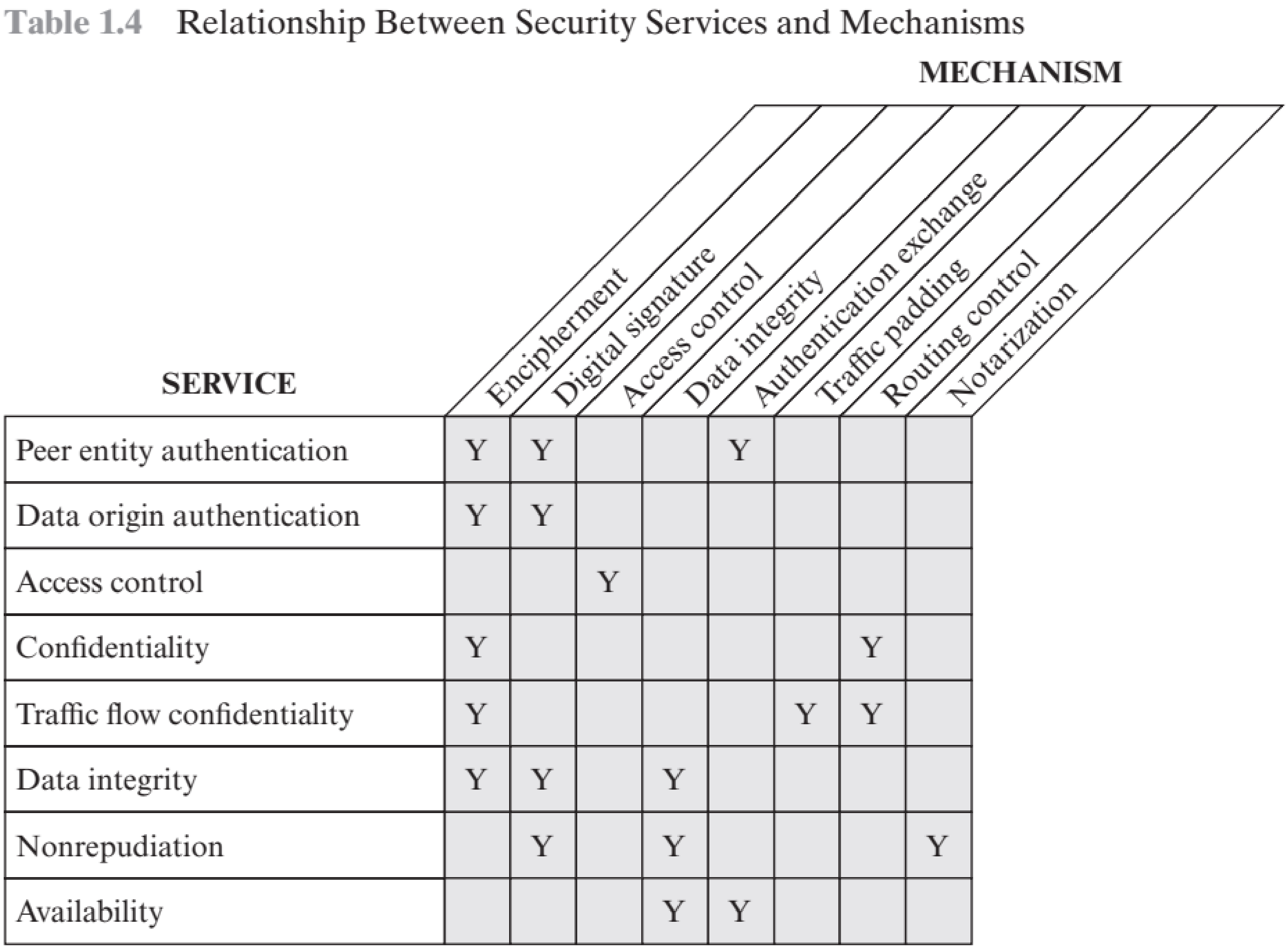


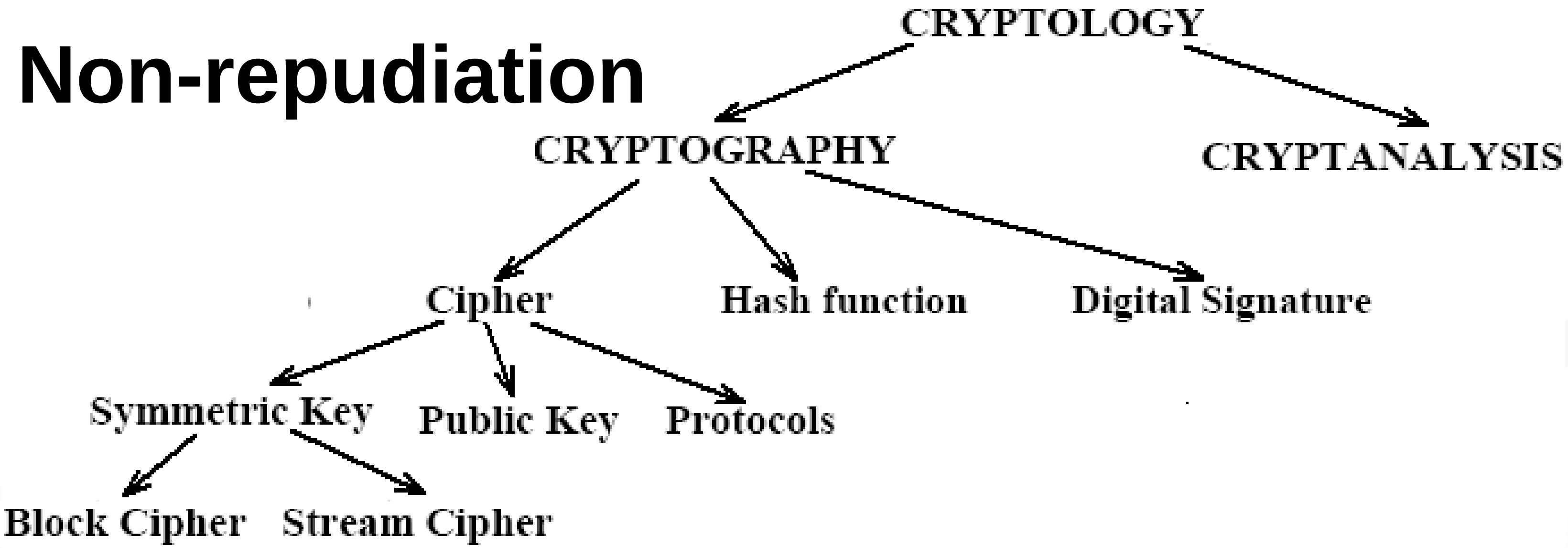
Table 1.4 Relationship Between Security Services and Mechanisms

SERVICE \ MECHANISM	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

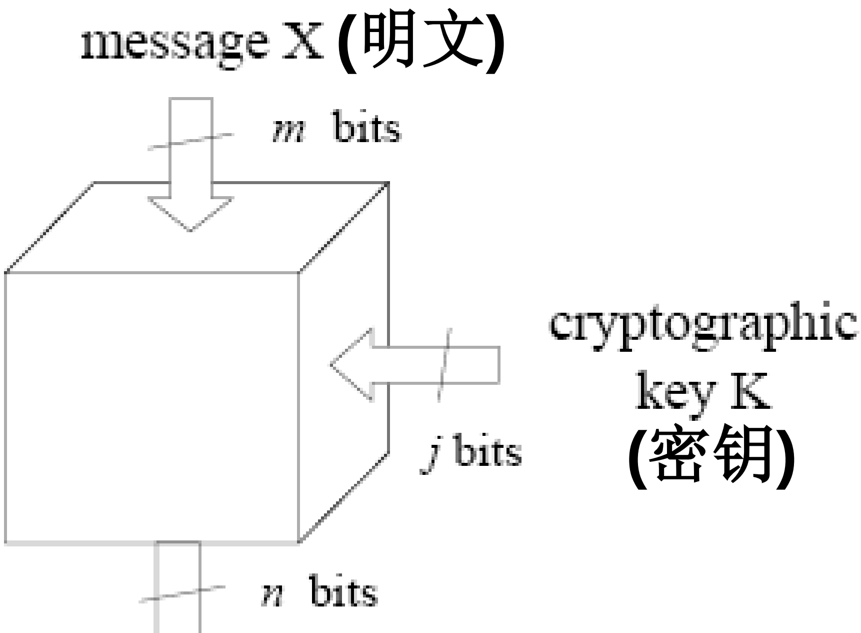
no single mechanism that will support all services required

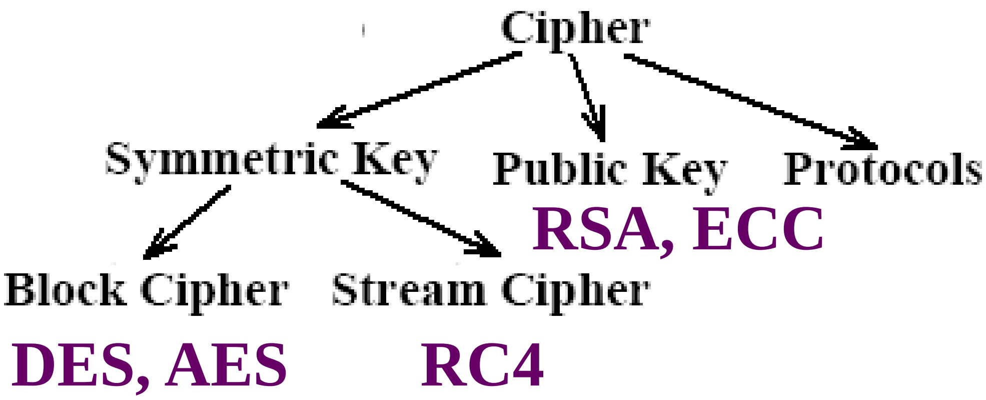
Implementation of Security Services

- Data Confidentiality
- Data Integrity
- Authentication
- Non-repudiation



Confidentiality: Cipher





Key Management:

- Secure distribution and share of Secret key
  - Confidentiality
- Secure distribution of public key
  - Authentication

Data Integrity: Hash Function

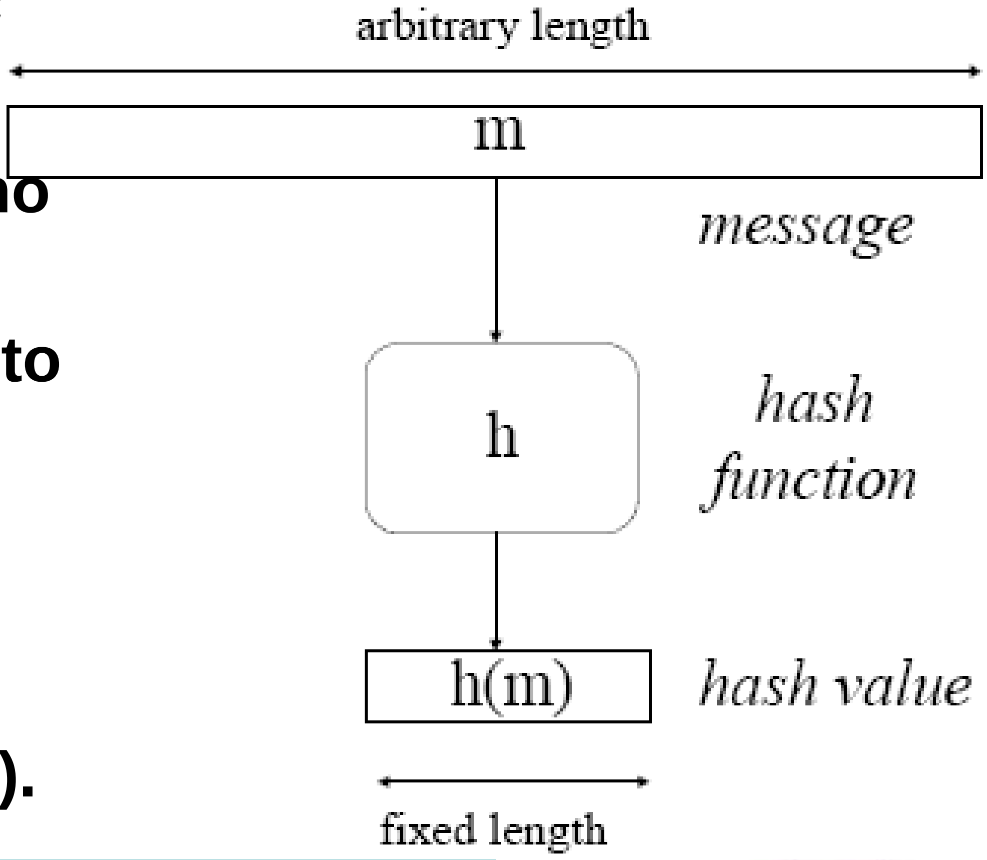
- Hash function Basic Requirements

  1) Public description, no key.

  2) *h(m)* can be applied to any size *m.*

  3) *h(m)* produces fixed length output.

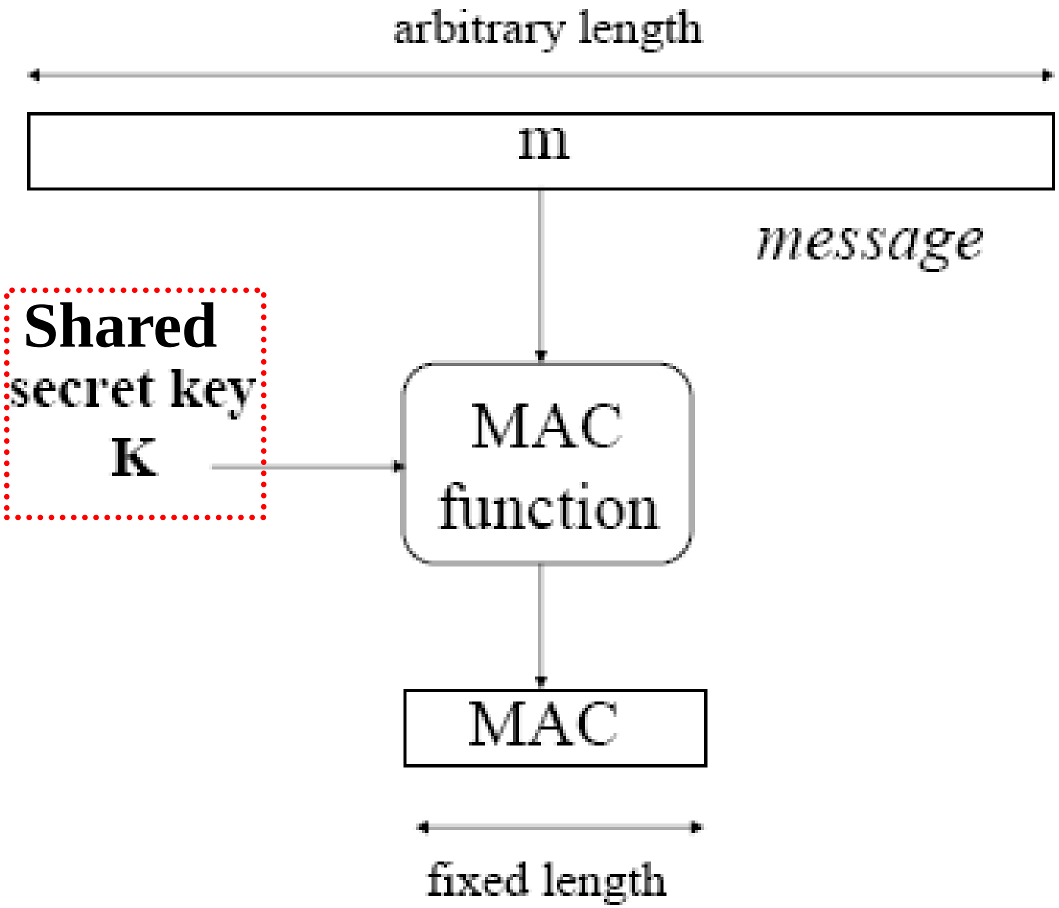
  4) *h(m)* is easy to compute (hw and sw).



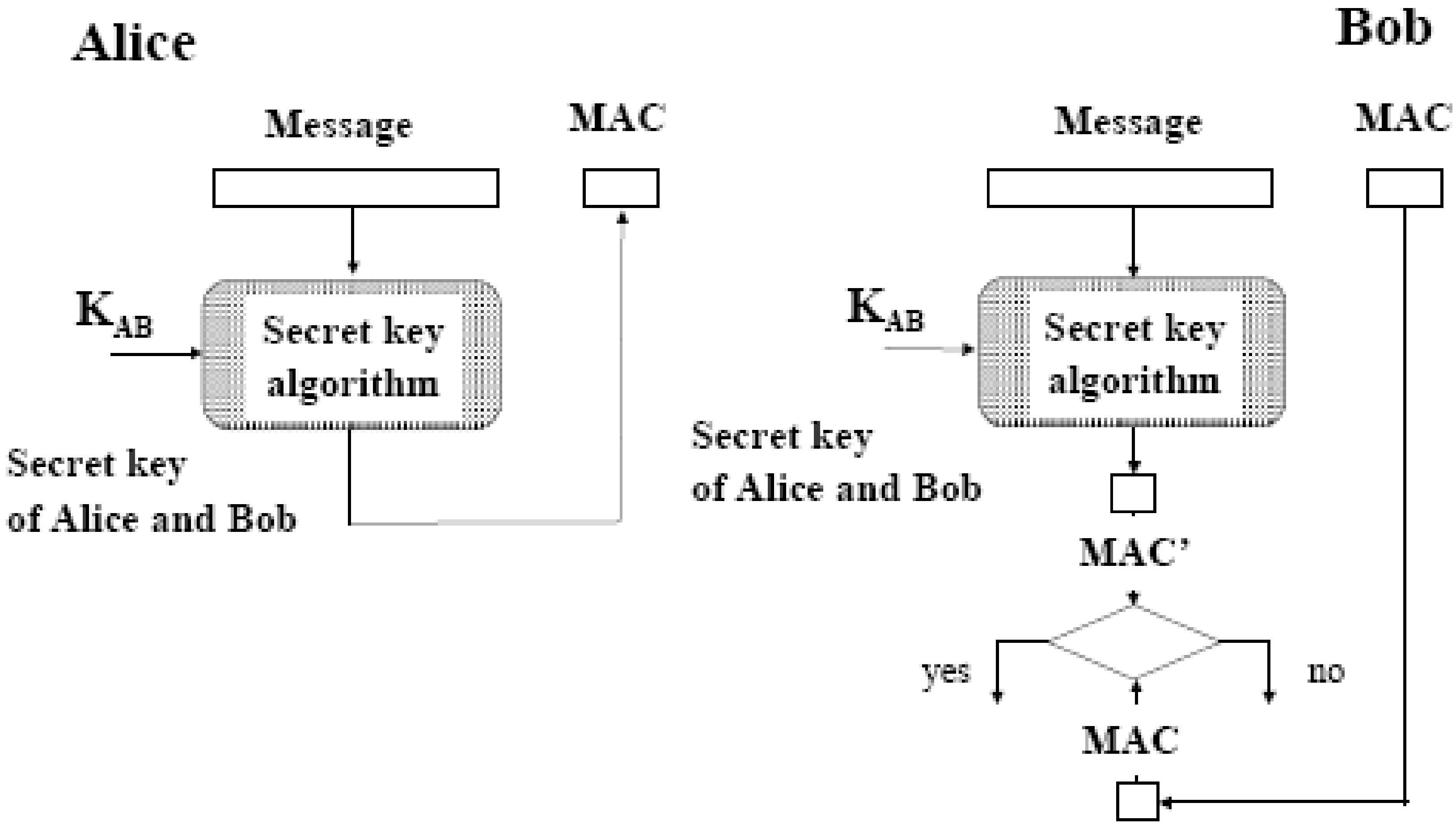
hardware and software

Message Authentication: MAC - Message Authentication Codes

- MAC=C(k,m)
  - HMAC: keyed hash functions
  - CMAC: Cipher Block Chaining MAC



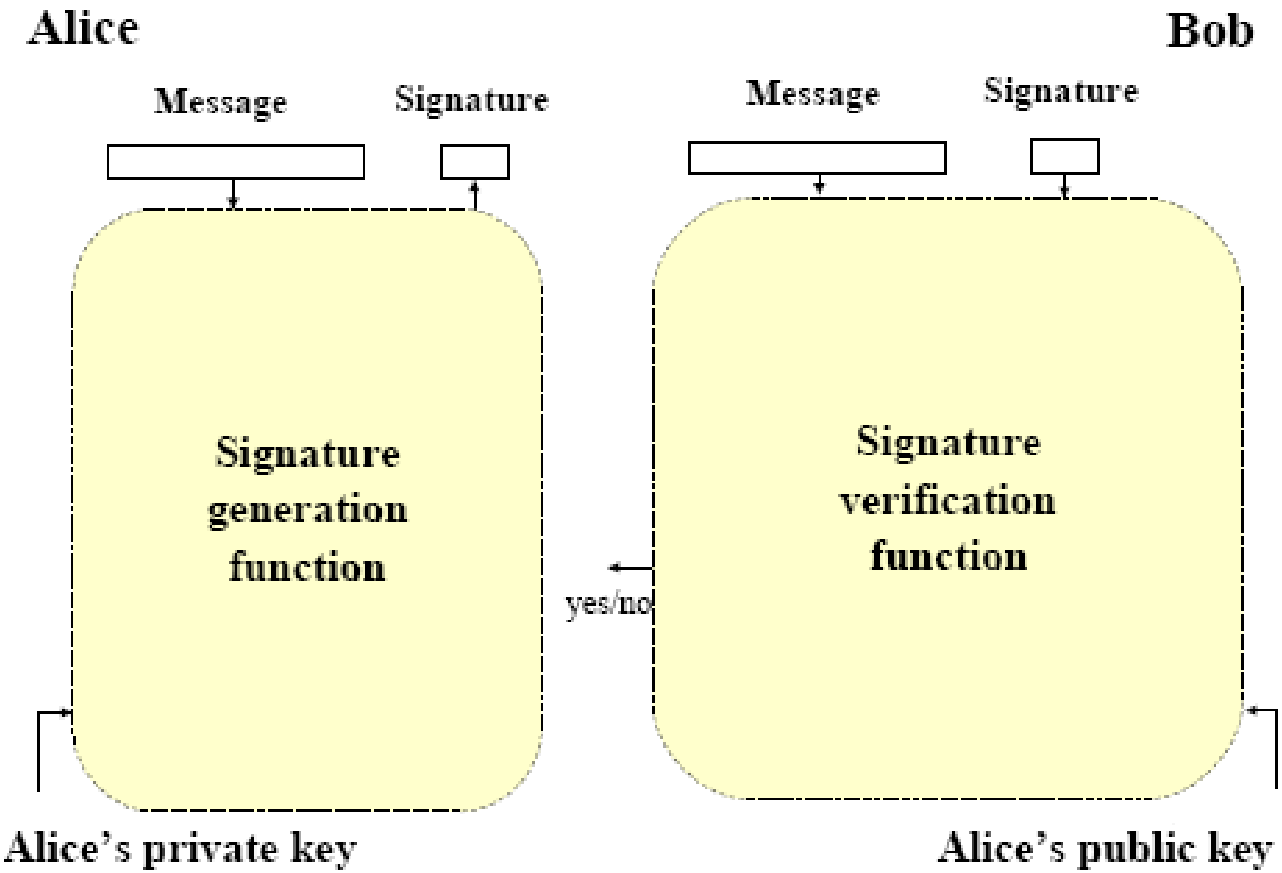
Example


Alice
Bob
Message
MAC
K_{AB}
Secret key algorithm
Secret key of Alice and Bob
Message
MAC
K_{AB}
Secret key algorithm
Secret key of Alice and Bob
MAC'
yes
no
MAC

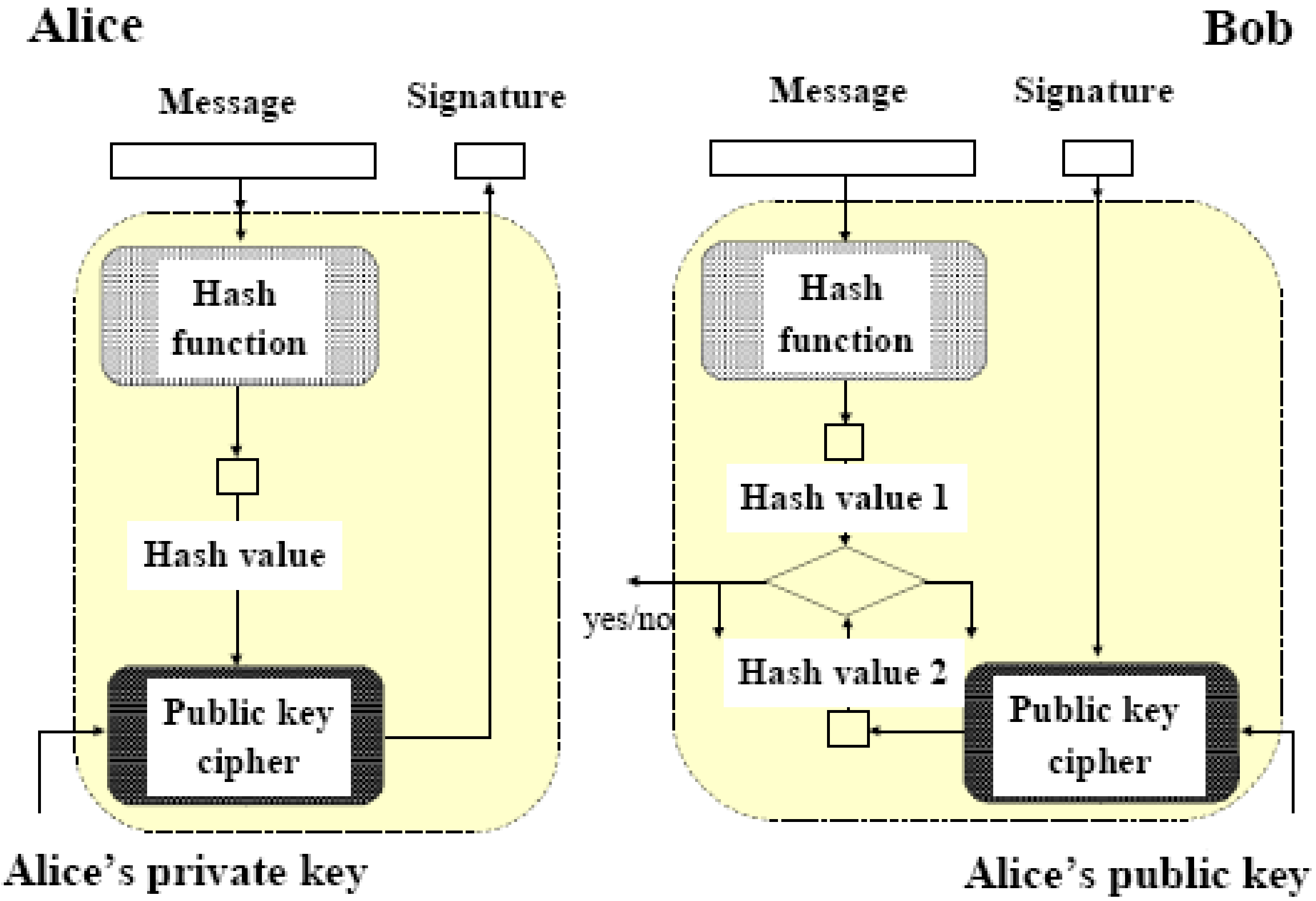
Identification (User Authentication)

- On the basis of
  - What you know: password, PINS
  - What you have: magnetic card, smart card
  - What you are: fingerprints, handprints, voiceprints, keystroke timing, retinal scanners

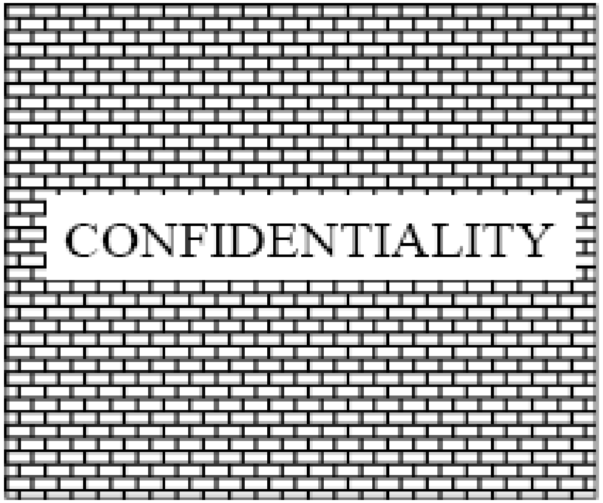
Non-repudiation

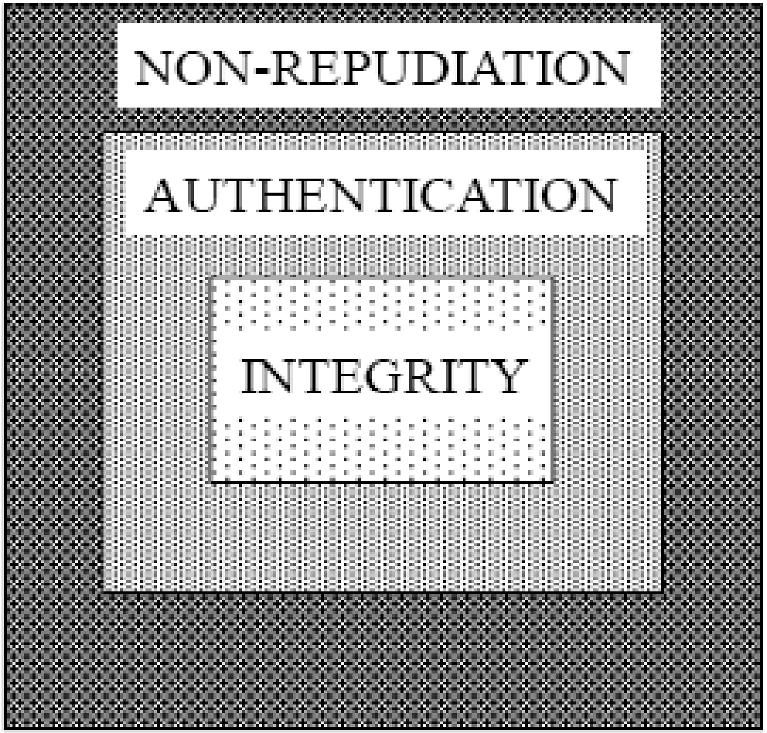


Non-repudiation

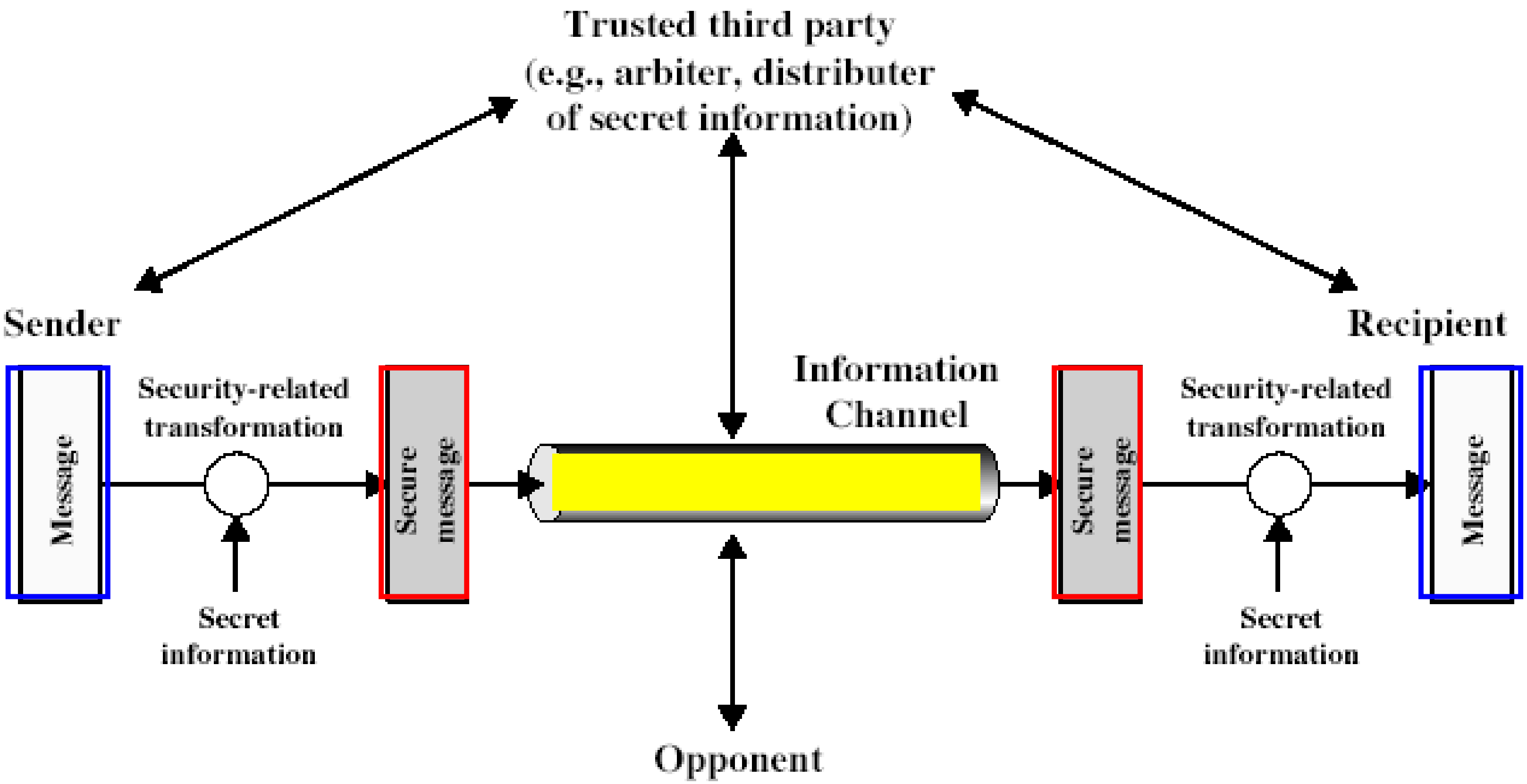


Relations among security services





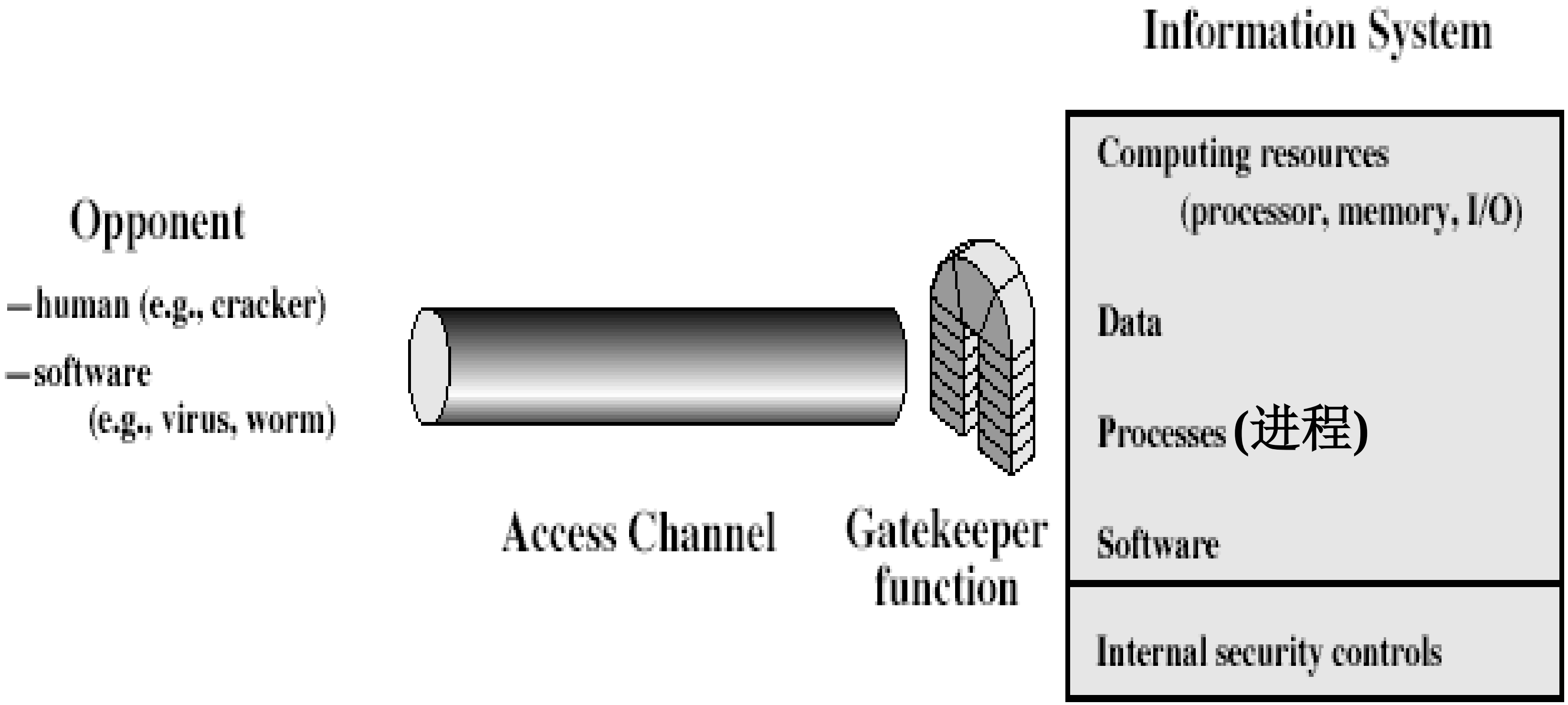
Model for Network Security



Model for Network Security

- using this model requires us to:
  1. design a suitable algorithm for the security transformation
  2. generate the secret information (keys) used by the algorithm
  3. develop methods to distribute and share the secret information
  4. specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



Information System

Computing resources
(processor, memory, I/O)

Data

Processes (进程)

Software

Internal security controls

Opponent

–human (e.g., cracker)

–software
(e.g., virus, worm)

Access Channel

Gatekeeper function

Model for Network Access Security

- using this model requires us to:
  1. select appropriate gatekeeper functions to identify users: login
  2. implement security controls to ensure only authorised users access designated information or resources: monitor in real-time.

Summary

- have considered:
  - definitions for:
    - computer, network, internet security
- X.800 standard
- security attacks, services, mechanisms
- Implementation of Security Services
- models for network (access) security

Review Questions

1.1 What is the OSI security architecture?

1.2 List and briefly define categories of security services.

1.3 List and briefly define categories of security mechanisms

Thanks!