

# CSE467: Computer Security

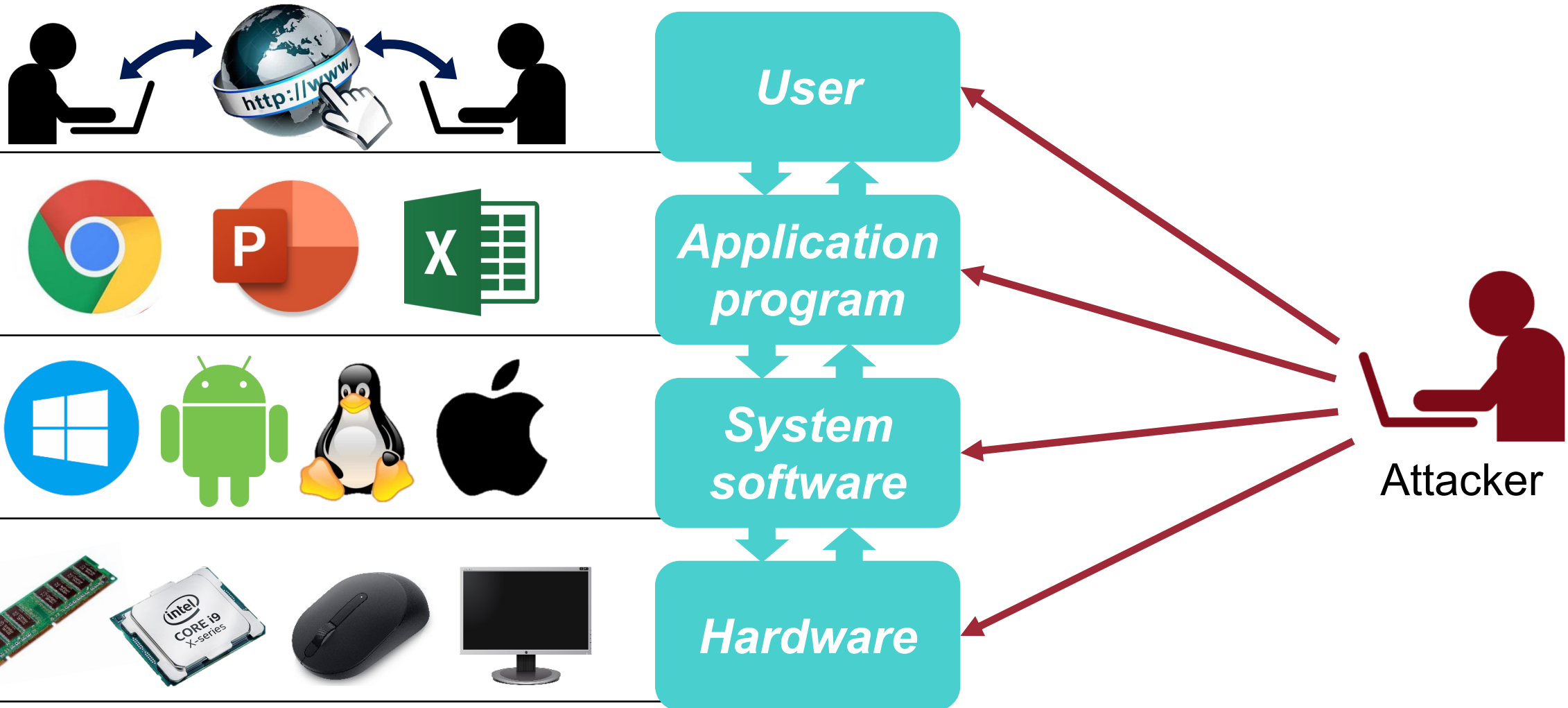
## 2. Concepts in Security

Seongil Wi

# What is Computer Security?

# Computer Security

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



# Q. Is Your Computer Secure?

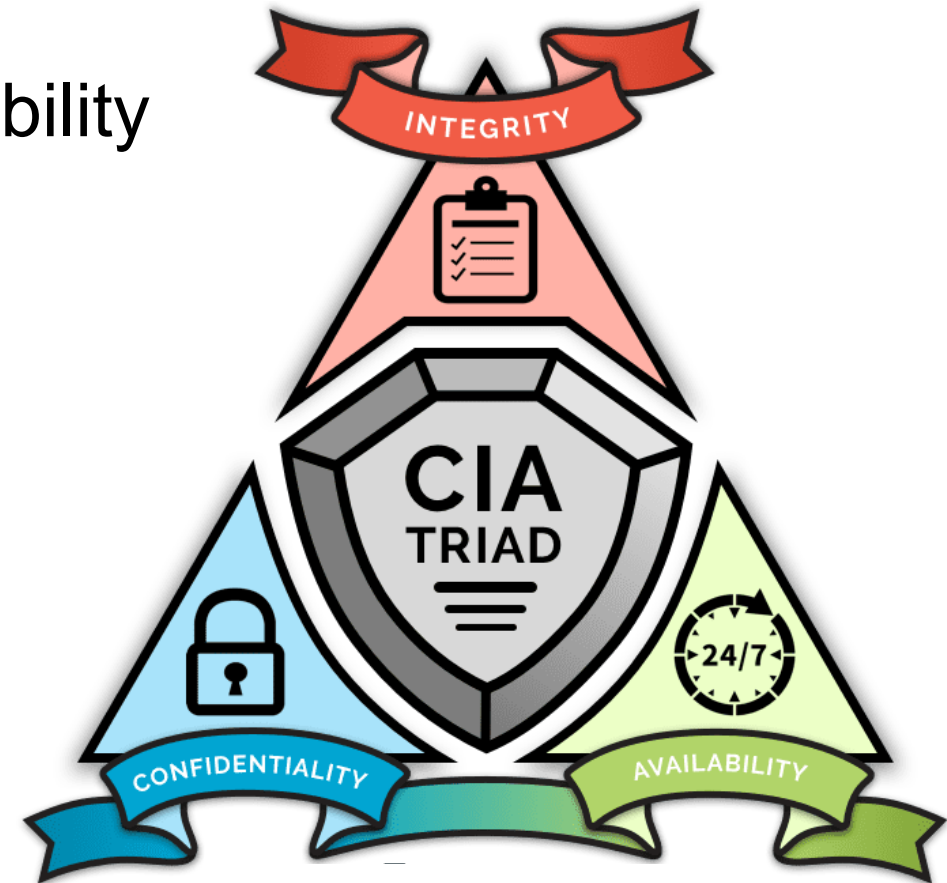
---



- **Under what conditions** can you say your computer is secure?

# Secure Systems Satisfy the CIA Properties 5

- Three most important **properties** of computer security
- **CIA**: Confidentiality, Integrity, and Availability
- Example: a bank system
  - Confidentiality?
  - Integrity?
  - Availability?



# Secure Systems Satisfy the CIA Properties 6

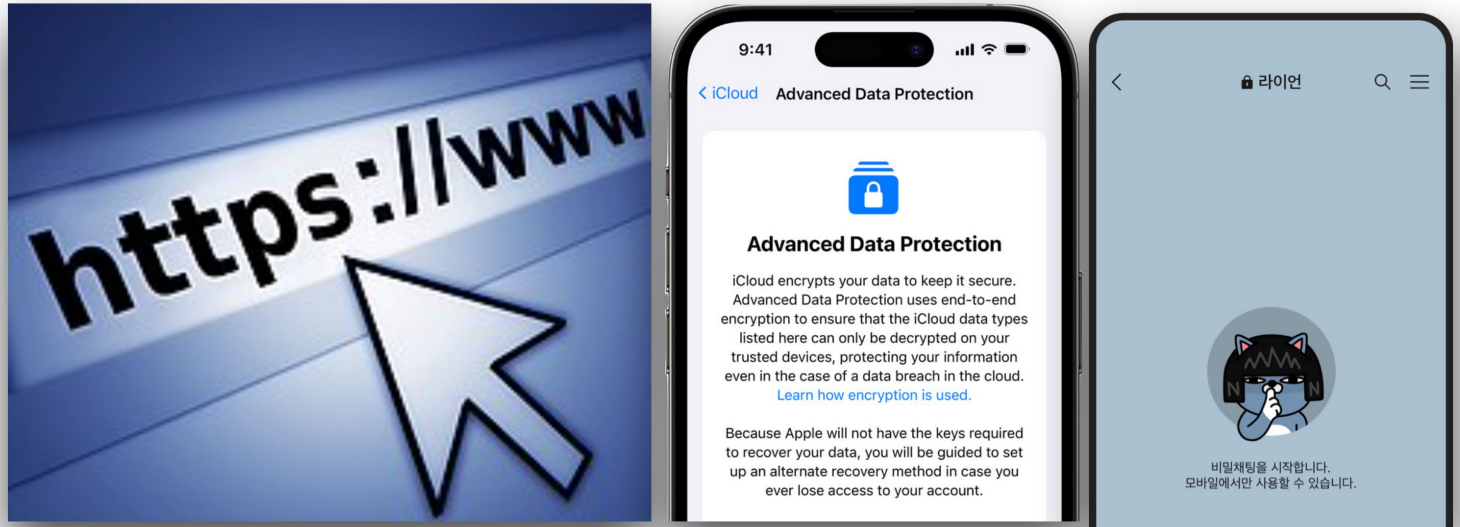
- **Confidentiality:** information is not made available to unauthorized parties
- **Integrity:** information is not modified in an unauthorized manner
- **Availability:** information is readily available when it is needed

# CIA (1): Confidentiality

- 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**: transformation of information
  - **Access control**: gatekeeper
  - **Authentication**: determination of identity

# 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 – Encryption

9

## Easily Breakable Encryption

S

Can you decrypt the following ciphertext?

Delecnac si ssalc txen



The provided ciphertext "Delecnac si ssalc txen" is already decrypted when read backward. When reversed, it reads "next class is cancelled." It seems like the text has been encoded using a simple backward or reversal transformation.

# CIA (1): Confidentiality – Access Control

10

- **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

11

## Access Control Failure



# CIA (1): Confidentiality – Authentication

12

- 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, ...)




UNIST | 로그인

계정생성 아이디찾기 비밀번호 초기화

ID

PW

로그인



UNIST

joon@unist.ac.kr

ID 확인

+XX XXXXXXXXXX79에 문자 메시지

+XX XXXXXXXXXX79에 전화

추가 정보

확인 방법이 최신 상태입니까? <https://aka.ms/mfasetup>에서 확인하세요.

취소

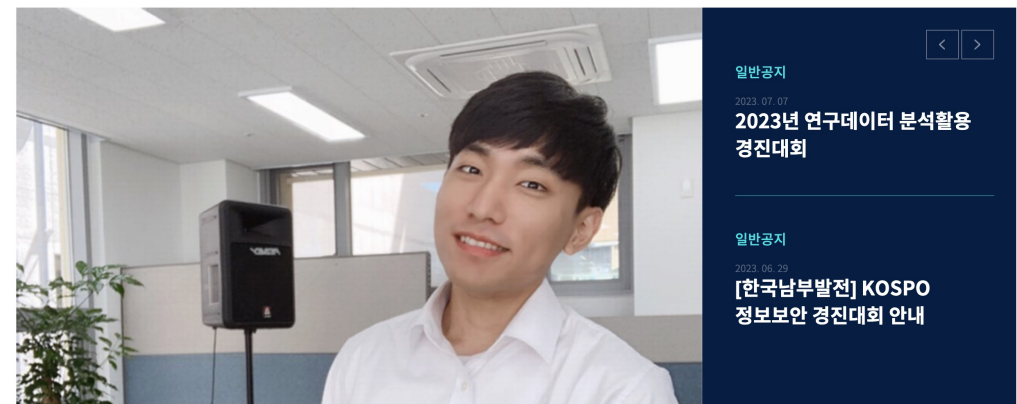
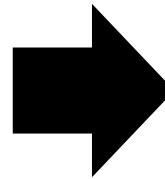
## **Exercise: Internet Banking**

- 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



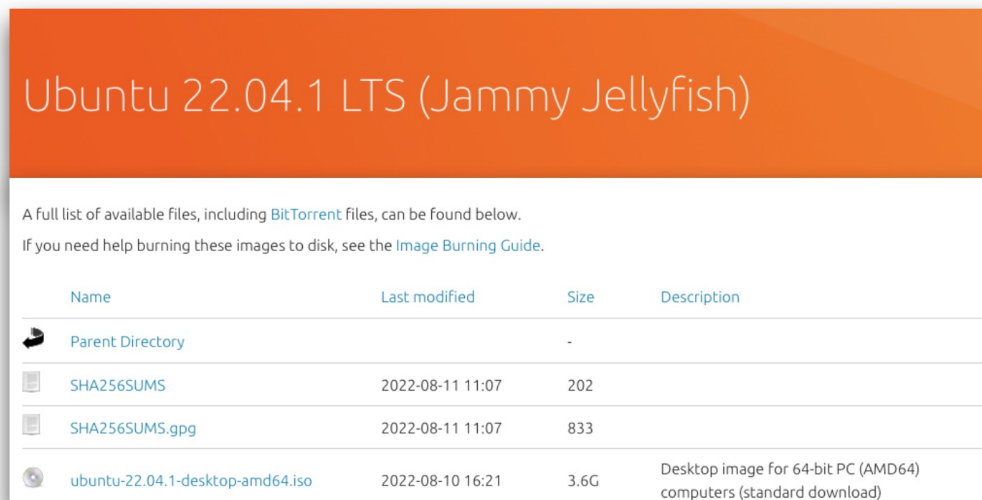
- Information has not been altered in an unauthorized way
- **Benign compromise**: information altered by accident
  - E.g., bit flips in memory due to cosmic ray
- **Malicious compromise**: information altered by attackers
  - E.g., malicious code that changes some files in a system









## 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



Ubuntu 22.04.1 LTS (Jammy Jellyfish)

A full list of available files, including [BitTorrent](#) files, can be found below.  
If you need help burning these images to disk, see the [Image Burning Guide](#).

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">SHA256SUMS</a>	2022-08-11 11:07	202	
 <a href="#">SHA256SUMS.gpg</a>	2022-08-11 11:07	833	
 <a href="#">ubuntu-22.04.1-desktop-amd64.iso</a>	2022-08-10 16:21	3.6G	Desktop image for 64-bit PC (AMD64) computers (standard download)

# 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?
- 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

**Kakao's meltdown raises big questions about its management**



“President office said  
KaKao’s network disturbance could even  
be **a threat to national security**”

# Other properties?

---



- **Confidentiality**
- **Integrity**
- **Availability**

# Other properties?

---



- **Confidentiality**
  - **Integrity**
  - **Availability**
- 
- + **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



- 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, ...)



The image shows the UNIST login page. At the top, it says 'UNIST | 로그인'. Below this are three tabs: '계정생성' (Account Creation), '아이디찾기' (Find ID), and '비밀번호 초기화' (Reset Password). The '아이디찾기' tab is selected. The main form has two input fields: 'ID' and 'PW'. To the right of the 'ID' field is a '로그인' (Login) button. Below the 'PW' field is a small icon of a password field. The background of the login page shows a scenic view of a forest.

The image shows the UNIST ID Confirmation page. At the top, it says 'UNIST' and 'joon@unist.ac.kr'. Below this is the title 'ID 확인'. There are two sections for confirmation: one for text message (+XX XXXXXXXXXX79에 문자 메시지) and one for phone call (+XX XXXXXXXXXX79에 전화). Below these is a section for '추가 정보' (Additional Information) with a link to 'https://aka.ms/mfasetup' for the latest confirmation method. At the bottom right is a '취소' (Cancel) button.

# Non-repudiation

---



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

# 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

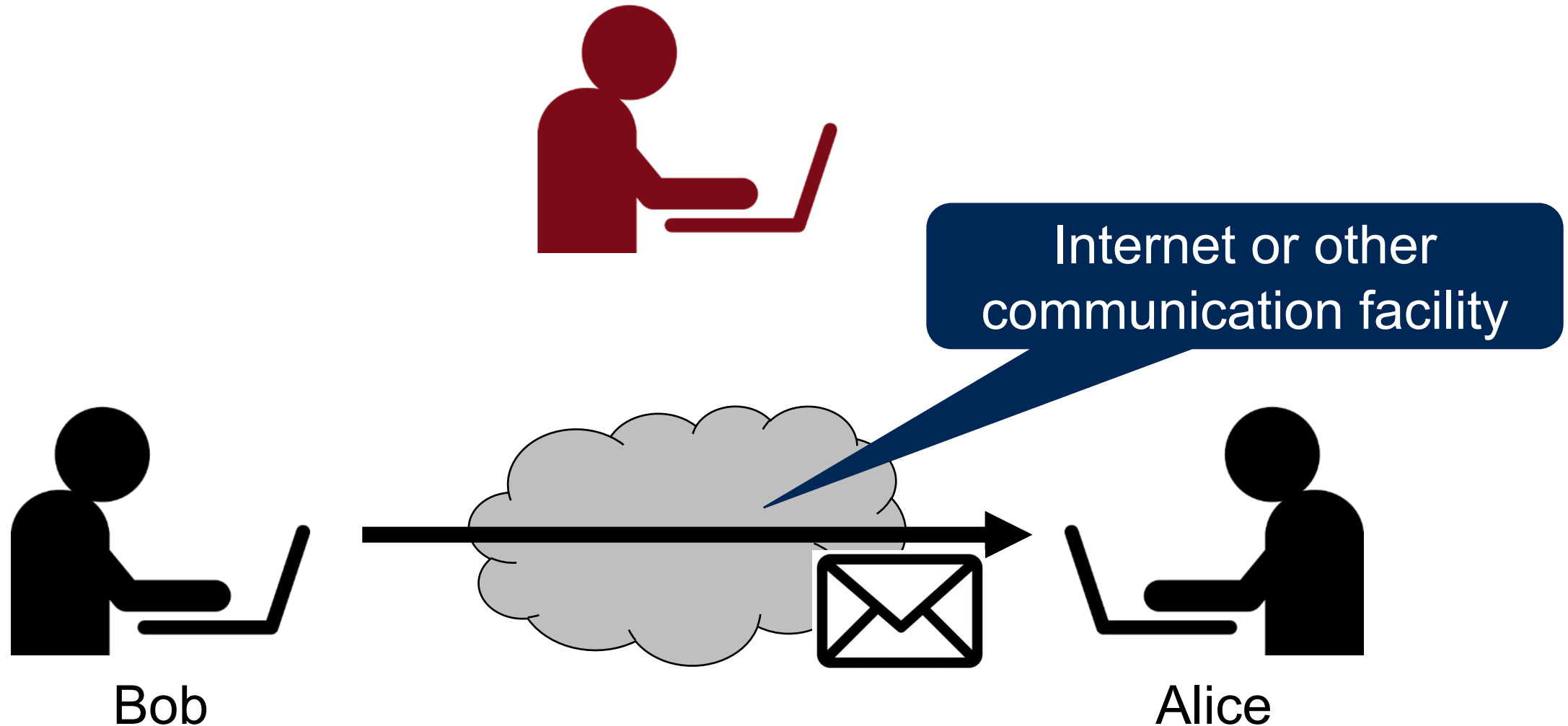
---



- Note terms
  - Threat: a potential for violation of security
  - Attack: an assault on system security, a deliberate attempt to evade 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

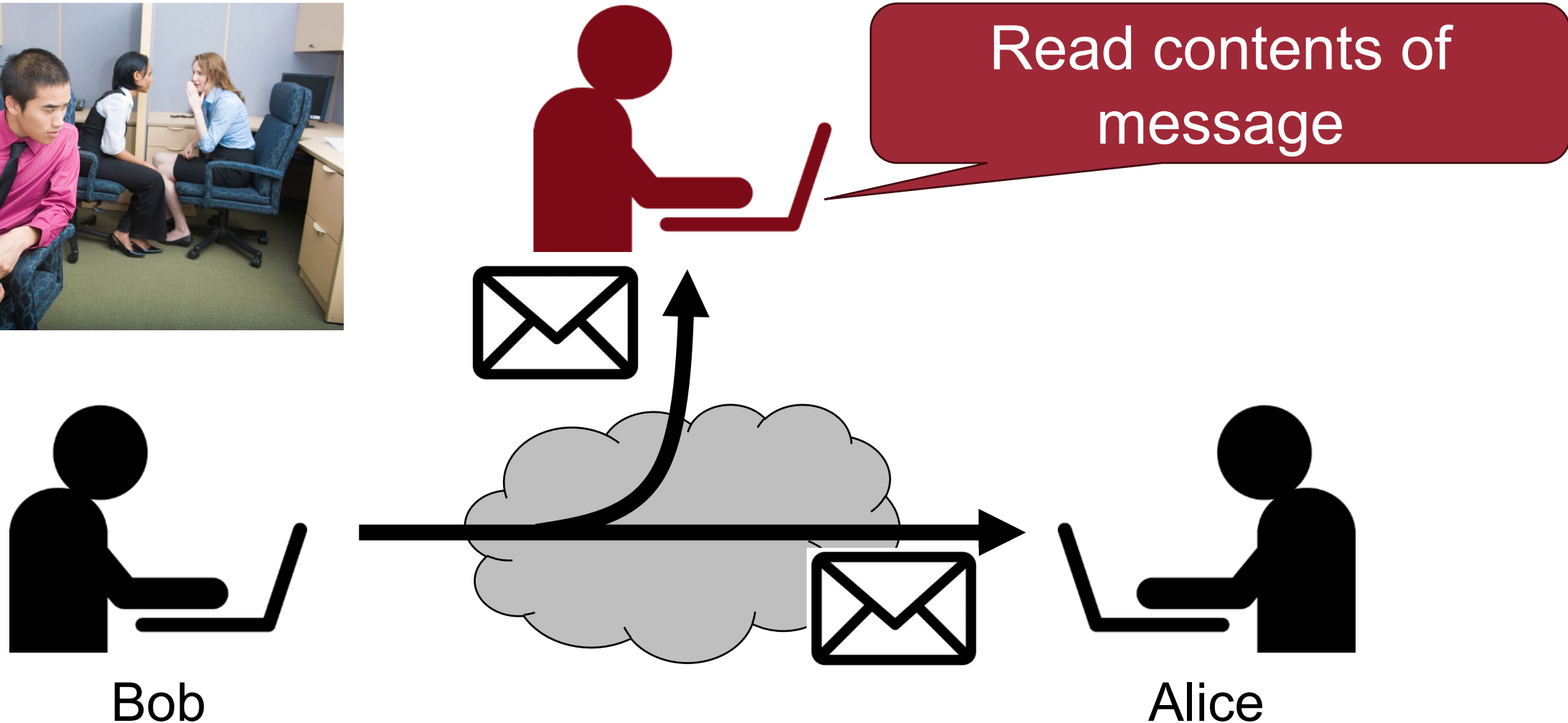
- Disclosure of message contents





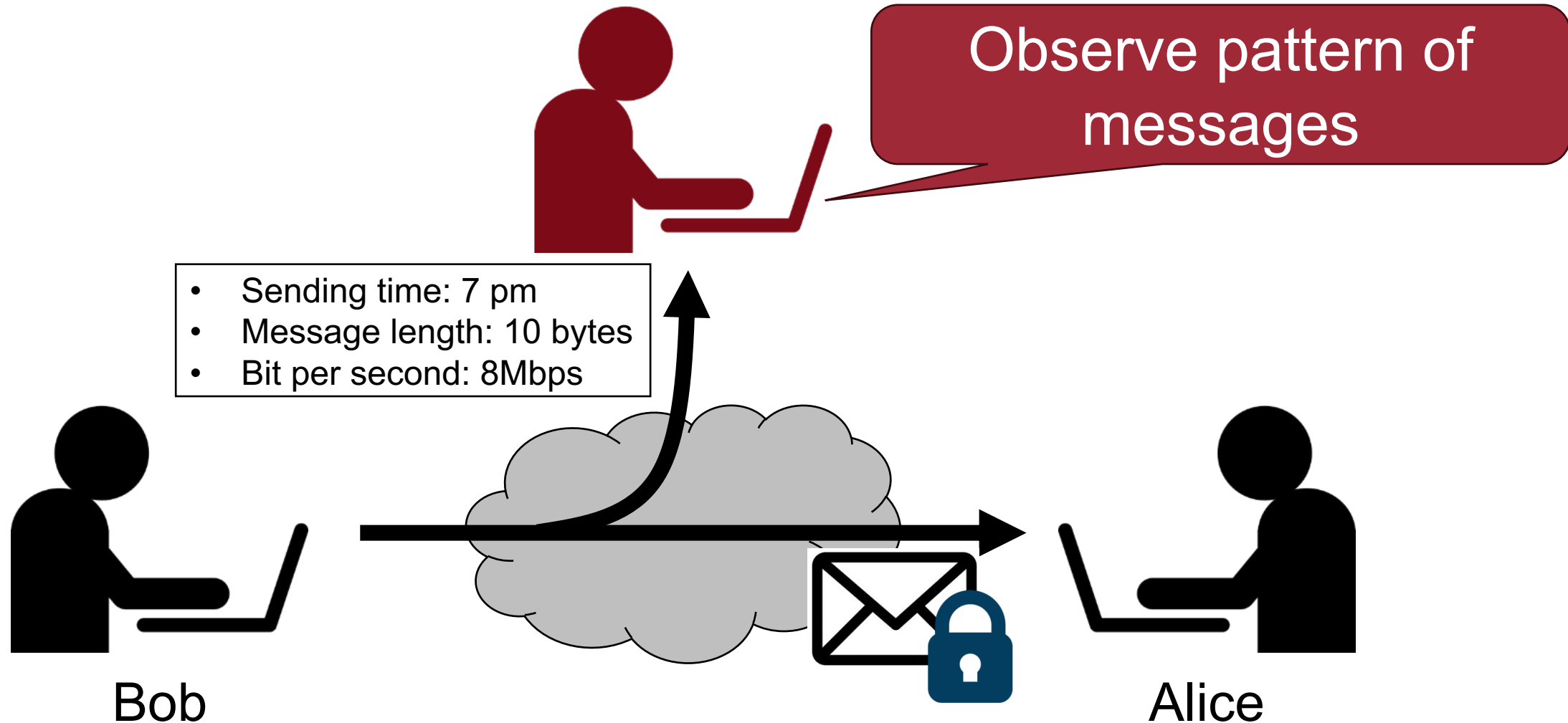
# Passive Attacks

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



# Passive Attacks

- Traffic analysis



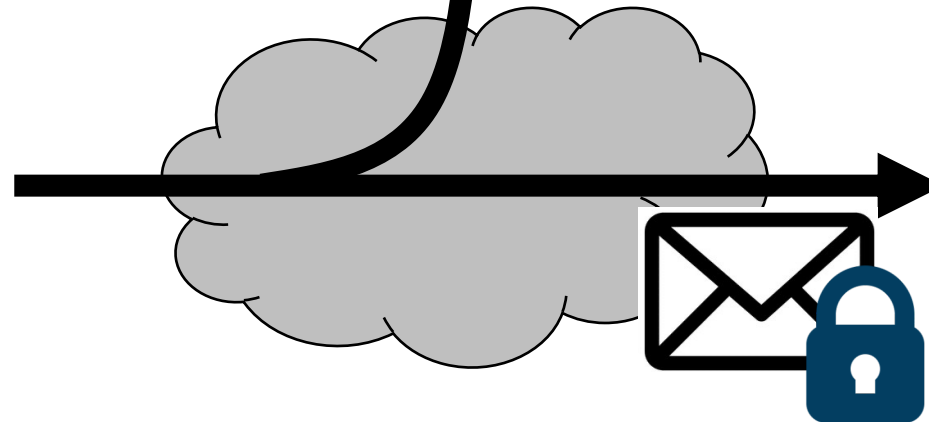
- Watching the Watchers: Practical Video Identification Attack in LTE Networks, *USENIX'22*
- Beauty and the Burst: Remote Identification of Encrypted Video Streams, *USENIX'17*

Observe pattern of messages

- Sending time: 7 pm
- Message length: 10 bytes
- Bit per second: 8Mbps



Bob



Alice

# 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

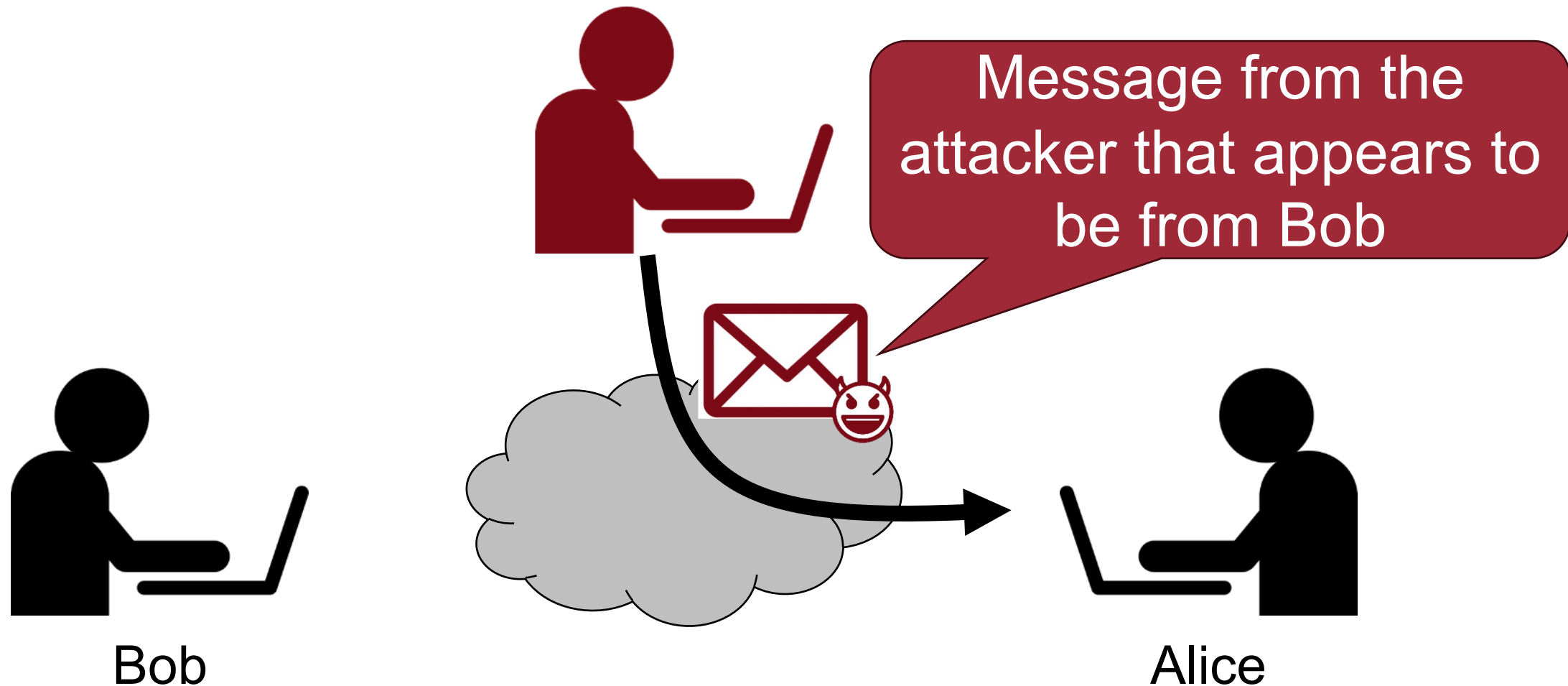
---



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

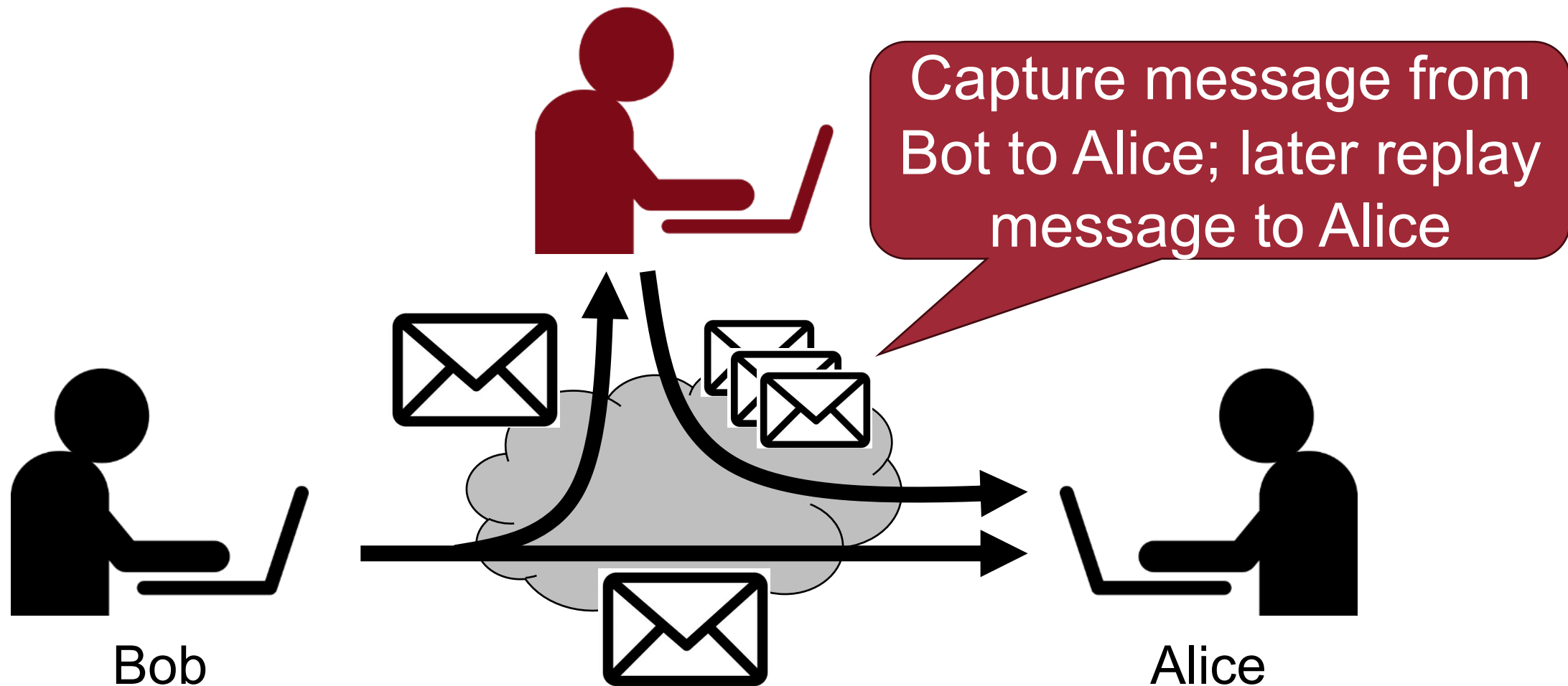
# Active Attacks

- Masquerade
  - One entity pretends to be a different entity



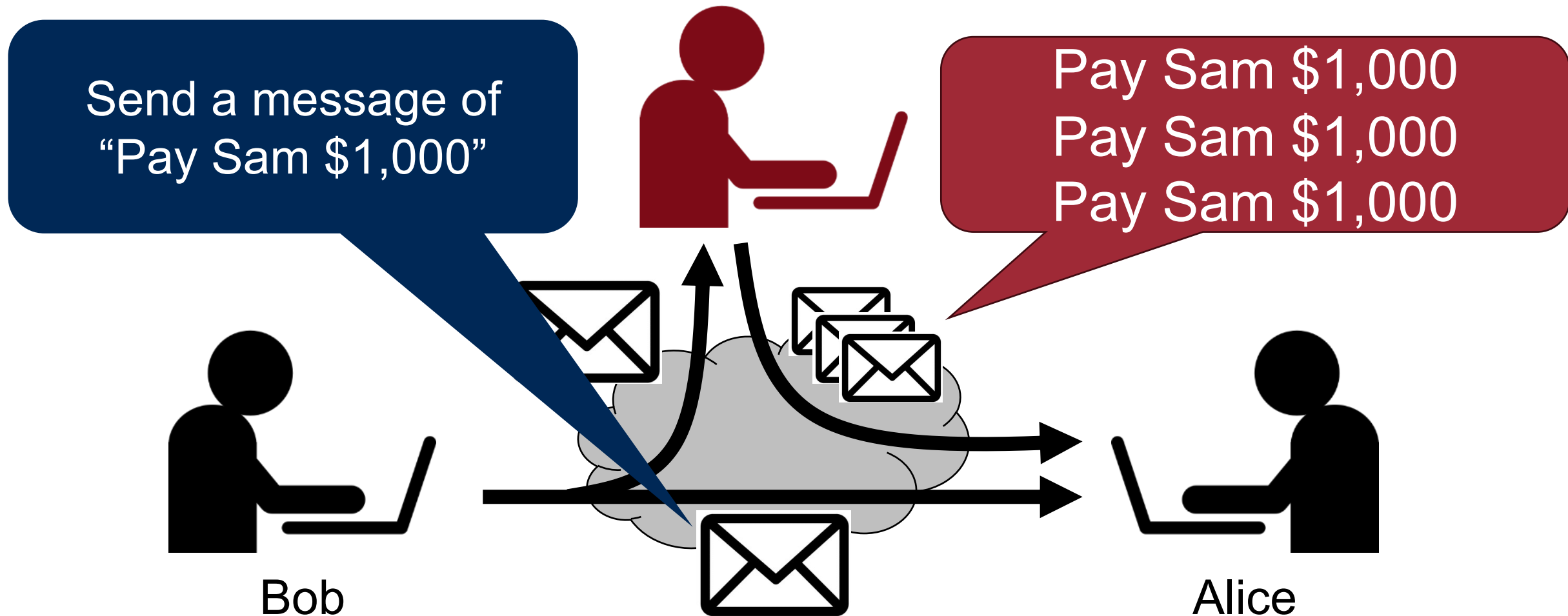
# Active Attacks

- Replay
  - A message is captured and retransmitted later



# Active Attacks

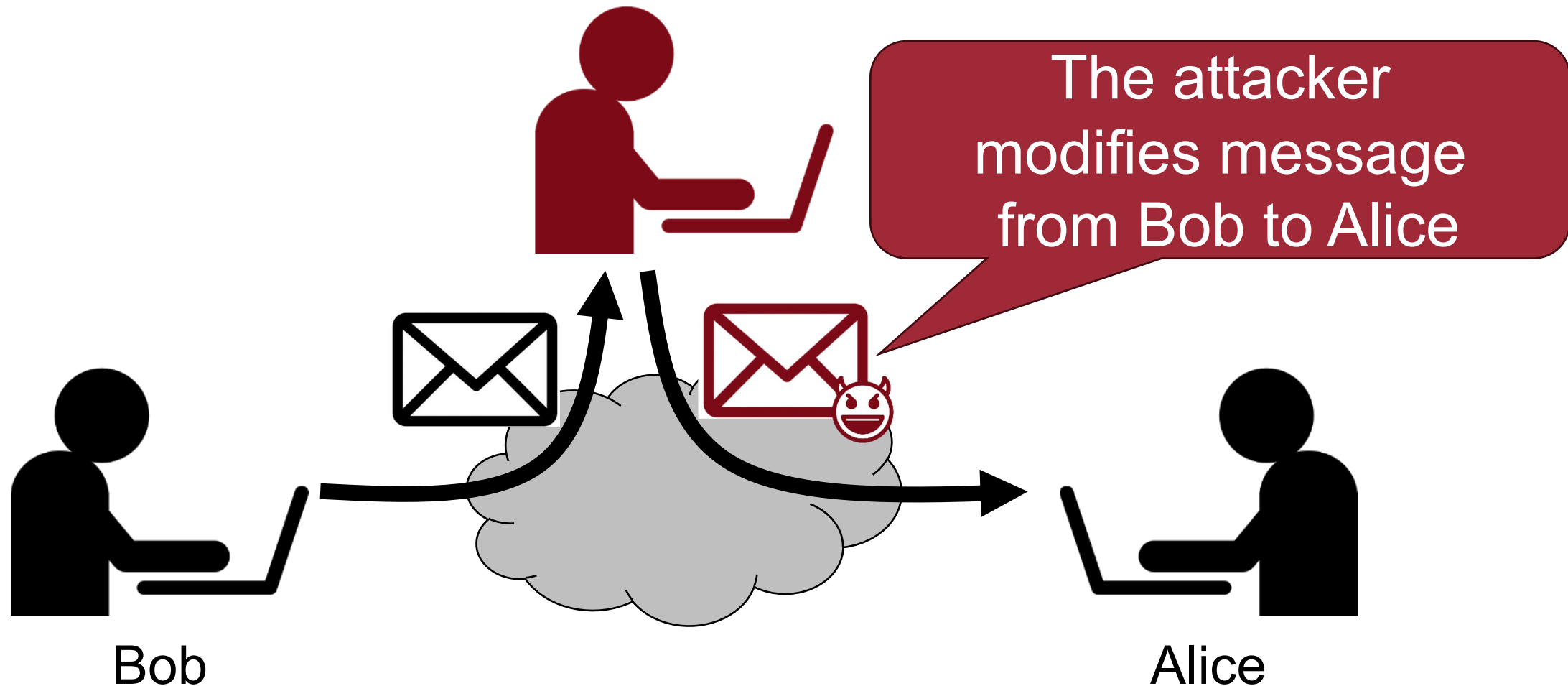
- Replay
  - A message is captured and retransmitted later





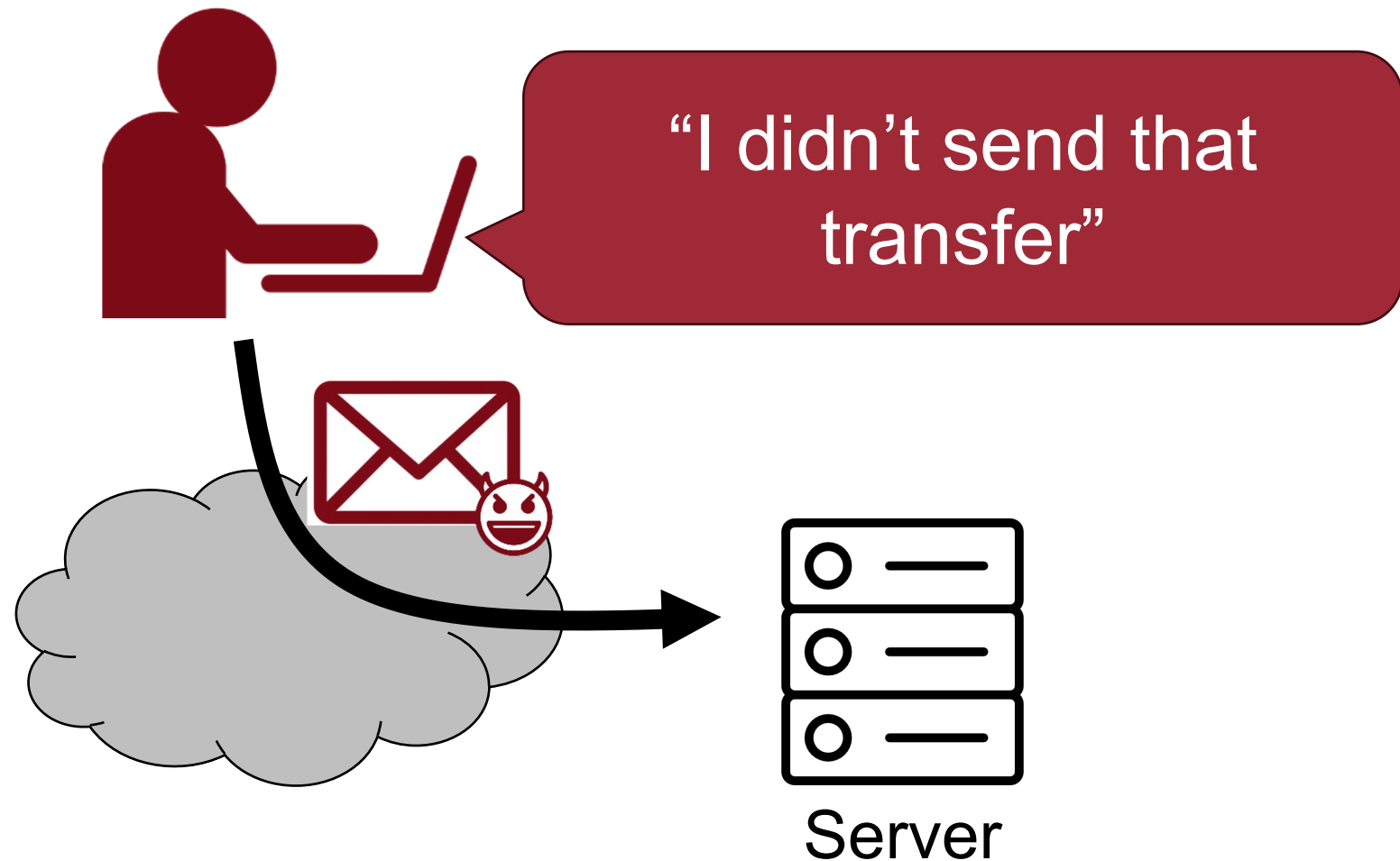
# Active Attacks

- 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)

# Cryptography – Overview

- Cryptography is about **confidentiality** and **integrity** (+ **authentication**, **non-repudiation**)



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



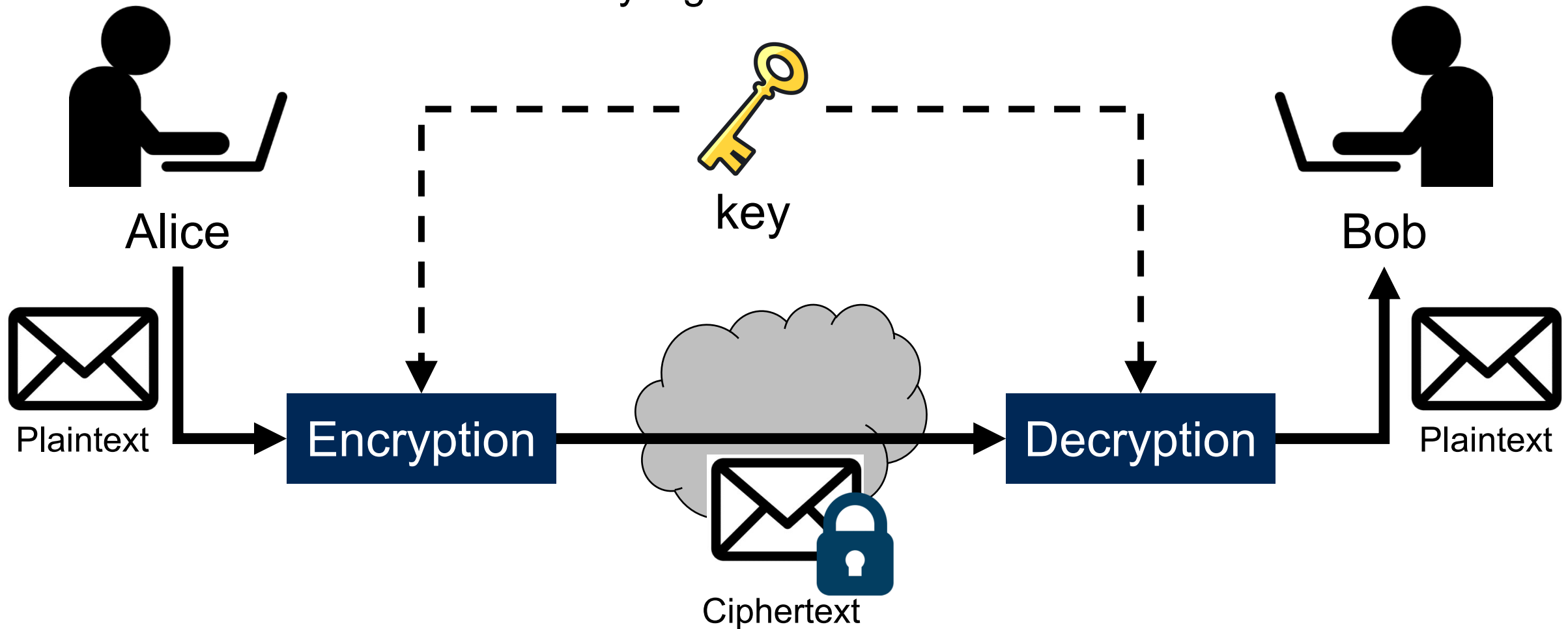
Bob

***Shared*** secret key



# Symmetric Key Cryptography

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



# Symmetric Key Cryptography

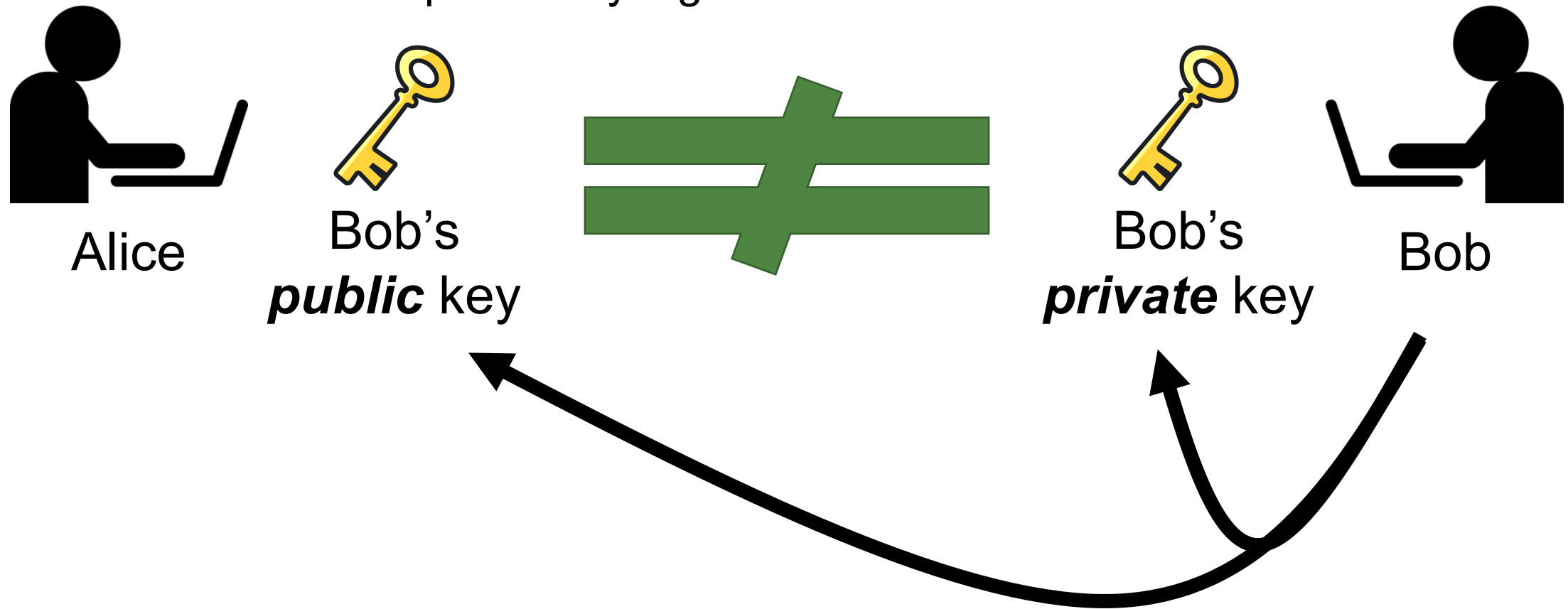
---



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

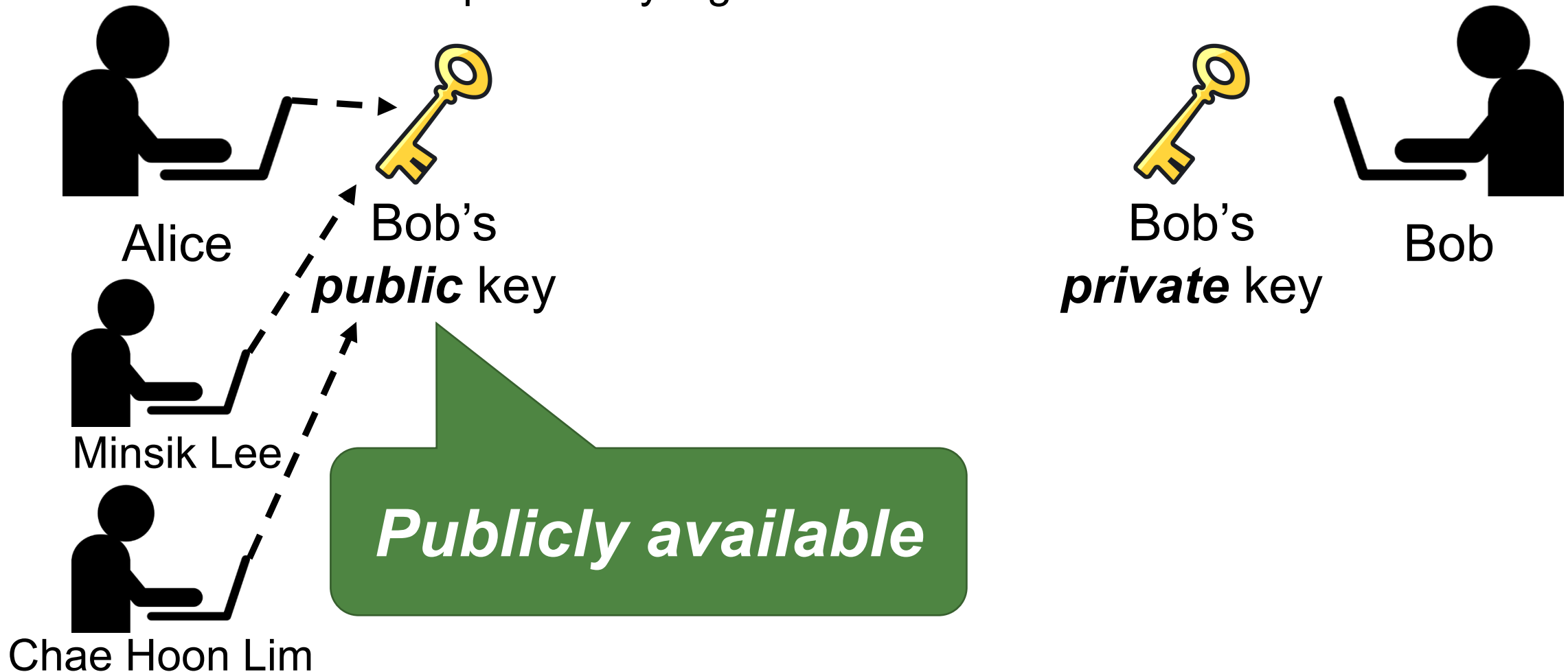
# Asymmetric Key Cryptography

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



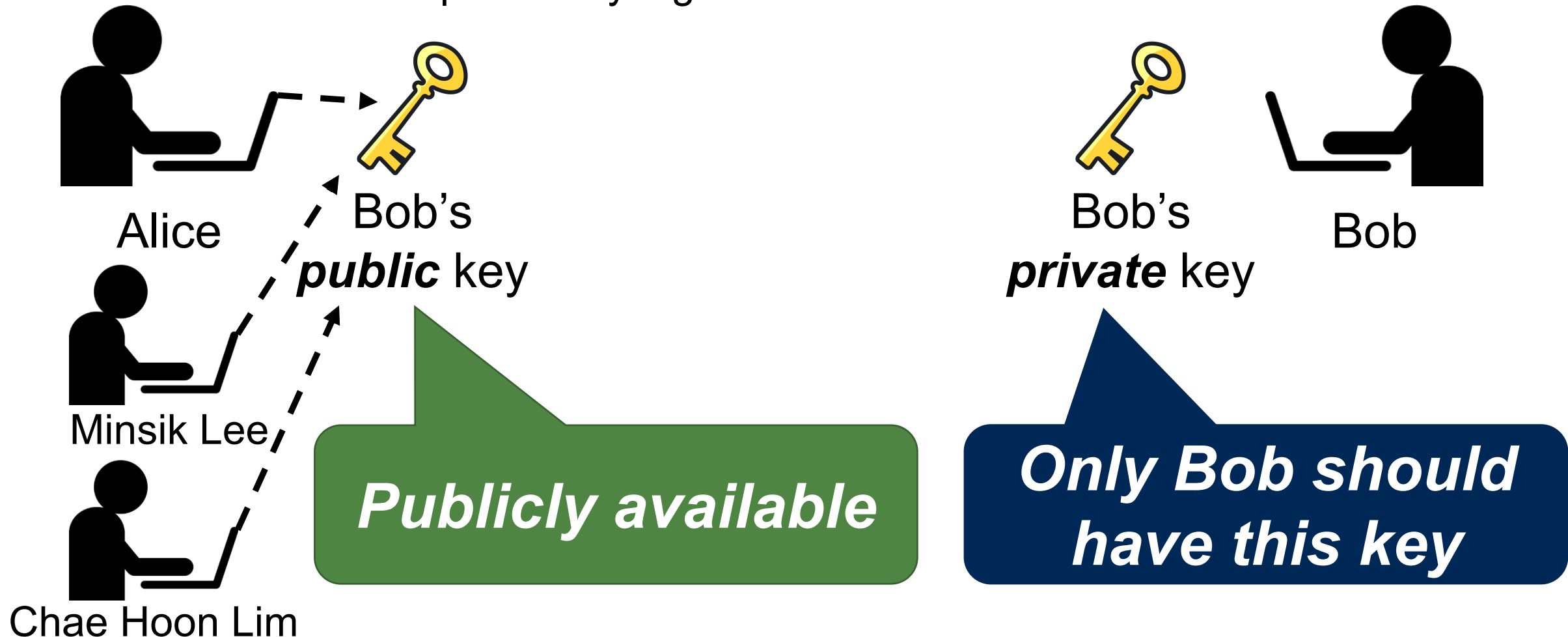
# Asymmetric Key Cryptography

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



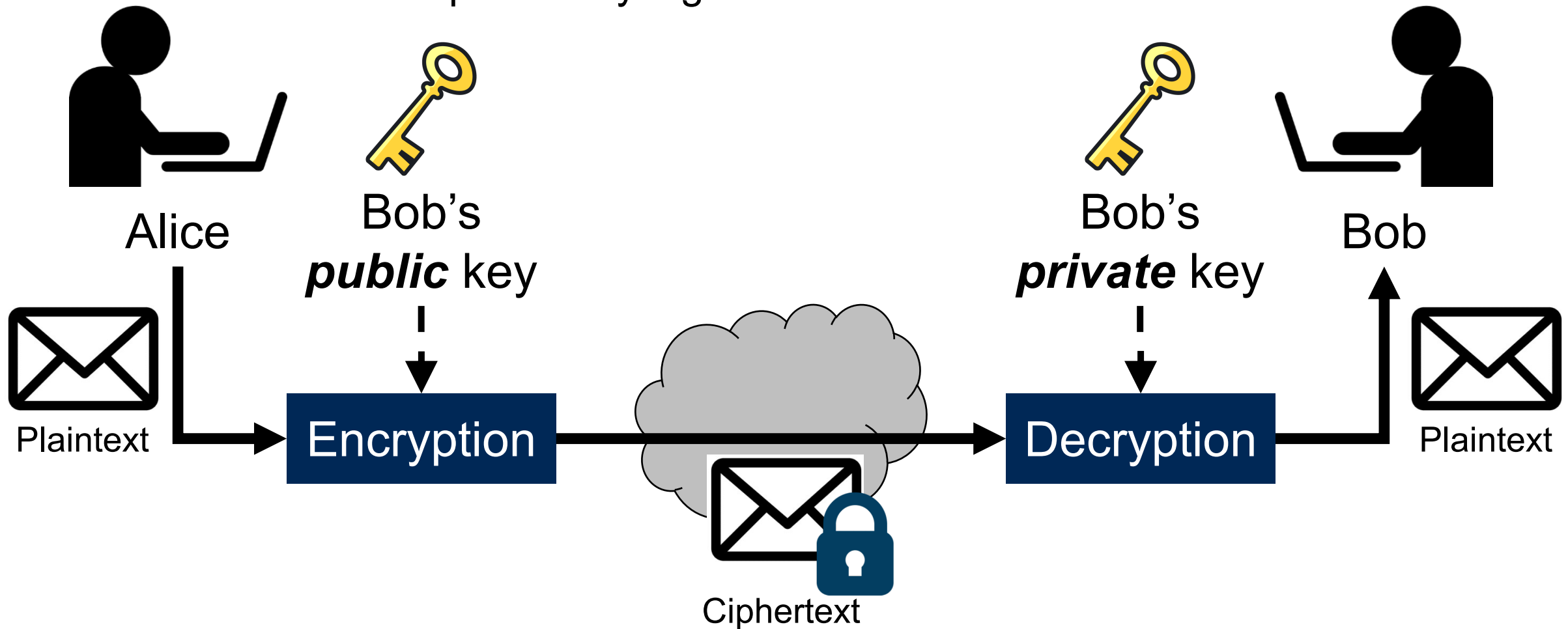
# Asymmetric Key Cryptography

- 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

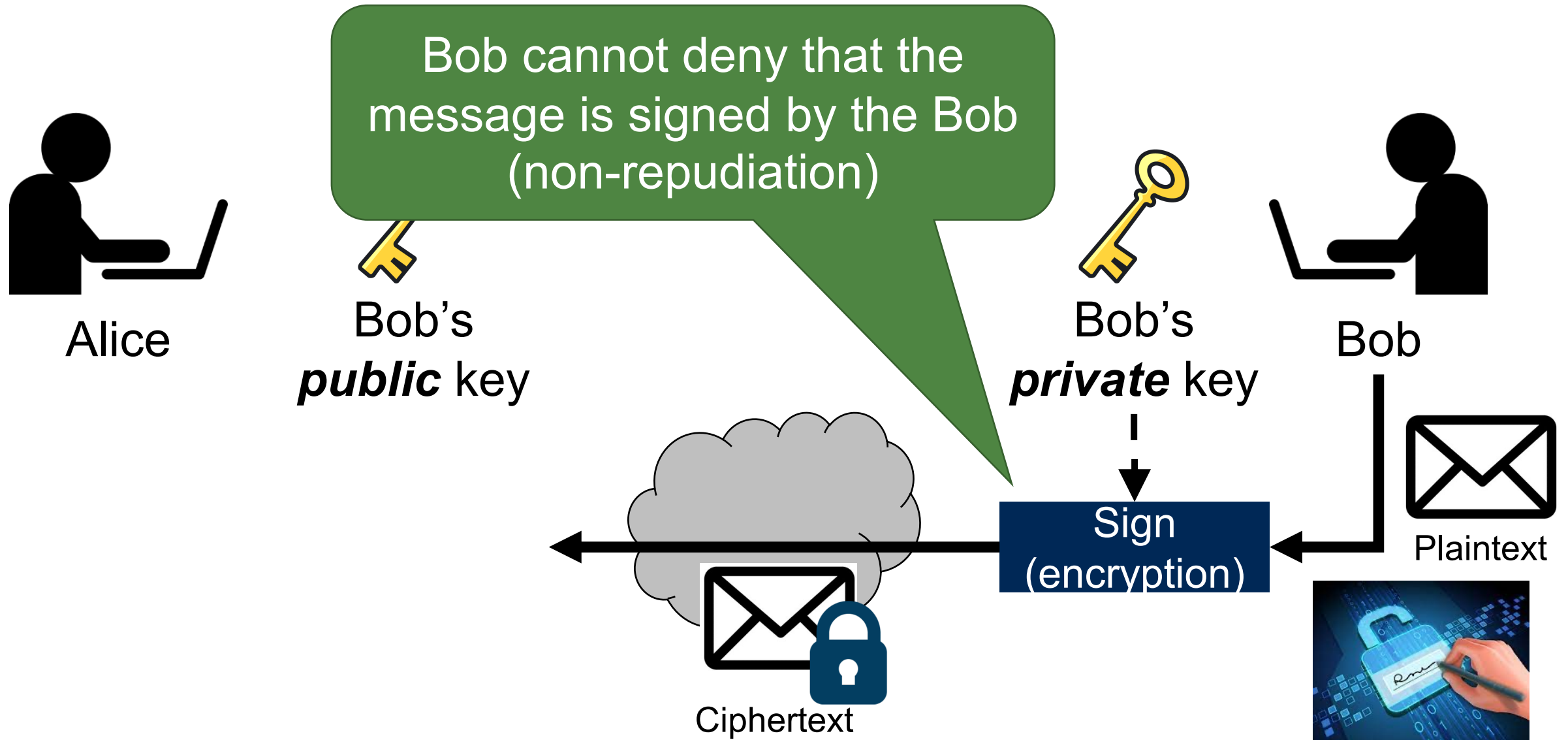


# Asymmetric Key Cryptography

---

- Pros?
- Cons?

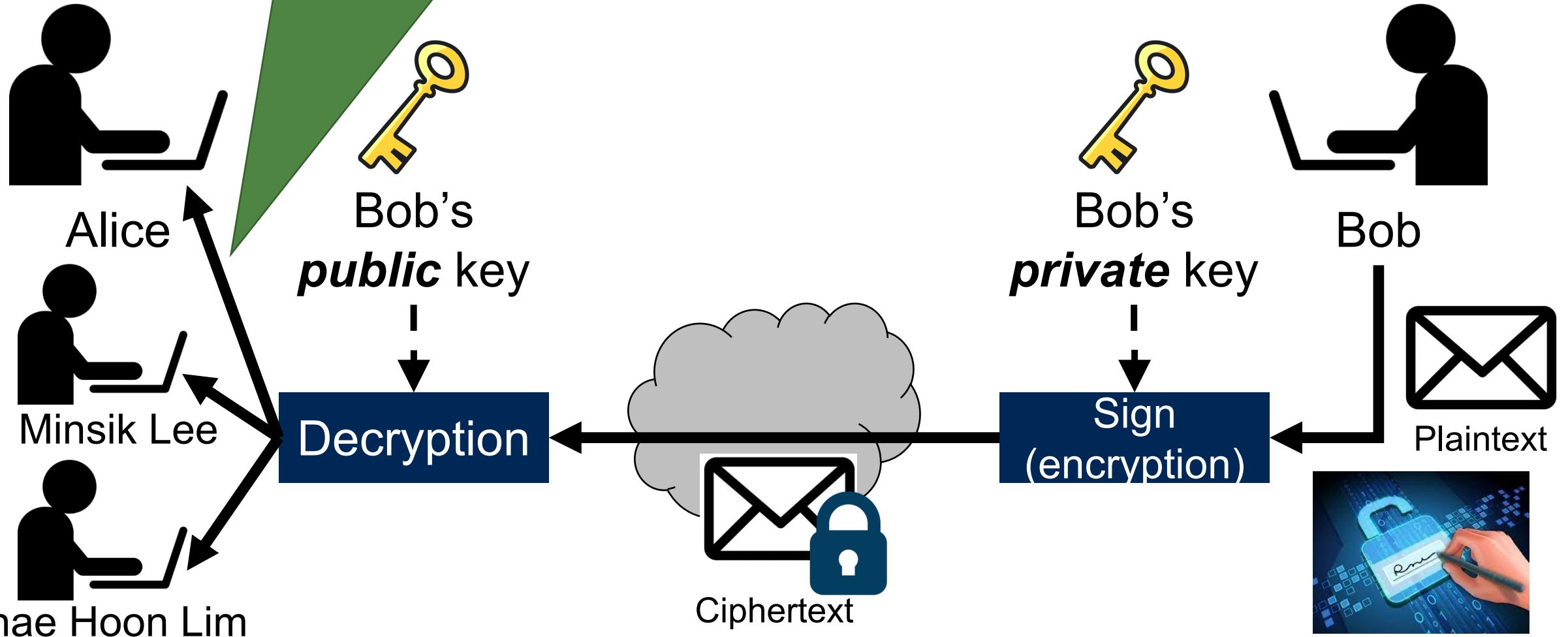
# Digital Signature





# Digital Signature

This message is from Bob  
(authentication)



# 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 how to use basic cryptographic primitives (next lecture)

# Question?