CSE467: Computer Security

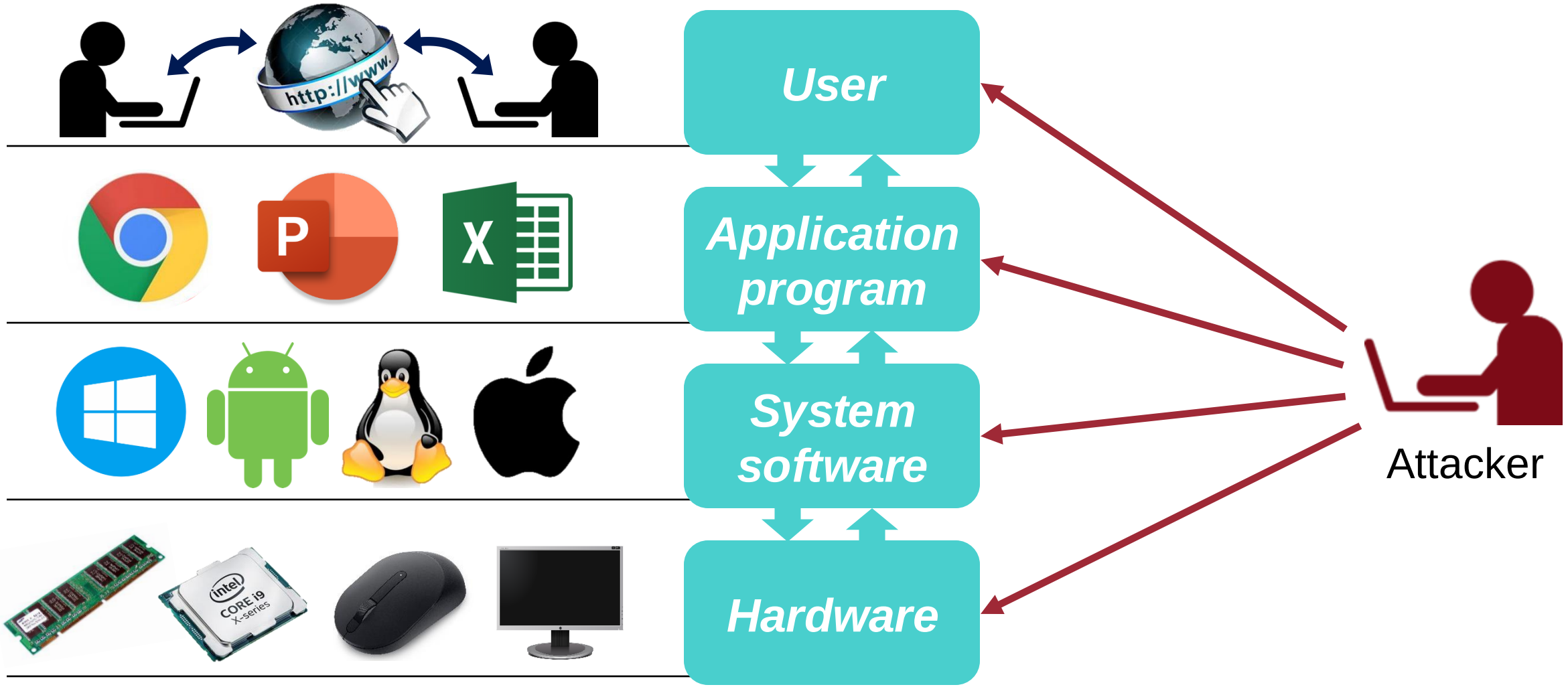
2. Concepts in Security

Seongil Wi

Department of Computer Science and Engineering

Computer Security

The protection of **computer systems** from unauthorized access



Security Properties

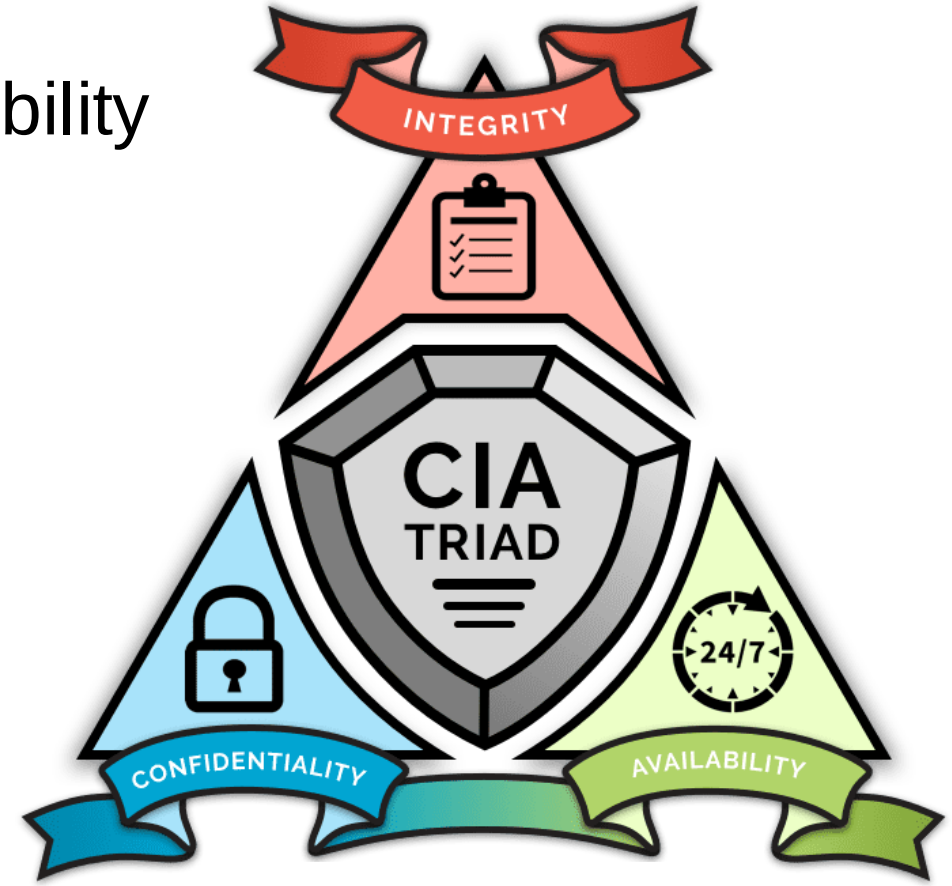
Q. Is Your Computer Secure?

Under what conditions can you say your computer is secure?

Secure Systems Satisfy the CIA Properties

- Three most important **properties** of computer security

- **CIA**: **C**onfidentiality, **I**ntegrity, and **A**vailability



CIA

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

CIA (1): Confidentiality (기밀성)

- **C**onfidentiality: information is not made available to unauthorized parties

- **I**ntegrity

- **A**vailability

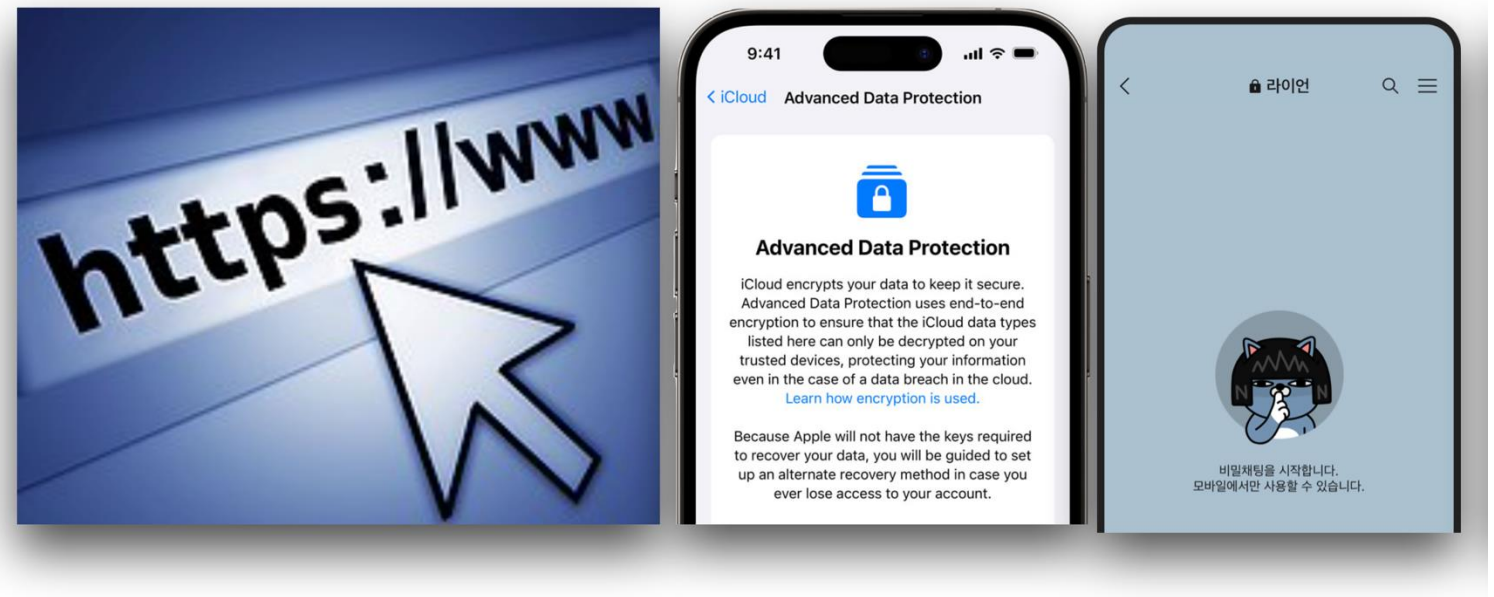
CIA (1): Confidentiality

- Information is not made available to unauthorized parties
- Avoidance of the unauthorized disclosure of information
  - Protection of data
  - Provide access for those who are allowed to see the data
  - Disallow others from learning anything about the data

- How to achieve confidentiality?
  - **Encryption (암호화)**: transformation of information
  - **Authentication (인증):** determination of identity
  - **Access control (접근제어):** gatekeeper

CIA (1): Confidentiality – Encryption

- Transformation of information using an encryption key
- Only be read by another user who has the decryption key
- Schemes: symmetric-key encryption, public-key encryption, etc
- Example:

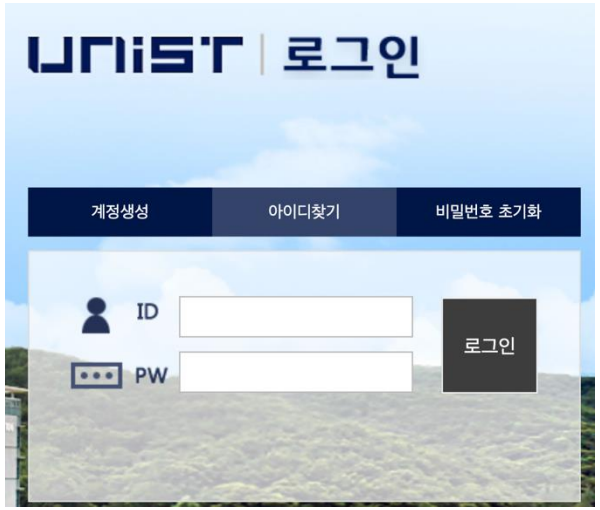


- To be secure: make it **extremely difficult** to decrypt the data without the decryption key

“Delecnac si ssalc txen”

CIA (1): Confidentiality – Authentication

- Determination of the **identity** or **role**
- Typical method
  - Something you are (Fingerprint, iris pattern, …)
  - Something you know (Password, PIN, …)
  - Something you have (Smart card, key, …)



CIA (1): Confidentiality – Access Control

- ***Rules*** and ***policies*** that limit access to confidential information
- Determine what users have permission to do
- Permission is determined by identity (e.g., name, serial) or role (e.g., professor, TA, student)
- Example: Linux file system

	/etc/passwd	/usr/bin	/home/prof/exam_problem/
root	rw	rwx	rwx
professor	r	rx	rwx
ta	r	rx	r
student1	r	rx	-
student2	r	rx	-

Students 1 and 2 are unable to read the exam problem!

CIA (1): Confidentiality – Access Control

Access Control Failure

CIA (1): Confidentiality

Exercise: Internet Banking

- What mechanism is used to achieve confidentiality?
  - Visit the bank website and login
  - ID and PW are sent to the server by your web browser using HTTPS
  - The server allows you to access only your account

CIA (2): Integrity (무결성)

- **C**onfidentiality: information is not made available to unauthorized parties

- **I**ntegrity

- **A**vailability

CIA (2): Integrity (무결성)

- **C**onfidentiality: information is not made available to unauthorized parties

- **I**ntegrity: information is not modified in an unauthorized manner

- **A**vailability

CIA (2): Integrity

Information has not been altered in an unauthorized way

- **Benign compromise**: information altered by accident
  - E.g., bit flips in memory due to cosmic ray

CIA (2): Integrity – Benign Compromise

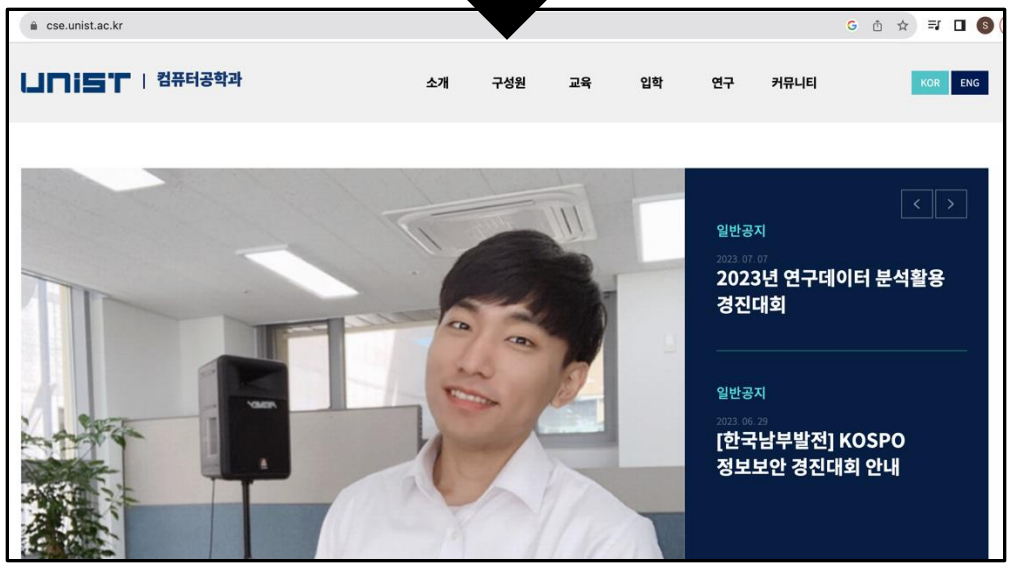
CIA (2): Integrity

Information has not been altered in an unauthorized way

- **Benign compromise**: information altered by accident
  - E.g., bit flips in memory due to cosmic ray

- **Malicious compromise**: information altered by attackers
  - E.g., malicious code that changes some files in a system

CIA (2): Integrity – Malicious Compromise



수면위로 떠오른 UNIST(유니스트) '해킹 사건'

입력 2017-04-29 09:28

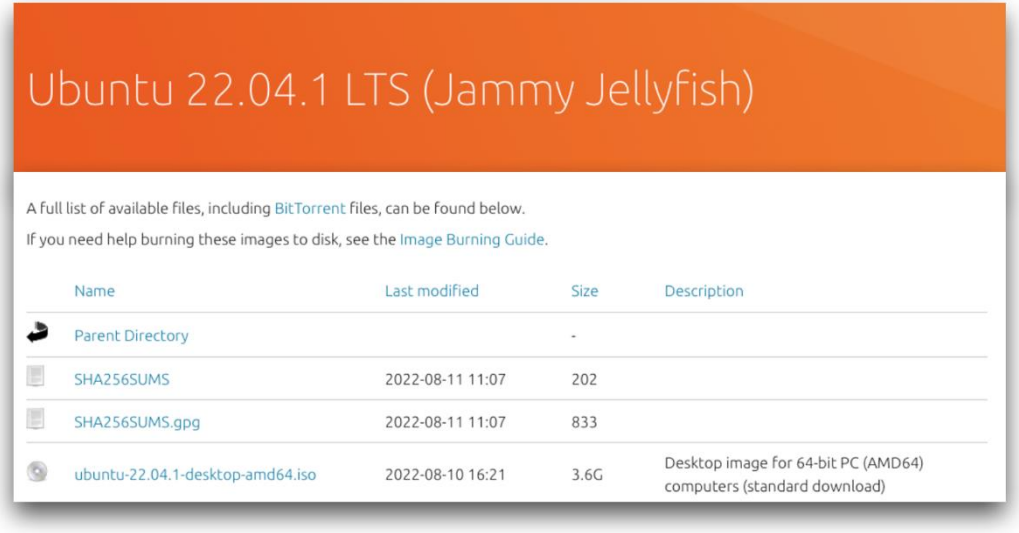
> '룸메이트 바꾸려고' 전산망 뚫어…2013년부터 총 4건
> 유니스트 보안 정보 둔감 '지적'

지난 2014년 3월 유니스트 해킹동아리가 학교전산망에 침입, 자신들의 해커 모집광고를 종합전산망 홈피에 게재해 놓은 배너 모습.

CIA (2): Integrity

Ensuring Integrity

- How to ensure the integrity of computer systems?
- **Backups**: periodic archiving of data
- **Checksums**: computation of a function that maps the data to a numerical value



CIA (3): Availability (가용성)

- **C**onfidentiality: information is not made available to unauthorized parties

- **I**ntegrity: information is not modified in an unauthorized manner

- **A**vailability

CIA (3): Availability (가용성)

- **C**onfidentiality: information is not made available to unauthorized parties

- **I**ntegrity: information is not modified in an unauthorized manner

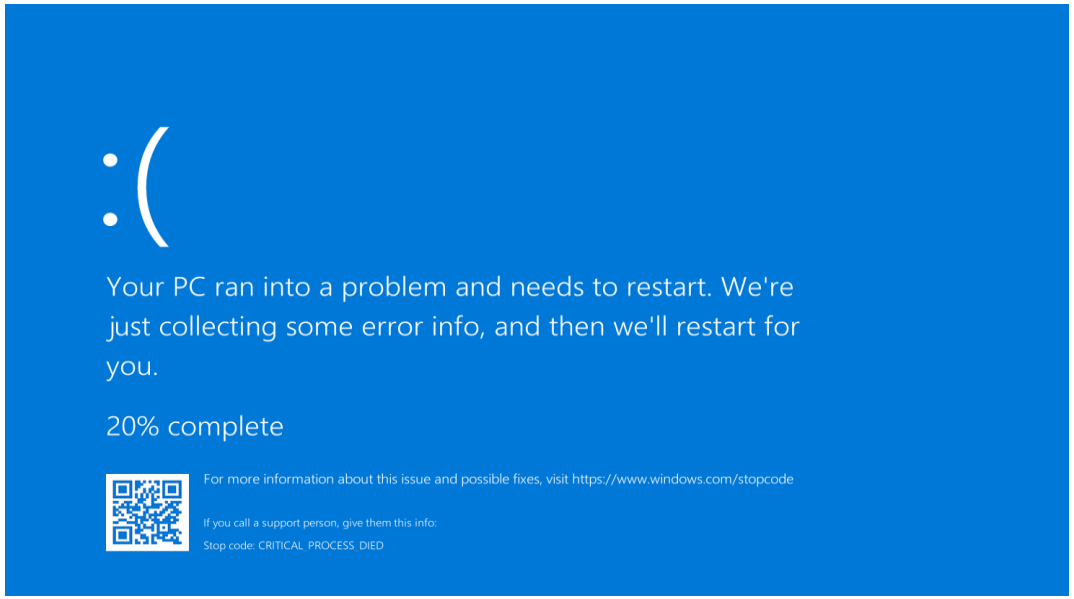
- **A**vailability: information is readily available when it is needed

CIA (3): Availability

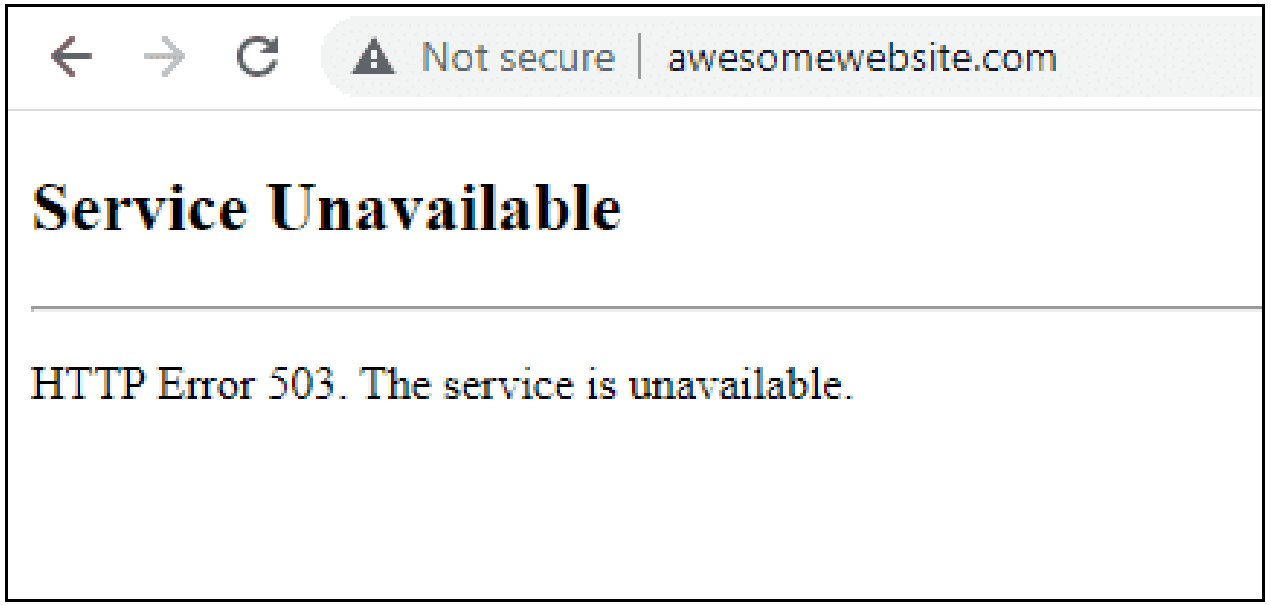
- Information is ***accessible*** and ***modifiable*** in a timely fashion
- Imagine a unbreakable and unopenable vault. Is it useful?

CIA (3): Availability

- Information is ***accessible*** and ***modifiable*** in a timely fashion
- Imagine a unbreakable and unopenable vault. Is it useful?



Blue Screen of Death



503 Error

CIA (3): Availability

- Information is ***accessible*** and ***modifiable*** in a timely fashion
- Imagine a unbreakable and unopenable vault. Is it useful?

Kakao's meltdown raises big questions about its management

"President office said
KaKao's network disturbance could even be **a threat to national security**"

CIA (3): Availability

- Information is ***accessible*** and ***modifiable*** in a timely fashion
- Imagine a unbreakable and unopenable vault. Is it useful?

- How to achieve availability?
  - **Physical protections**: keep information available even in physical challenges (e.g., storms, earthquakes, or power outages)
  - **Computational redundancies**: computers that serve as fallbacks in the case of failure

Other properties?

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

Other properties?

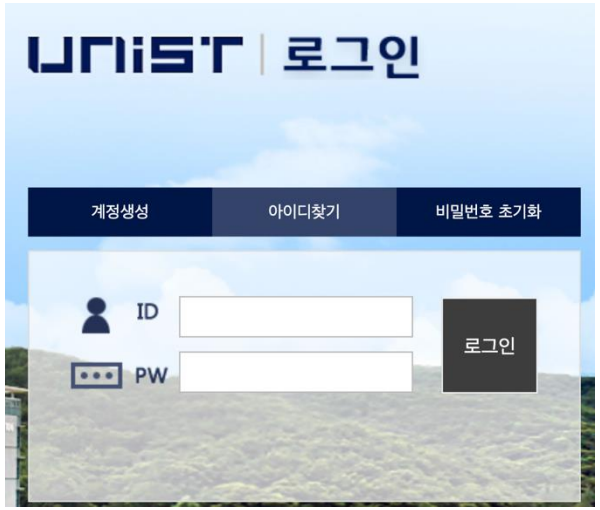
- **C**onfidentiality
- **I**ntegrity
- **A**vailability

+ **Authentication**: the ability of a computer system to *confirm the sender's identity*

+ **Non-repudiation**: the ability of a computer system to *confirm that the sender can not deny about something sent*

Authentication (인증)

- Determination of the **identity** or **role**
- Typical method
  - Something you are (Fingerprint, iris pattern, …)
  - Something you know (Password, PIN, …)
  - Something you have (Smart card, key, …)



Non-repudiation (부인방지)

- A party cannot deny the authenticity of a message or transaction
- How to determine that statements, policies, and permissions are genuine?

- What happens if those can be faked?
  - "I did not make commitment. Maybe someone pretended to be me! (오리발 내밀기)"

- **Non-repudiation** by secure authentication: authentic statement cannot be denied
  - E.g., digital signature

Aspects of Security

Aspects of Security

- Consider three aspects of information security:
  - **Security attack:** Any action that compromises the security of information (e.g., DDoS)
  - **Security service:** A service which ensures adequate security of the systems or of data transfers (e.g., availability, confidentiality)
  - **Security mechanism:** A mechanism that is designed to detect, prevent, or recover from a security attack (e.g., firewall)

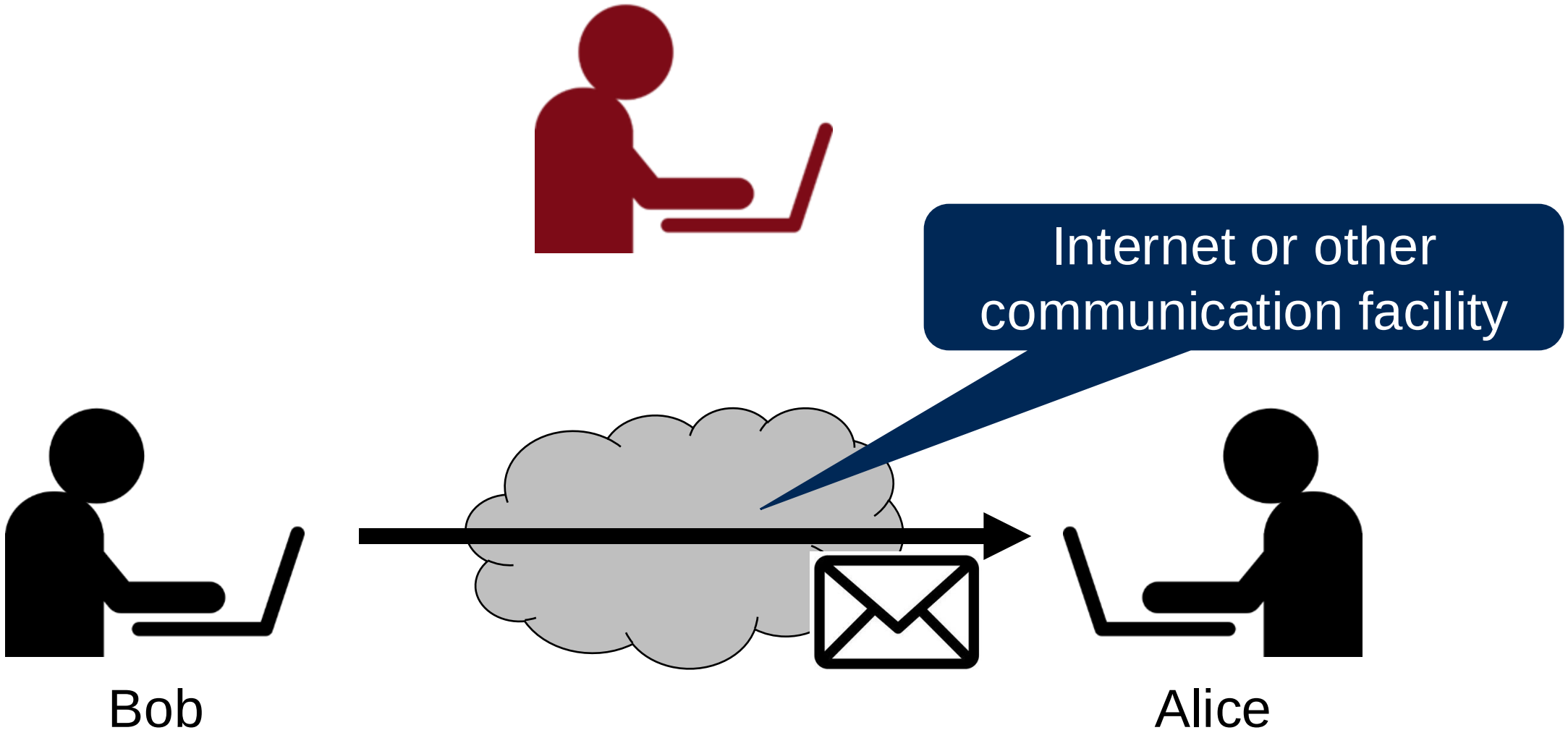
Security Attacks

- Note terms
  - Threat: a potential for violation of security
  - Attack: an attempt to evade/compromise security services

- **Passive attacks**
  - Observing the information from the system without affecting system resources

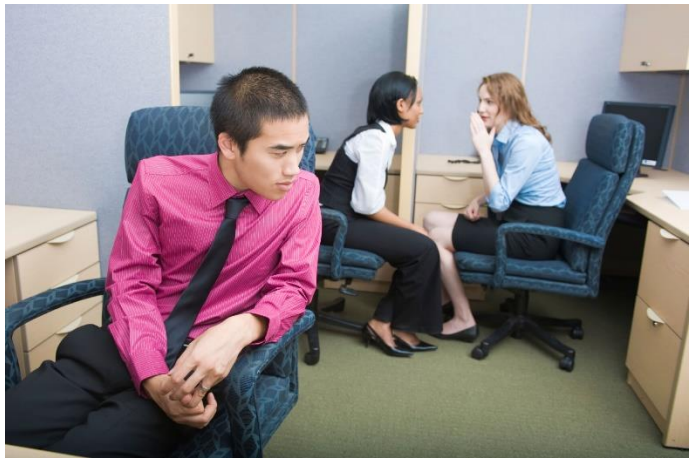
- **Active attacks**
  - Try to alter system resources or affect their operation

Passive Attacks



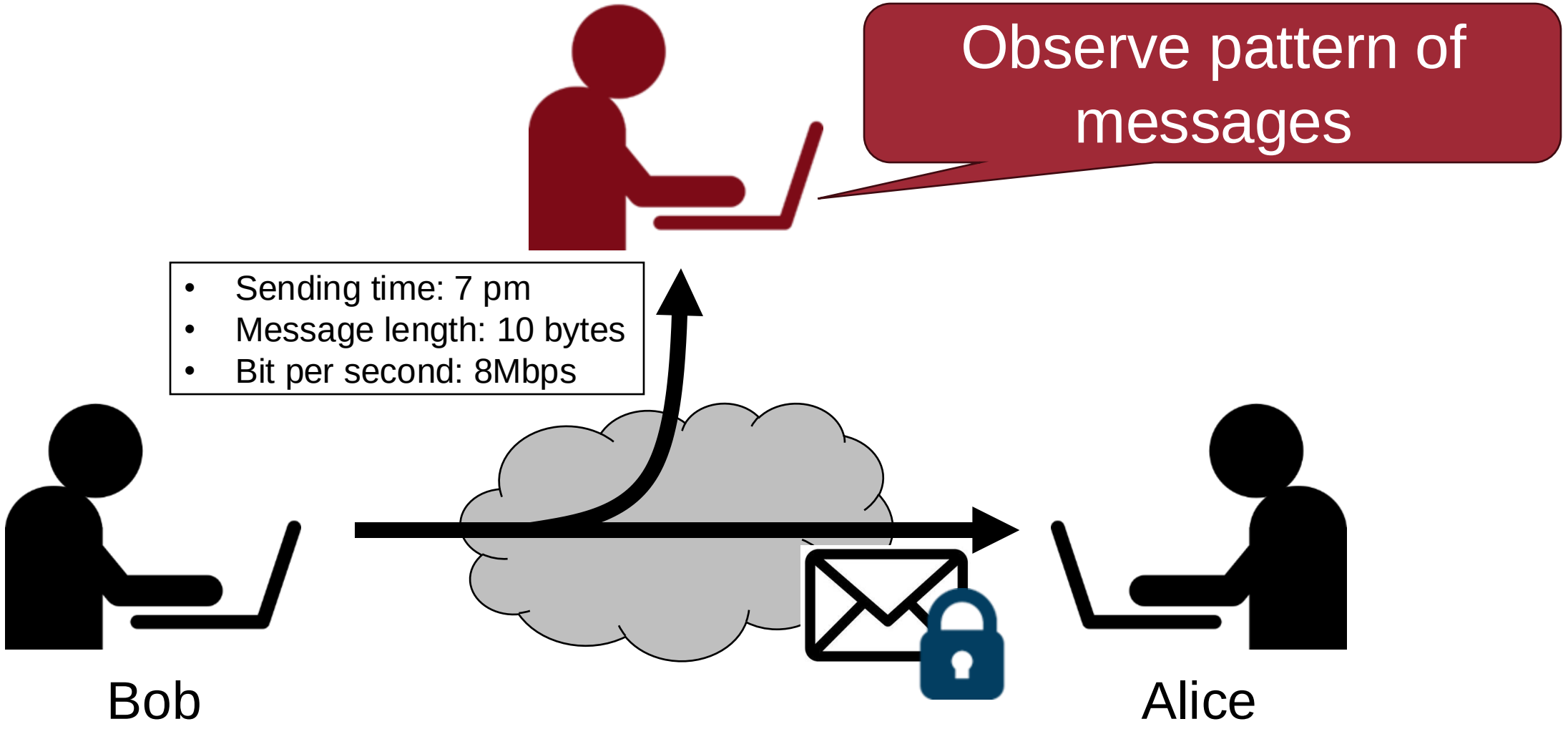
Passive Attacks

- Disclosure of message contents (e.g., eavesdropping)



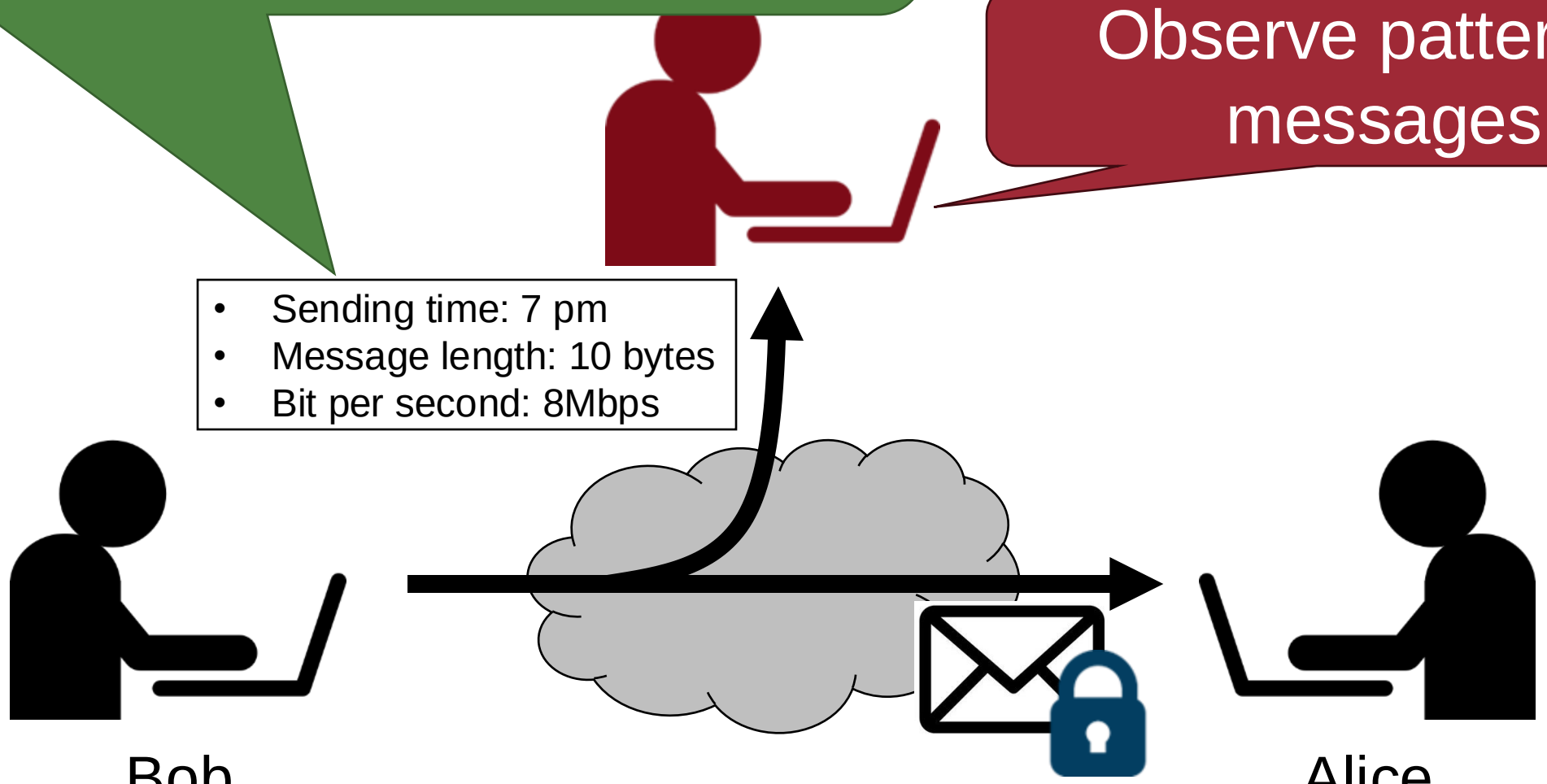
Passive Attacks

- Traffic analysis



- Watching the Watchers: Practical Video Identification Attack in LTE Networks, ***USENIX'22***
- Beauty and the Burst: Remote Identification of Encrypted Video Streams, ***USENIX'17***

Observe pattern of messages



Passive Attacks – Lessons

- Difficult to ***detect*** (after they occurred)
  - Because they do not involve any change of the data

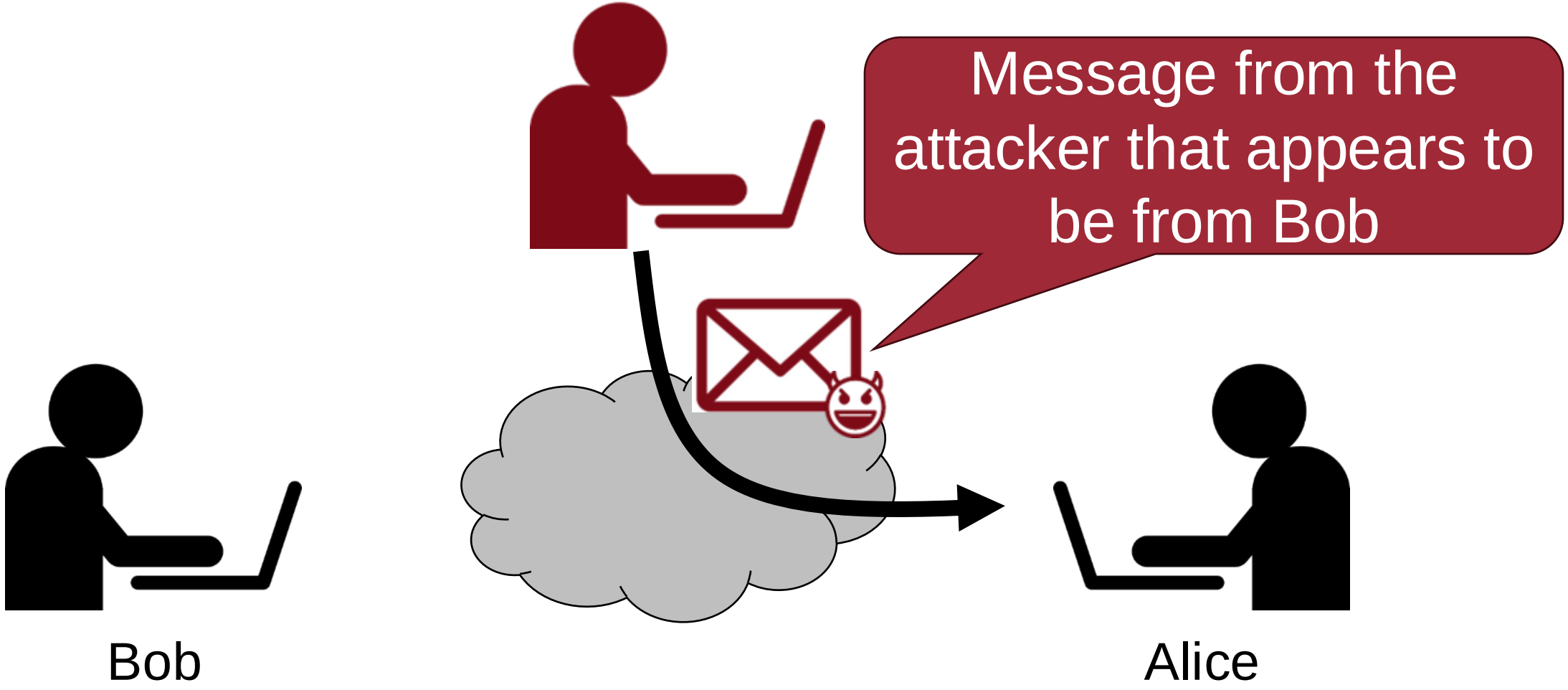
- Thus, they should be **prevented** rather than be **detected**

Active Attacks

- **Creating illegitimate messages**
  - Masquerade (who)
  - Replay (when)
  - Modification of messages (what)
- **Denying legitimate messages**
  - Repudiation
- **Making system facilities unavailable**

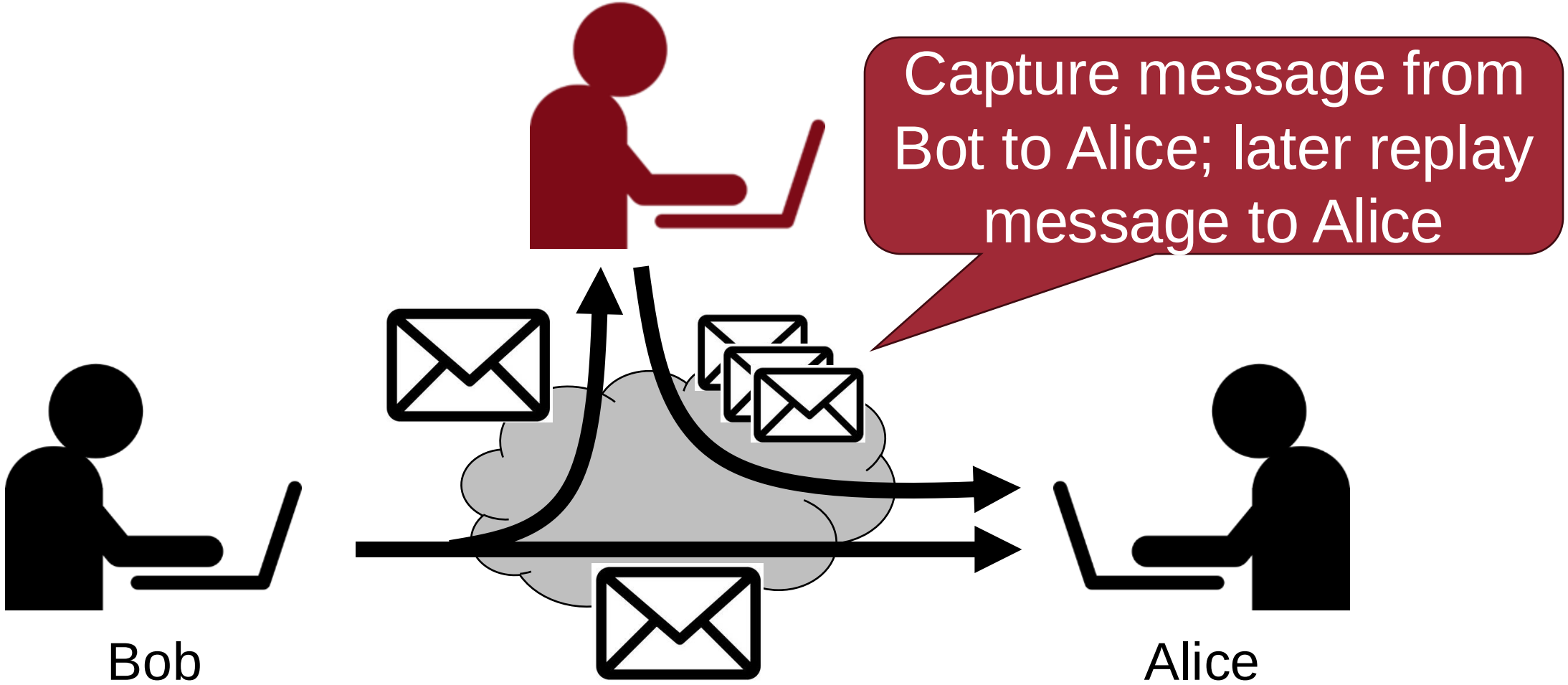
Active Attacks

- Masquerade
  - One entity pretends to be a different entity



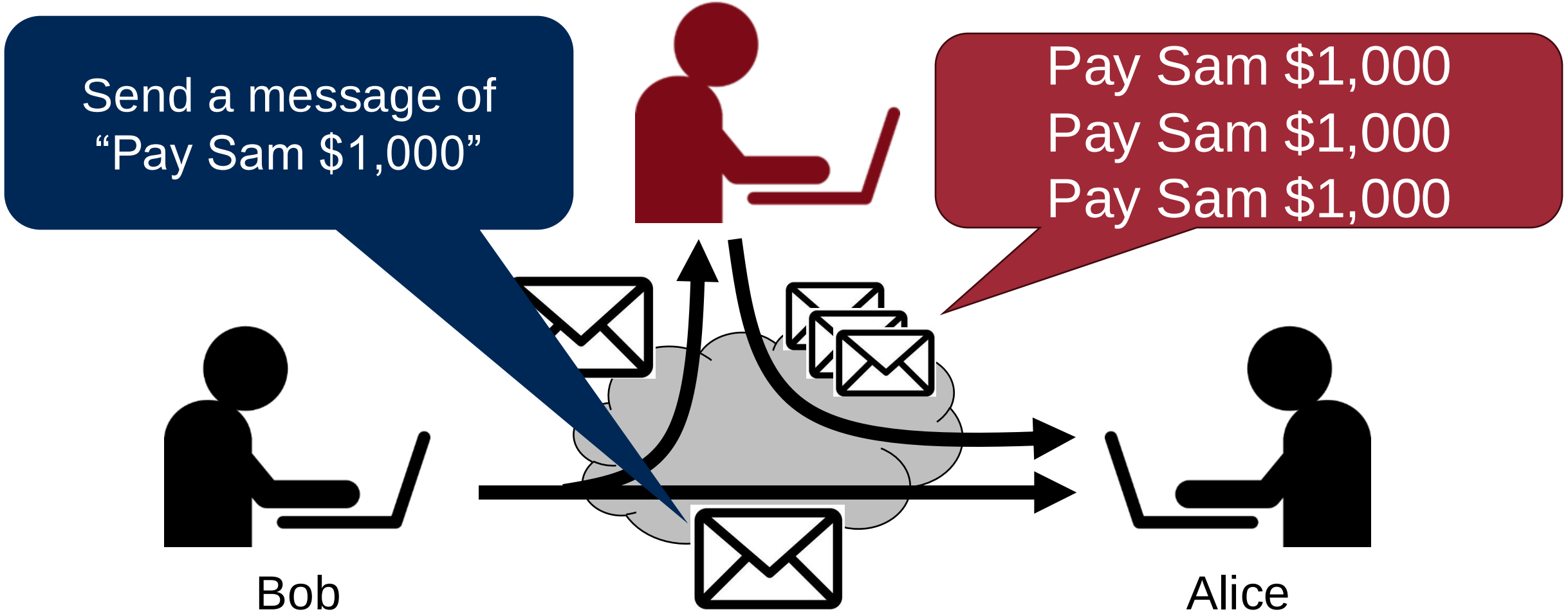
Active Attacks

- Replay
  - A message is captured and retransmitted later



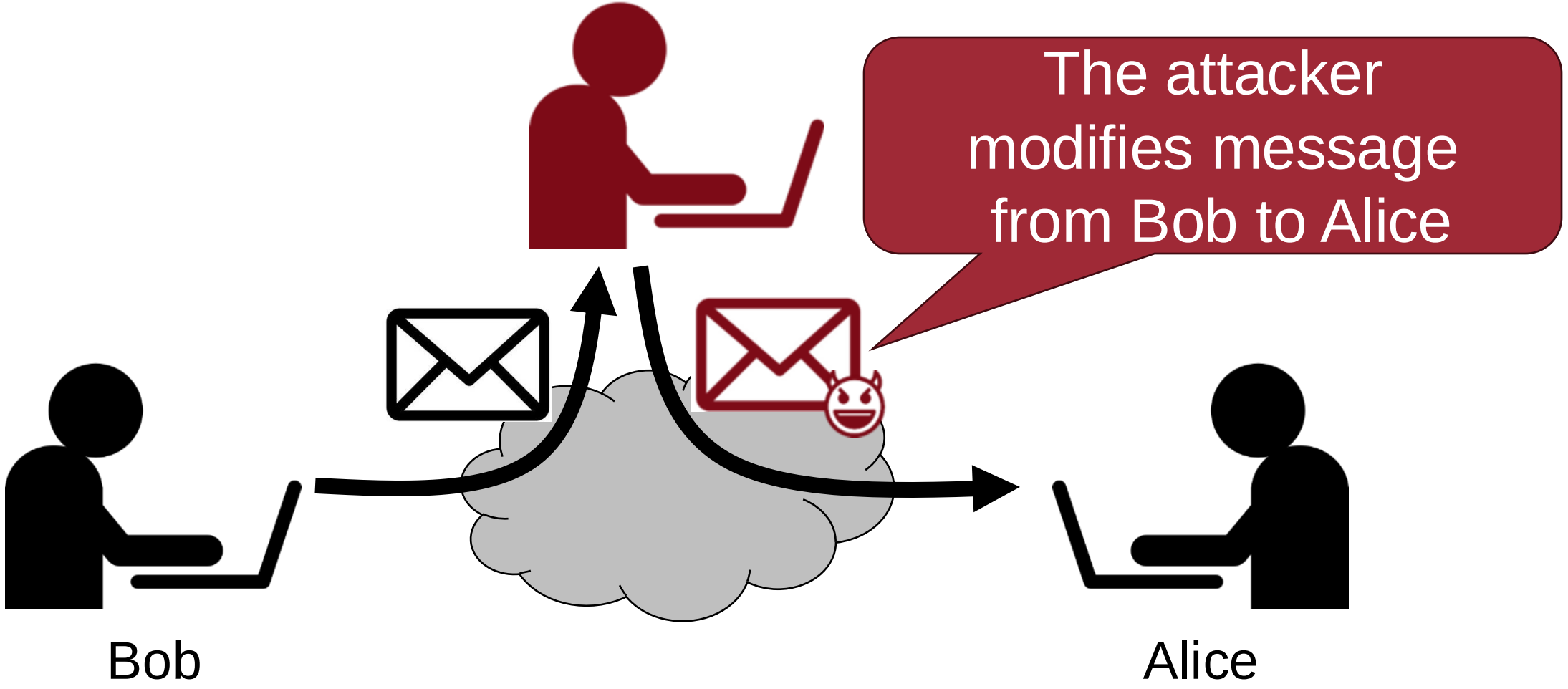
Active Attacks

- Replay
  - A message is captured and retransmitted later



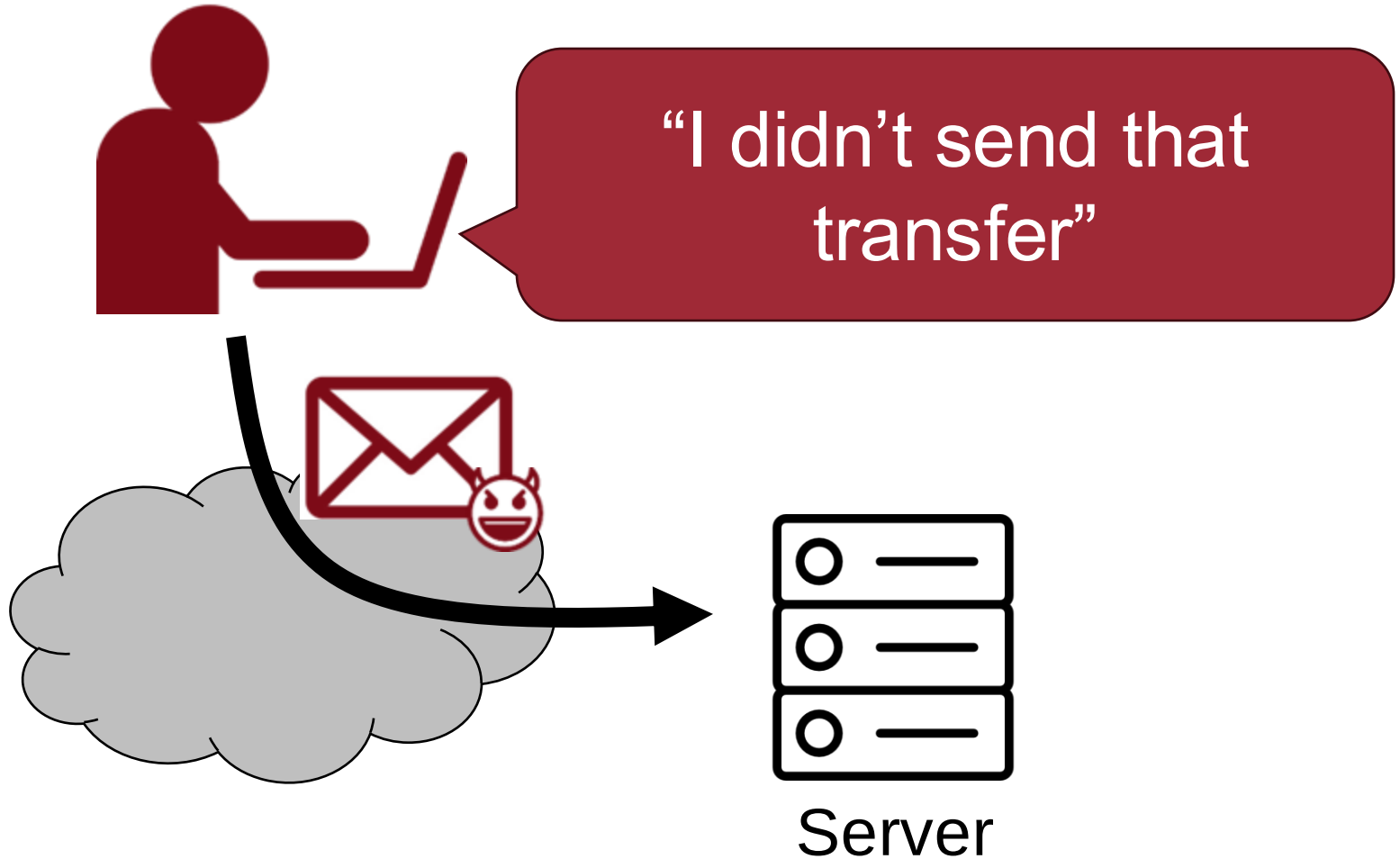
Active Attacks

- Modification of messages
  - A message is captured, modified, and transmitted



Active Attacks

- Repudiation
  - Denial of sending or receiving messages



Active Attacks

- Denial of Service (DoS)
  - Making system facilities unavailable

Active Attacks – Lessons

- Difficult to ***prevent***
  - Because of new/unknown vulnerabilities

- So, the goal is to **detect** active attacks and to **recover** as soon as possible

Security Mechanism

- Feature designed to detect, prevent, or recover from a security attack

- E.g., Cryptography (encipherment, digital signatures)

Introduction to Cryptography

Cryptography – Overview

- Cryptography is about **confidentiality** and **integrity**

What about availability?

Cryptographic Primitives

- Symmetric key encryption/decryption
- Asymmetric key encryption/decryption
- Digital signatures
- Hash functions
- Etc.

Symmetric Key Cryptography

- The same key is used to encrypt/decrypt messages
  - Also known as secret key algorithm

Alice

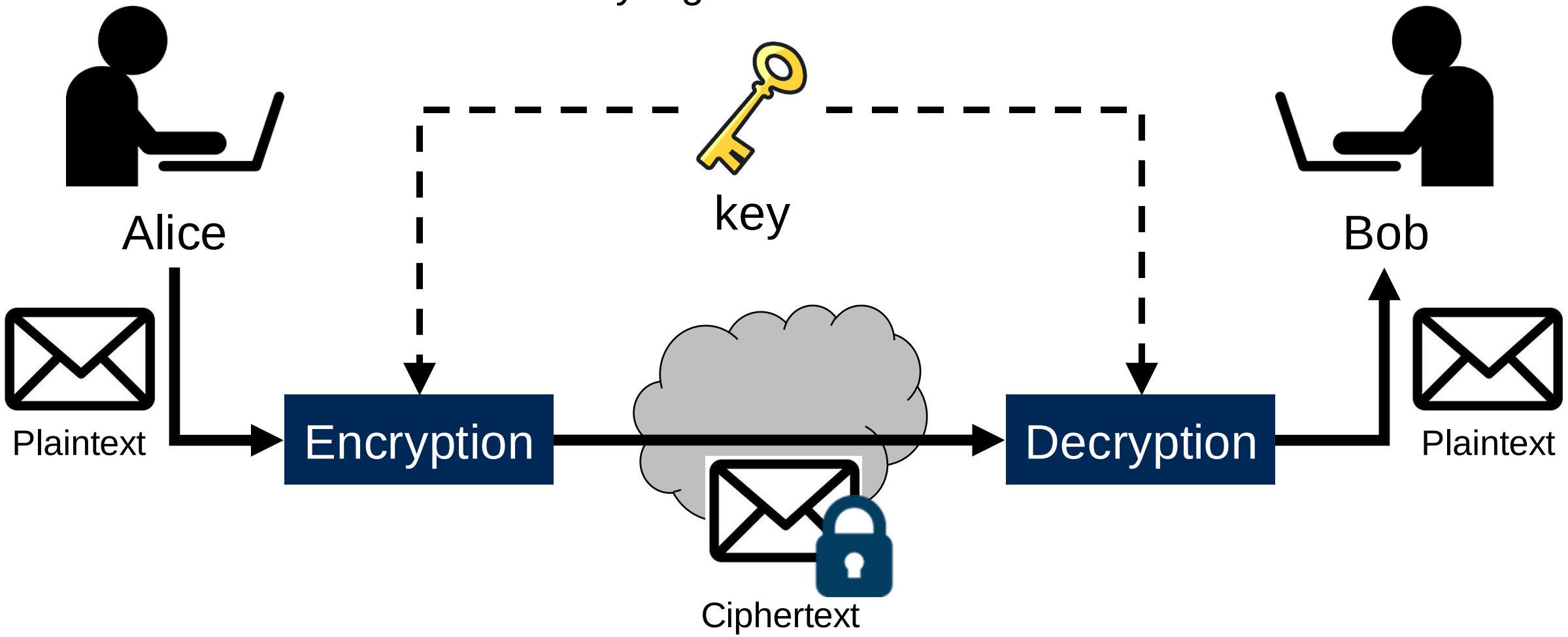
key

Bob

Shared secret key

Symmetric Key Cryptography

- The same key is used to encrypt/decrypt messages
  - Also known as secret key algorithm



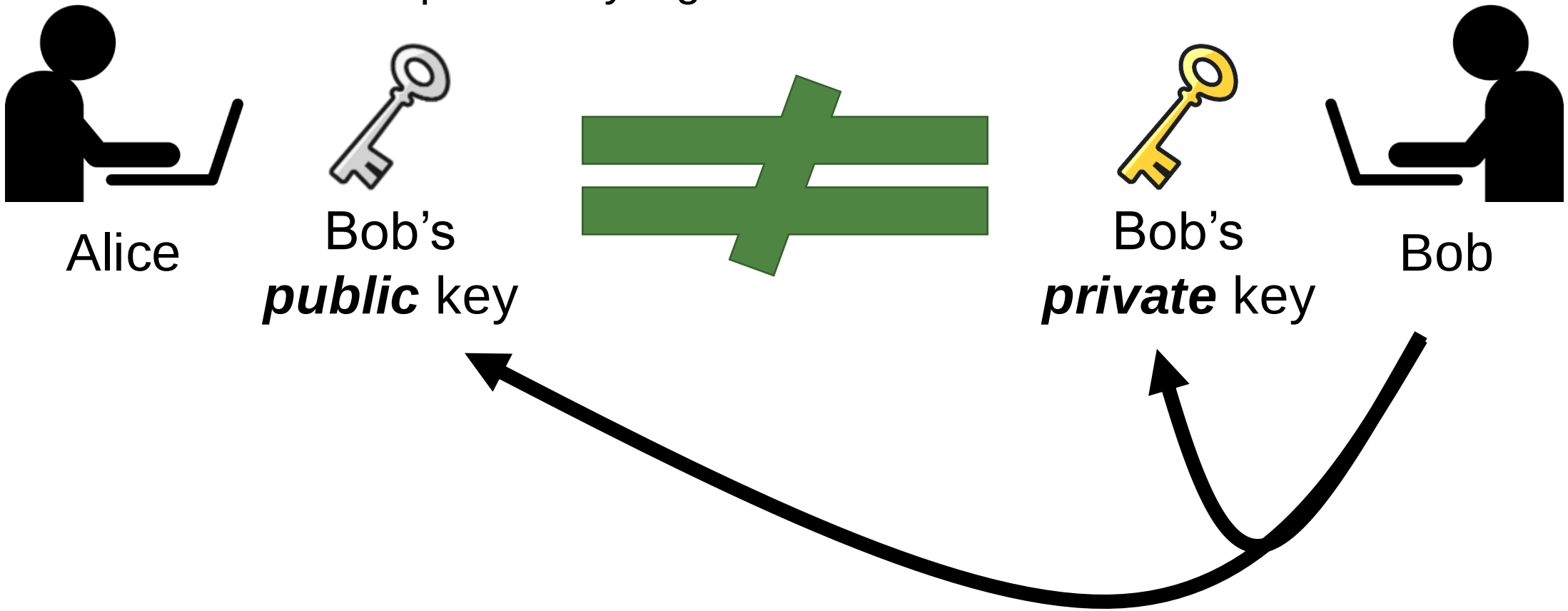
Symmetric Key Cryptography

- Pros?
  - Fast
  - Intuitive

- Cons?
  - Once the key is compromised, then the whole system becomes useless
  - Key sharing is difficult
  - Digital sign is difficult

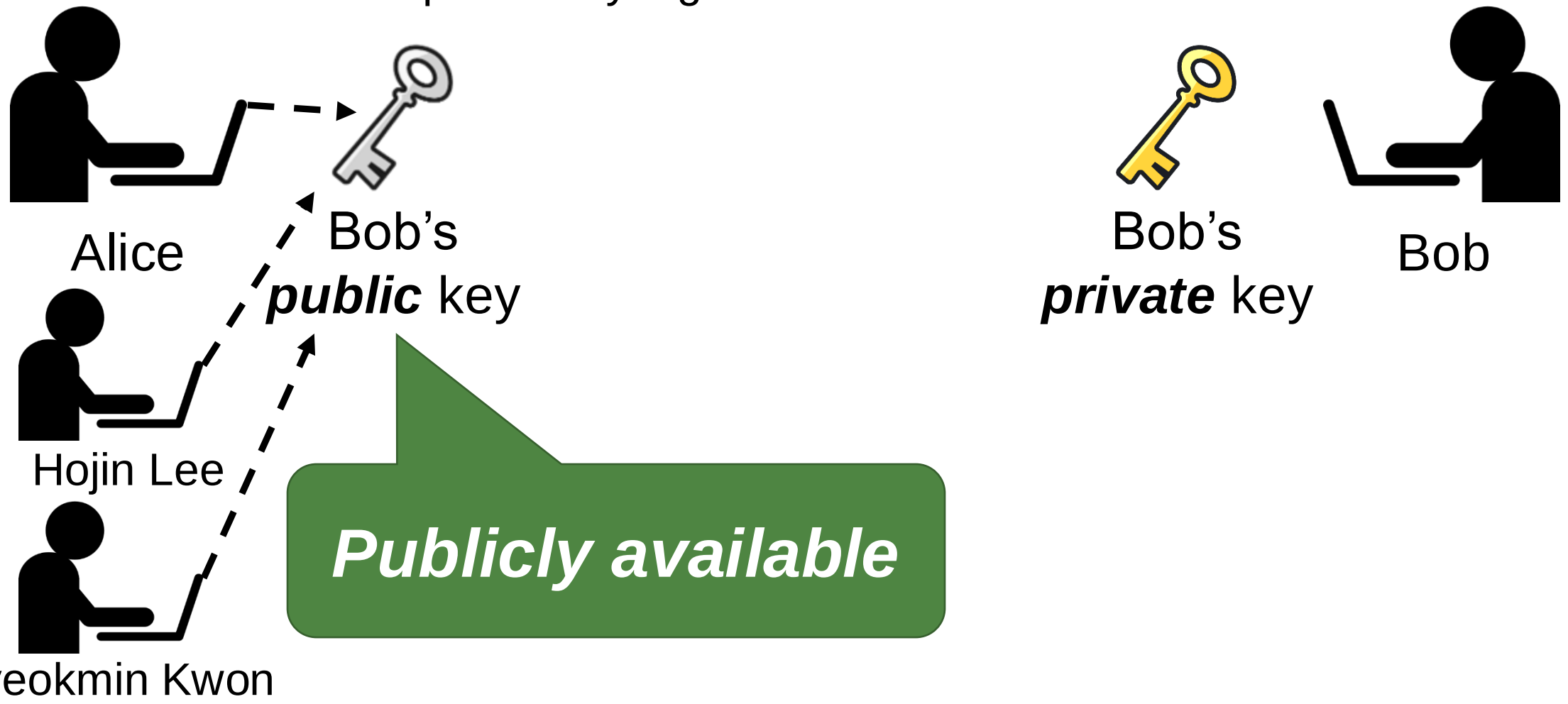
Asymmetric Key Cryptography

- Each party has two distinct keys: public key and private key
  - Also known as public-key algorithm



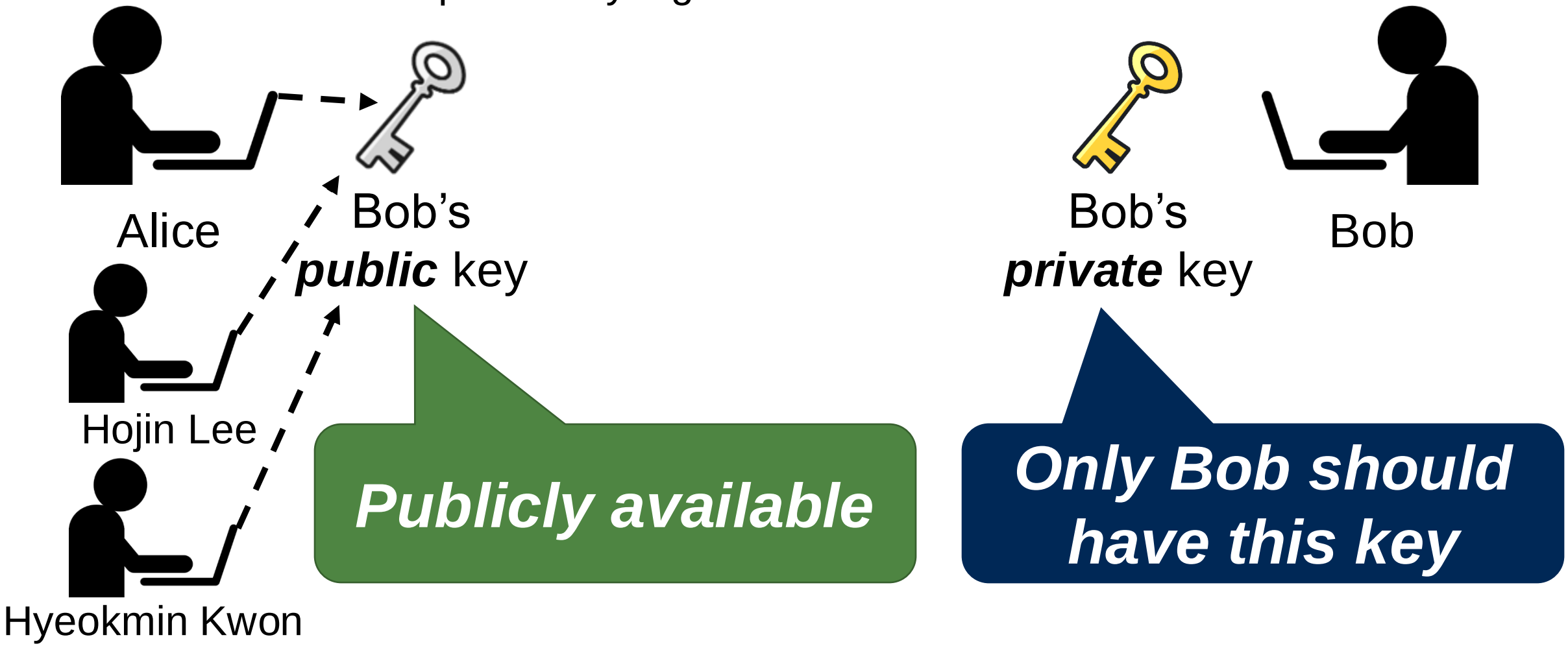
Asymmetric Key Cryptography

- Each party has two distinct keys: public key and private key
  - Also known as public-key algorithm



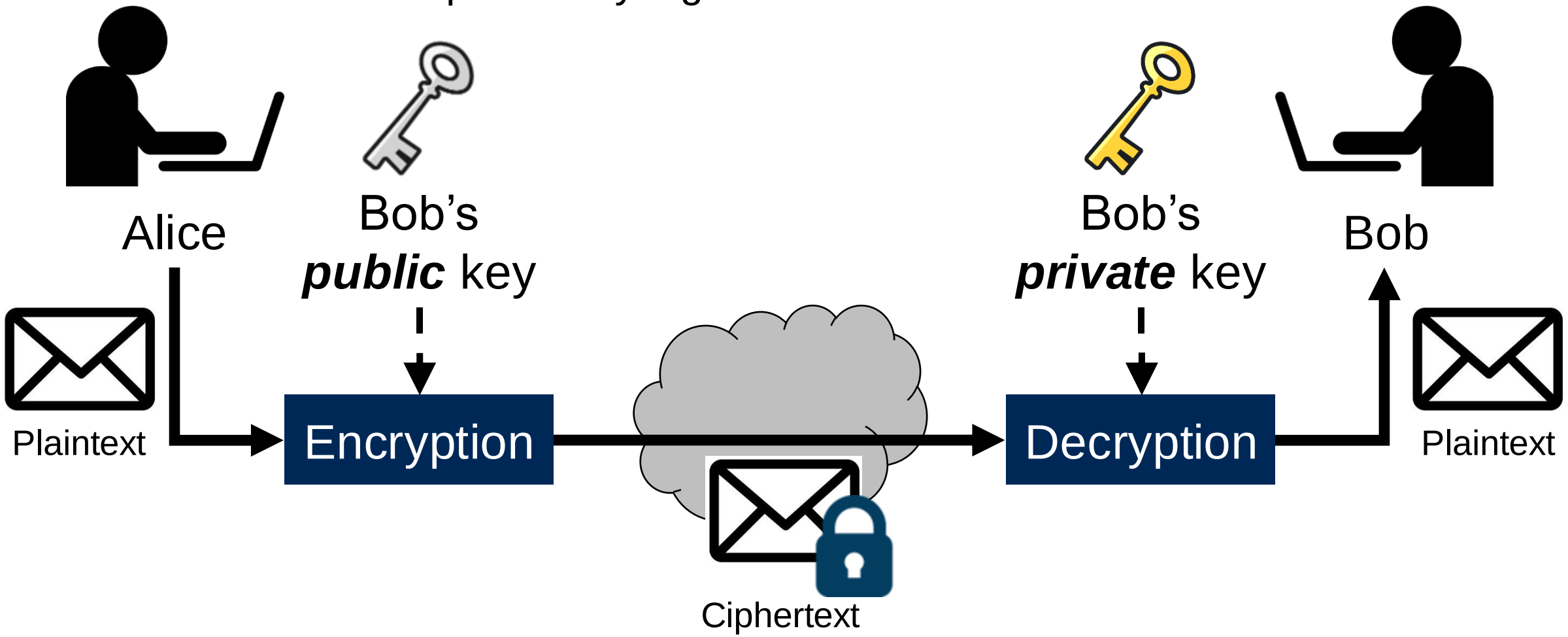
Asymmetric Key Cryptography

- Each party has two distinct keys: public key and private key
  - Also known as public-key algorithm



Asymmetric Key Cryptography

- Each party has two distinct keys: public key and private key
  - Also known as public-key algorithm

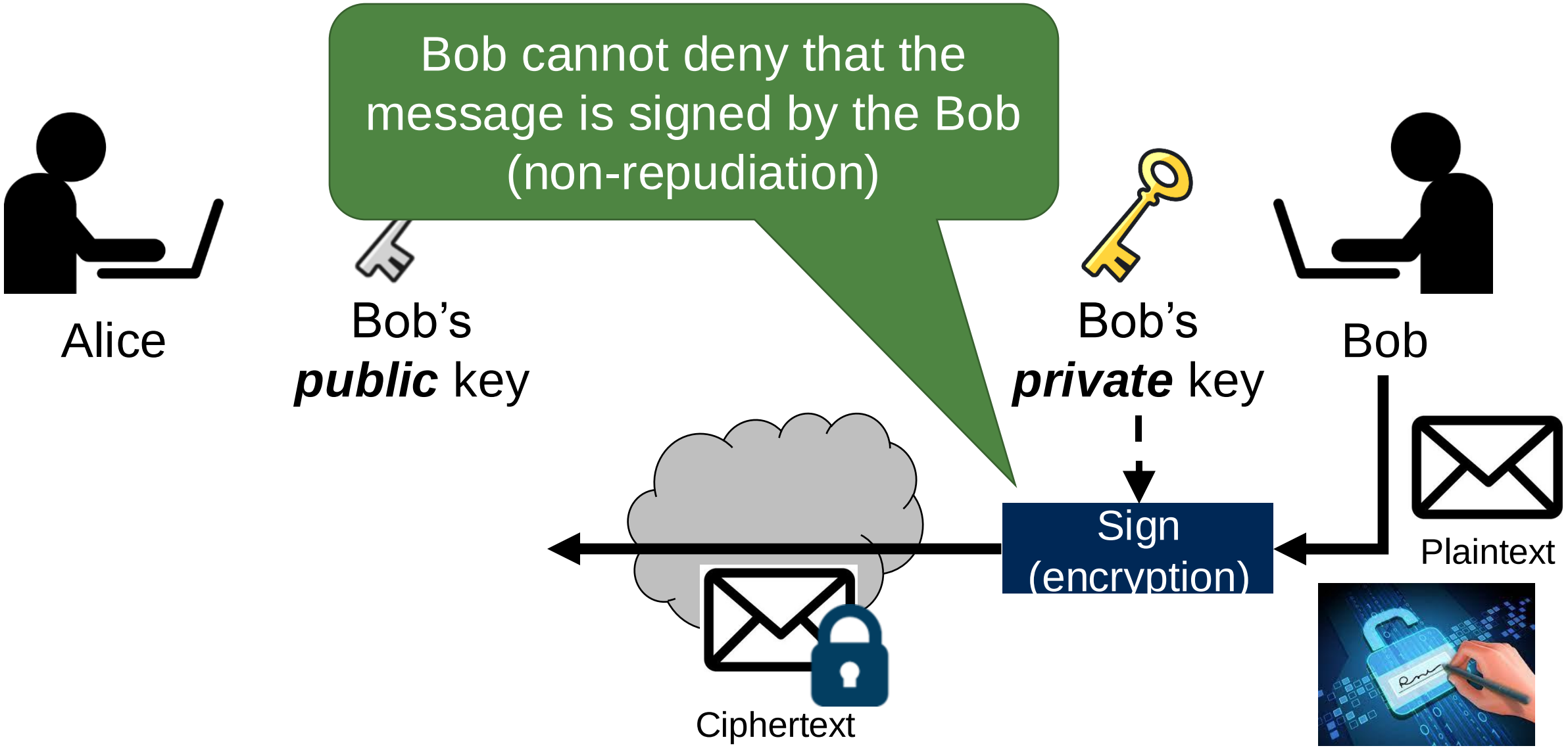


Asymmetric Key Cryptography

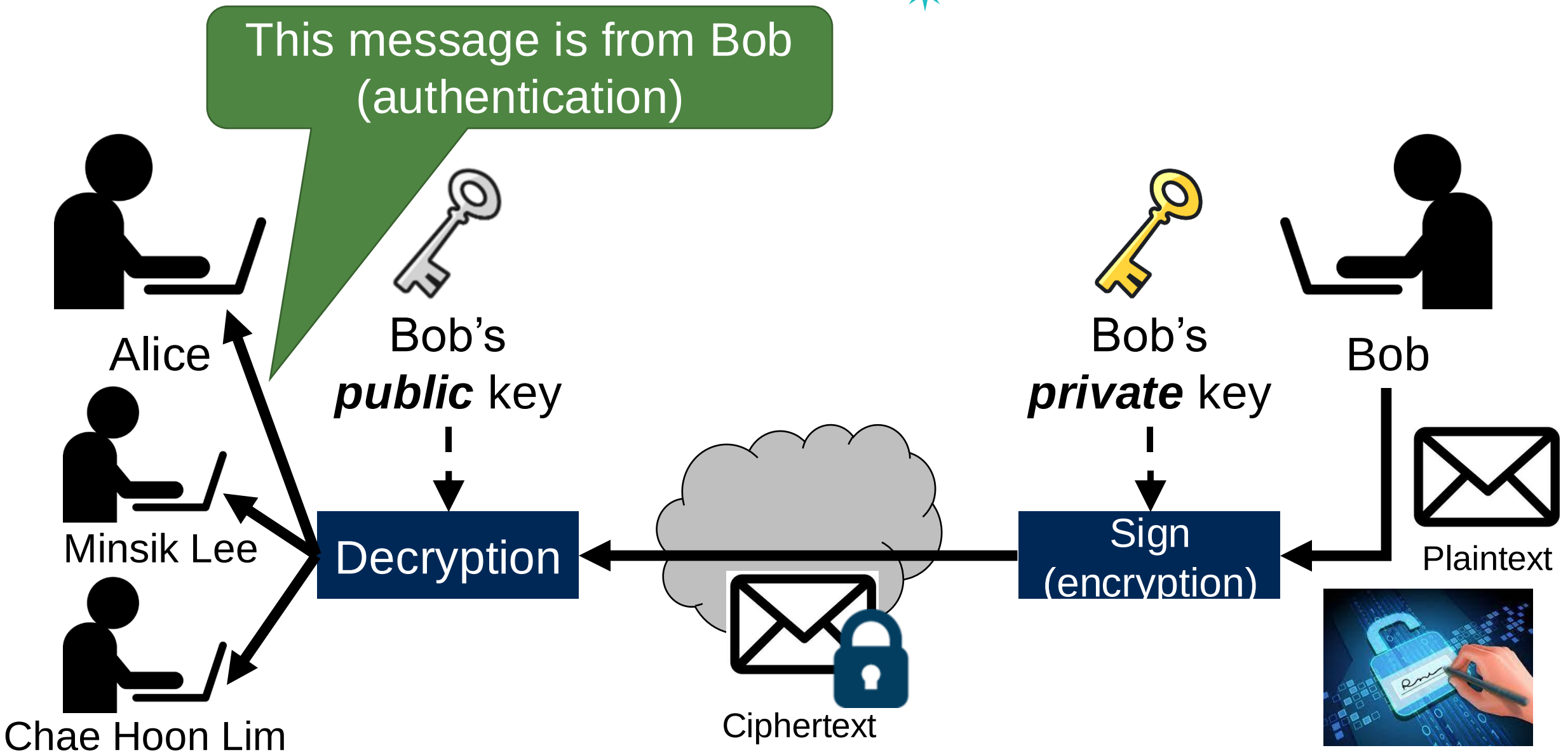
- Pros?

- Cons?

Digital Signature



Digital Signature



Summary

- **The goal of security**: understanding possible threats in computer systems
- **The CIA triad**: fundamental security properties
  - − Confidentiality, Integrity, Availability
  - + Authentication, Non-repudiation
- **Aspects of security**:
  - − Security attack, Security service, Security mechanism
- What should you do now in order to make your software/information/computer secure?
  - − Learn the basic cryptographic primitives (next lecture)

Question?