CSE551: Advanced Computer Security

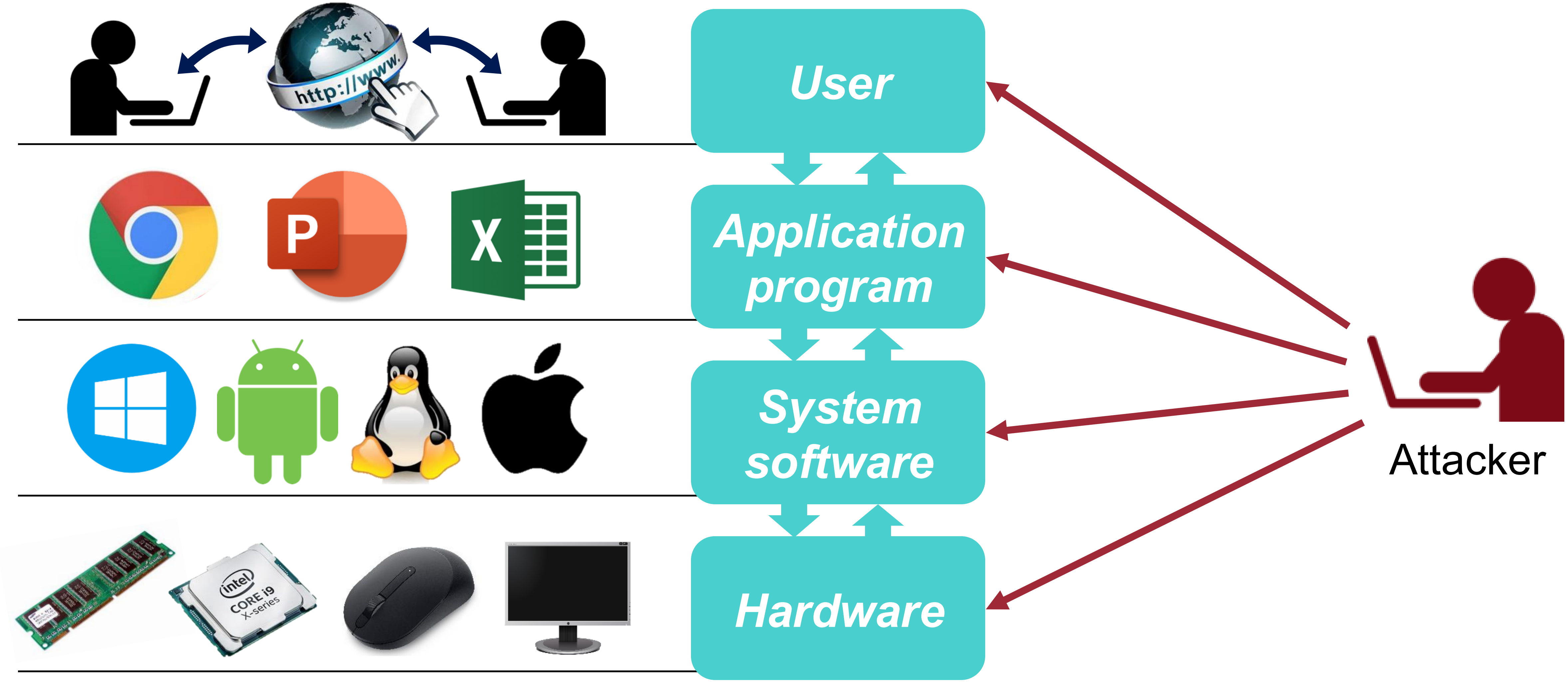
2. Concepts in Security

Seongil Wi

Department of Computer Science and Engineering

Recap: Computer Security

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



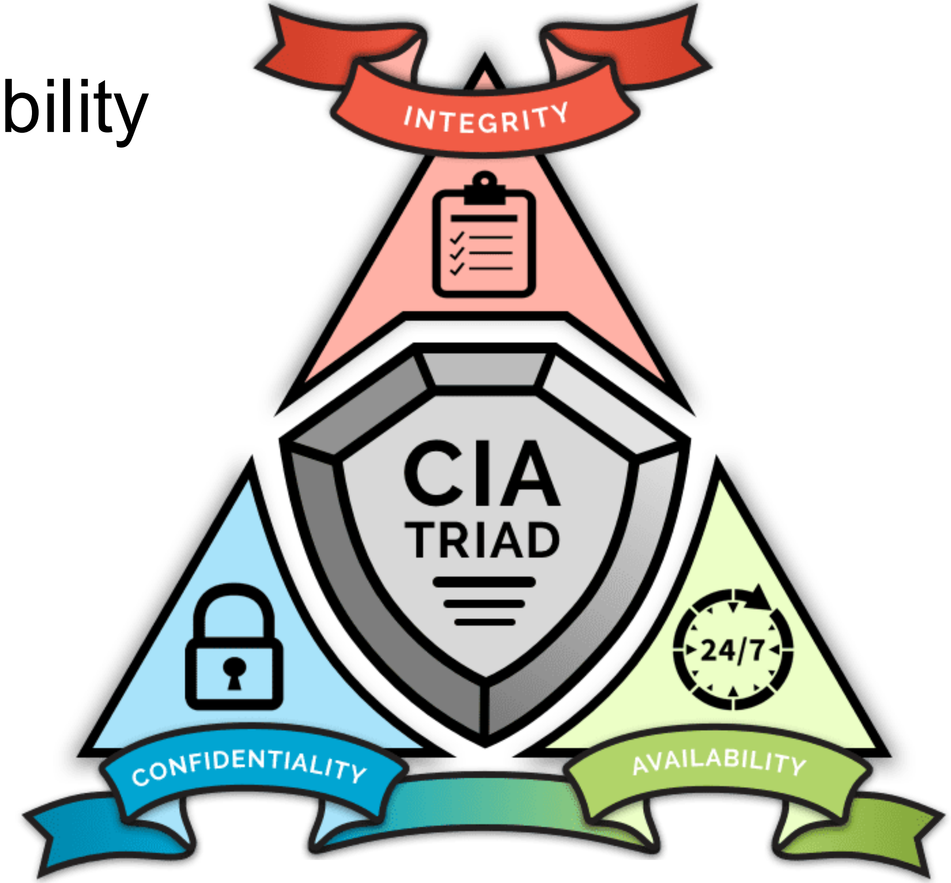
Security Properties (Basic Concepts)

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

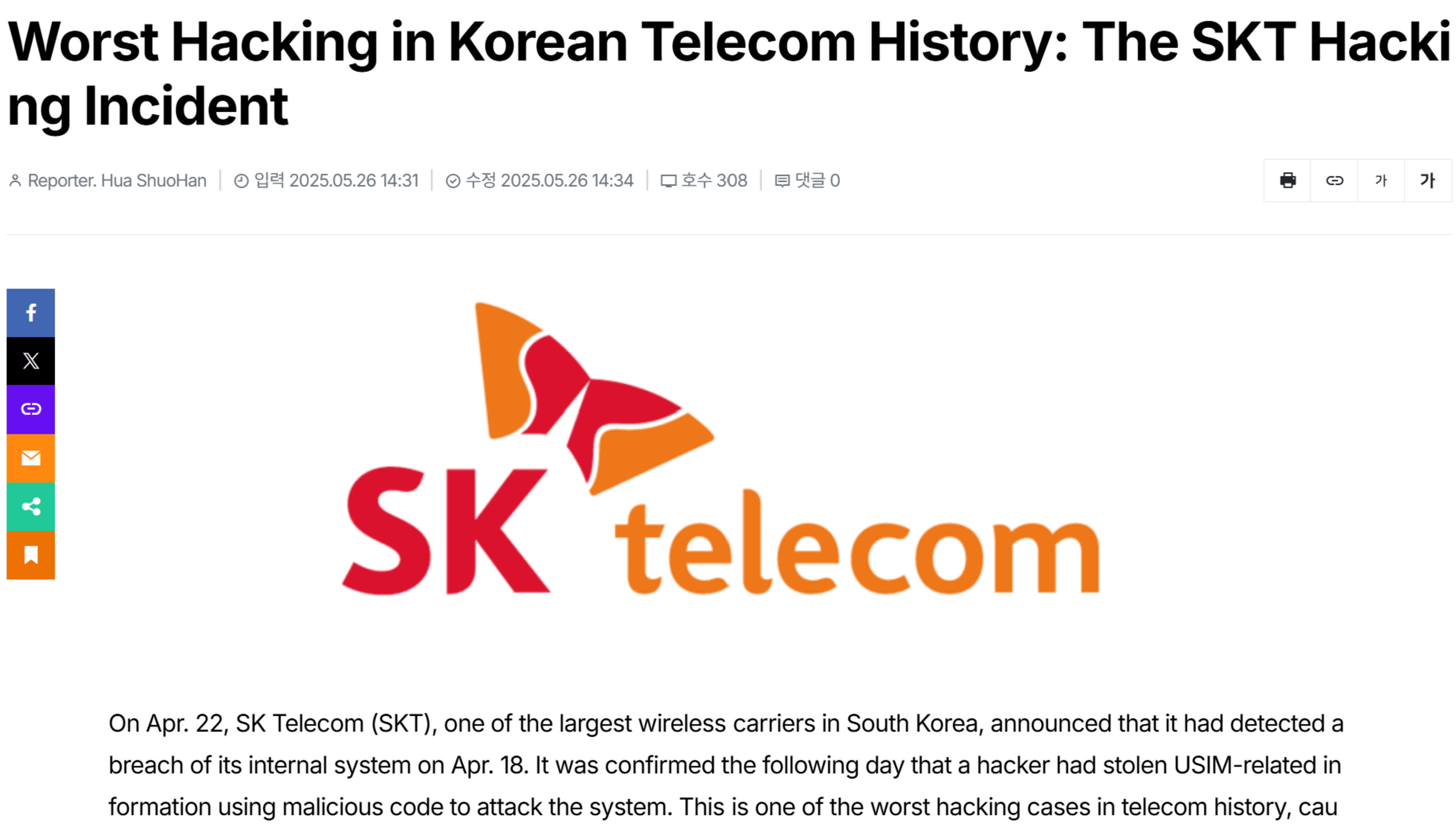
- **I**ntegrity

- **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

CIA (1): Confidentiality – Compromise



Worst Hacking in Korean Telecom History: The SKT Hacking Incident

Reporter. Hua ShuoHan | 입력 2025.05.26 14:31 | 수정 2025.05.26 14:34 | 호수 308 | 댓글 0

On Apr. 22, SK Telecom (SKT), one of the largest wireless carriers in South Korea, announced that it had detected a breach of its internal system on Apr. 18. It was confirmed the following day that a hacker had stolen USIM-related information using malicious code to attack the system. This is one of the worst hacking cases in telecom history, cau

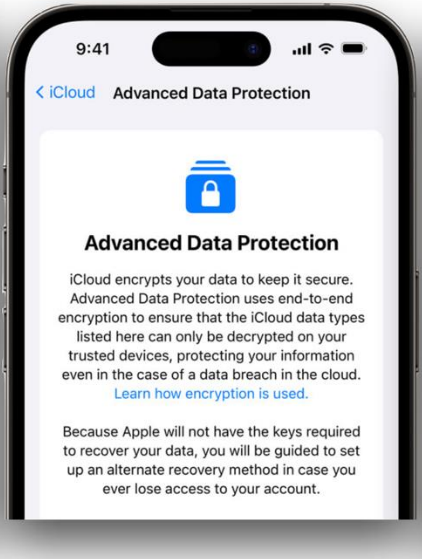
CIA (1): Confidentiality

- 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:

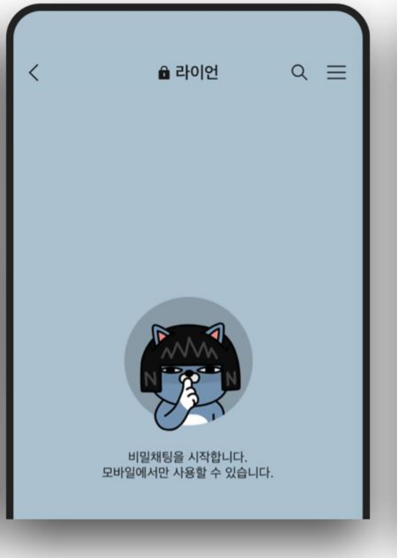

9:41

< iCloud Advanced Data Protection

Advanced Data Protection

iCloud encrypts your data to keep it secure. Advanced Data Protection uses end-to-end encryption to ensure that the iCloud data types listed here can only be decrypted on your trusted devices, protecting your information even in the case of a data breach in the cloud. Learn how encryption is used.

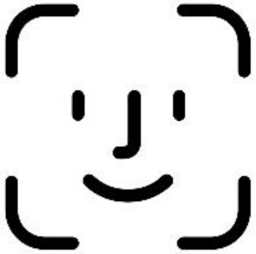
Because Apple will not have the keys required to recover your data, you will be guided to set up an alternate recovery method in case you ever lose access to your account.

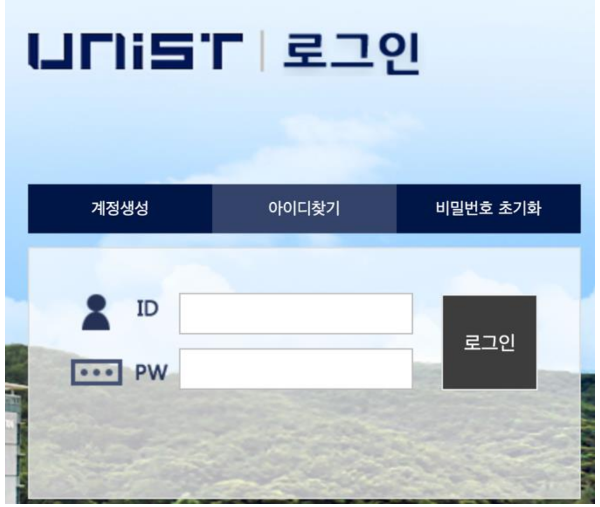

라이언

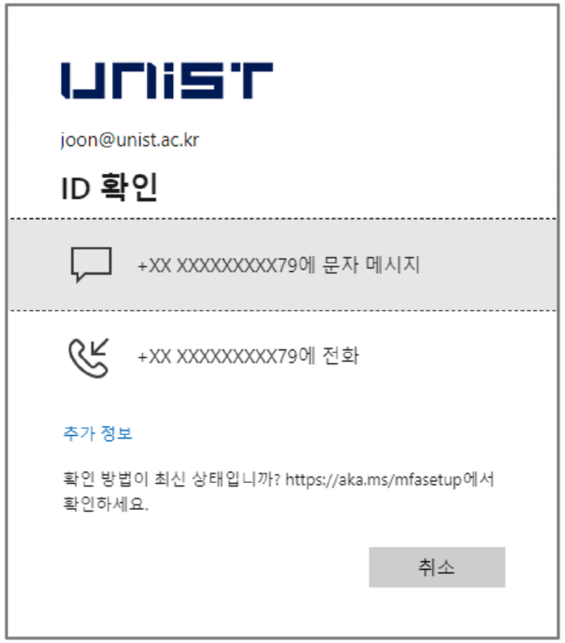
비밀채팅을 시작합니다.
모바일에서만 사용할 수 있습니다.

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, …)







UNIST

joon@unist.ac.kr

ID 확인

+XX XXXXXXXXX79에 문자 메시지

+XX XXXXXXXXX79에 전화

추가 정보

확인 방법이 최신 상태입니까? https://aka.ms/mfasetup에서 확인하세요.

취소

CIA (1): Confidentiality – Access Control

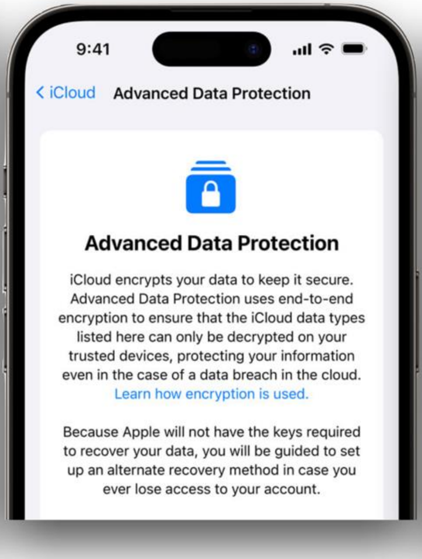
- ***Rules*** and ***policies*** that limit access to confidential information
- Determine what users have permission to do
- Permission is determined by identity (e.g., name, serial) or role (e.g., professor, TA, student)
- Example: Linux file system

	/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 – Encryption

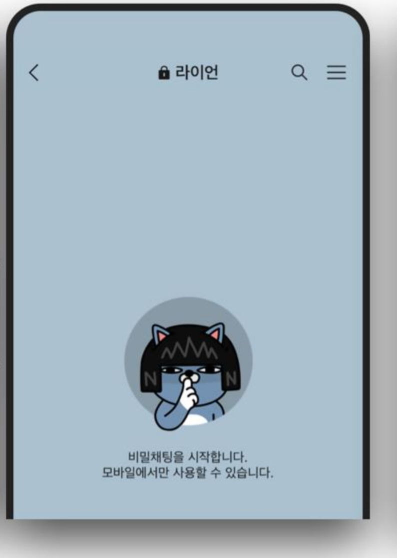
- Transformation of information using an encryption key
- Only be read by another user who has the decryption key
- Schemes: symmetric-key encryption, public-key encryption, etc
- Example:



Advanced Data Protection

iCloud encrypts your data to keep it secure. Advanced Data Protection uses end-to-end encryption to ensure that the iCloud data types listed here can only be decrypted on your trusted devices, protecting your information even in the case of a data breach in the cloud. Learn how encryption is used.

Because Apple will not have the keys required to recover your data, you will be guided to set up an alternate recovery method in case you ever lose access to your account.

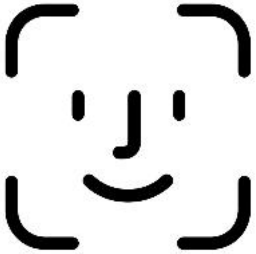


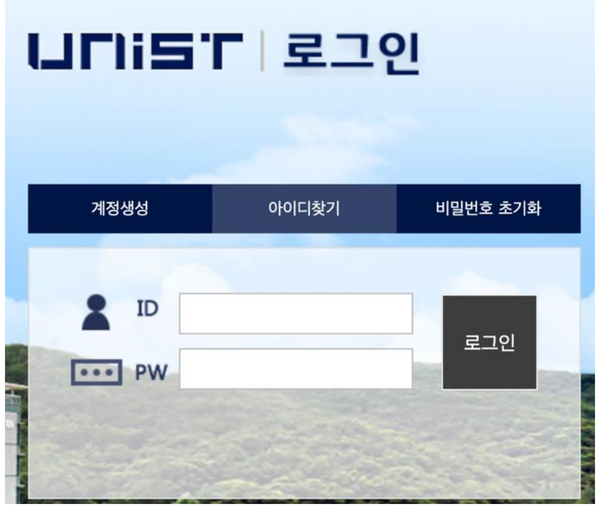
비밀채팅을 시작합니다.
모바일에서만 사용할 수 있습니다.

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

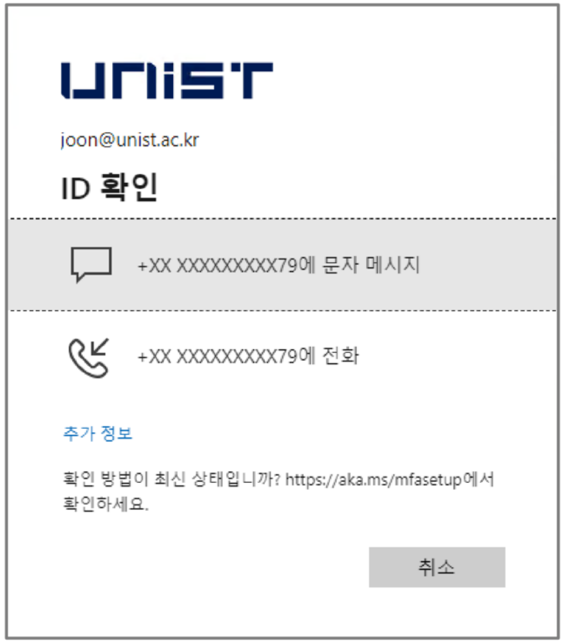
CIA (1): Confidentiality – Authentication

- 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, …)





UNIST | 로그인



UNIST

joon@unist.ac.kr

ID 확인

+XX XXXXXXXXXX79에 문자 메시지

+XX XXXXXXXXXX79에 전화

추가 정보

확인 방법이 최신 상태입니까? https://aka.ms/mfasetup에서 확인하세요.

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

Exercise: Internet Banking

- What mechanism is used to achieve confidentiality?

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

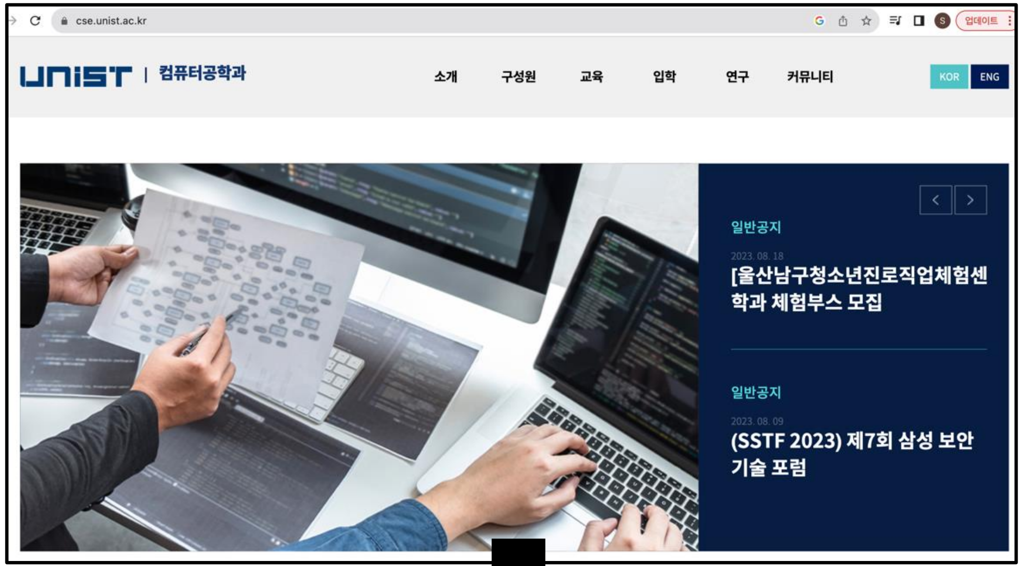
CIA (2): Integrity

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


cse.unist.ac.kr

UNIST | 컴퓨터공학과

일반공지

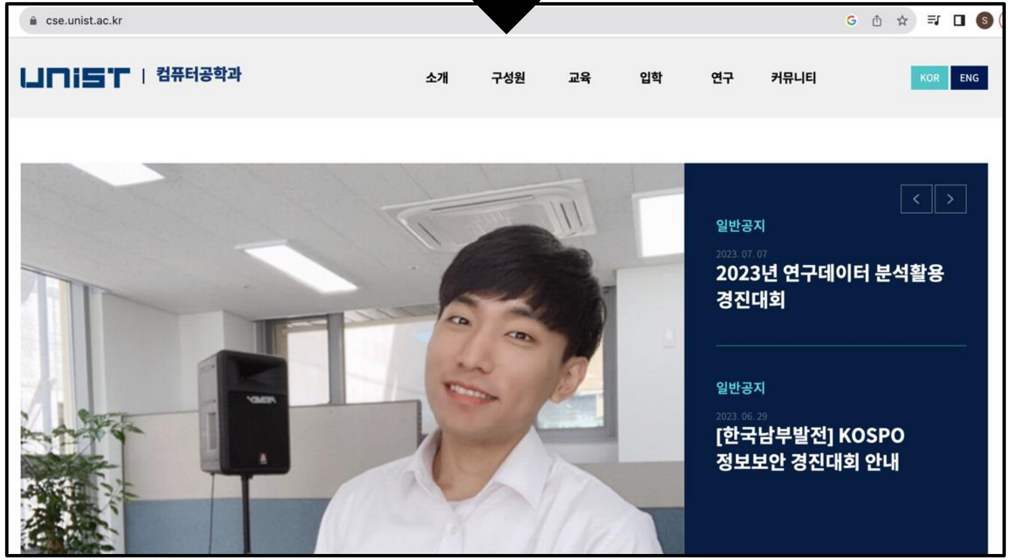
2023. 08. 18

[울산남구청소년진로직업체험센 학과 체험부스 모집

일반공지

2023. 08. 09

(SSTF 2023) 제7회 삼성 보안 기술 포럼


cse.unist.ac.kr

UNIST | 컴퓨터공학과

일반공지

2023. 07. 07

2023년 연구데이터 분석활용 경진대회

일반공지

2023. 06. 29

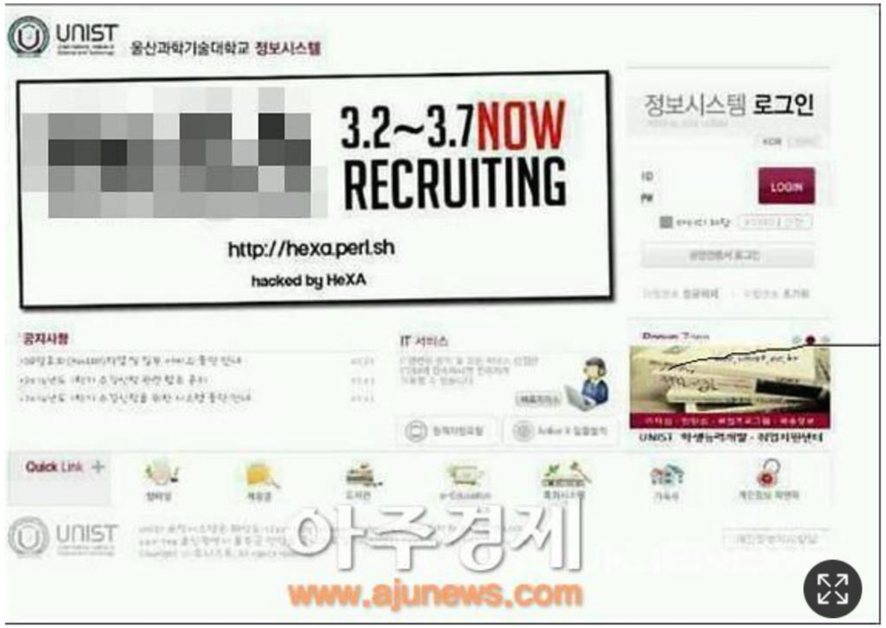
[한국남부발전] KOSPO 정보보안 경진대회 안내

수면위로 떠오른 UNIST(유니스트) '해킹 사건'

입력 2017-04-29 09:28

'룸메이트 바꾸려고' 전산망 뚫어…2013년부터 총 4건

유니스트 보안 정보 둔감 '지적'

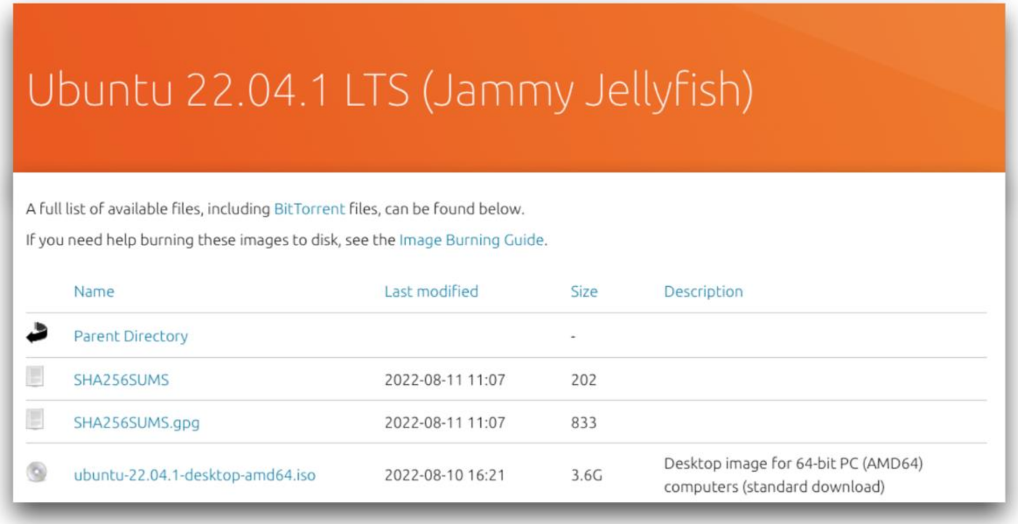


지난 2014년 3월 유니스트 해킹동아리가 학교전산망에 침입, 자신들의 해커 모집광고를 종합전산망 홈피에 게재해 놓은 배너 모습.

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



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
Parent Directory		-	
SHA256SUMS	2022-08-11 11:07	202	
SHA256SUMS.gpg	2022-08-11 11:07	833	
ubuntu-22.04.1-desktop-amd64.iso	2022-08-10 16:21	3.6G	Desktop image for 64-bit PC (AMD64) computers (standard download)

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

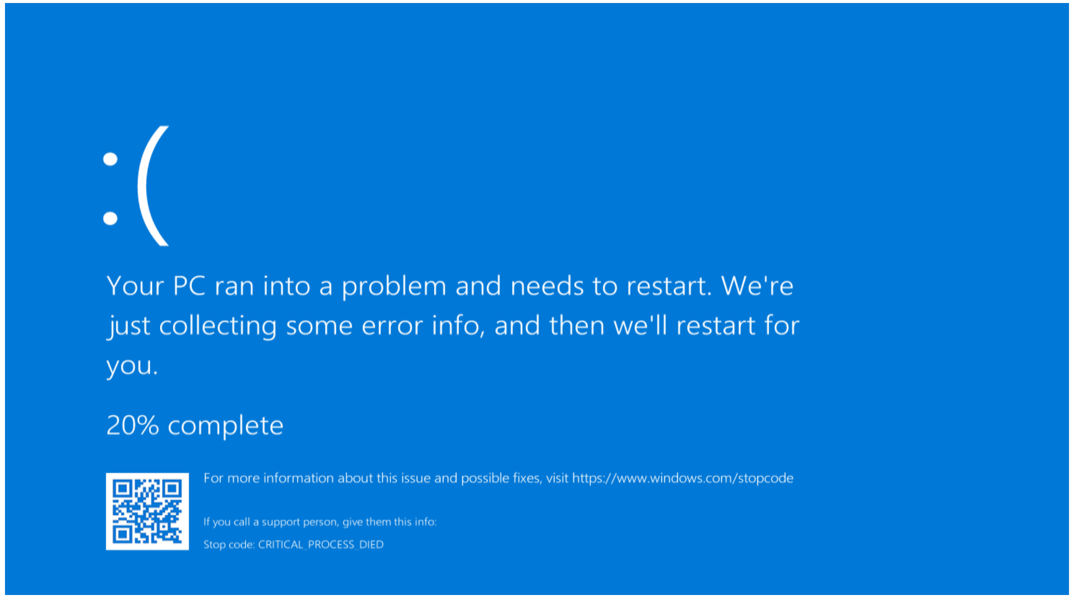
- **A**vailability: information is readily available when it is needed

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?



:(

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

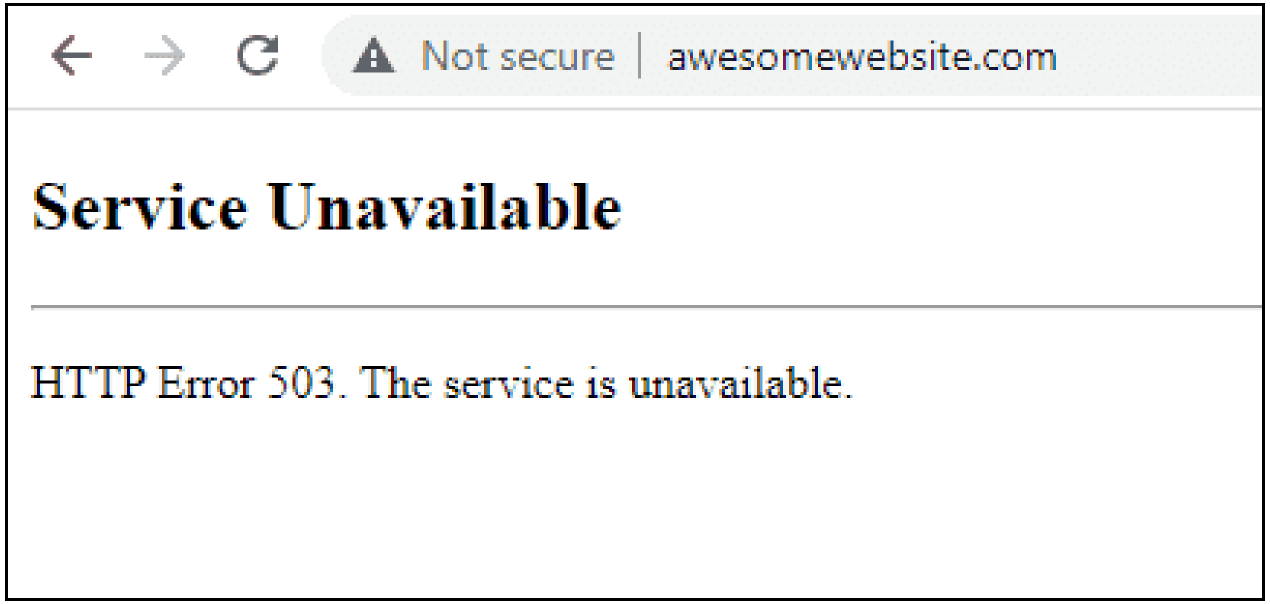
20% complete

For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

If you call a support person, give them this info:

Stop code: CRITICAL_PROCESS_DIED

Blue Screen of Death



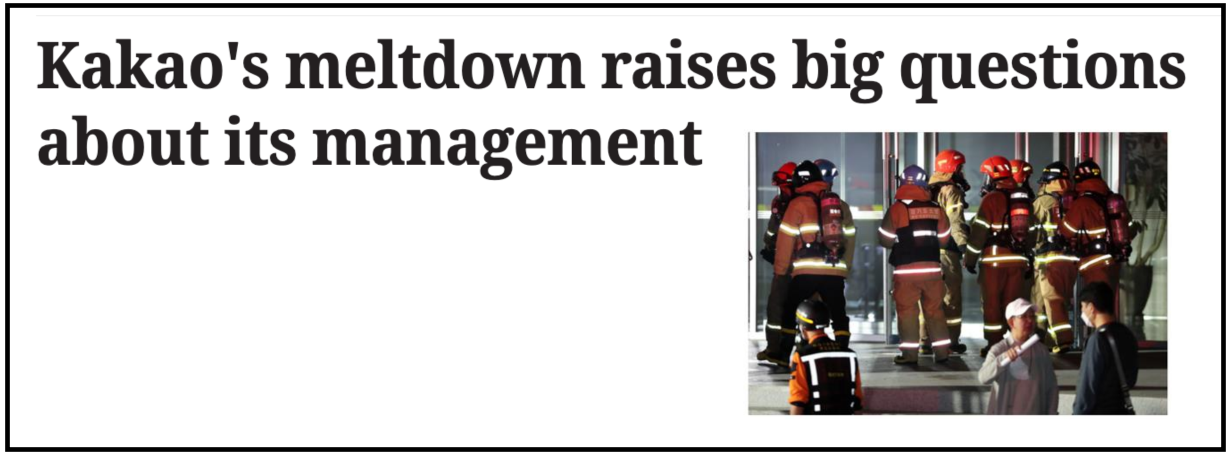
Service Unavailable

HTTP Error 503. The service is unavailable.

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?

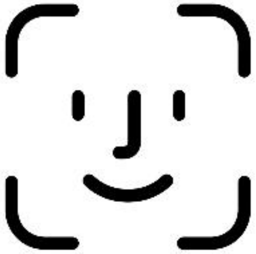
- **C**onfidentiality
- **I**ntegrity
- **A**vailability

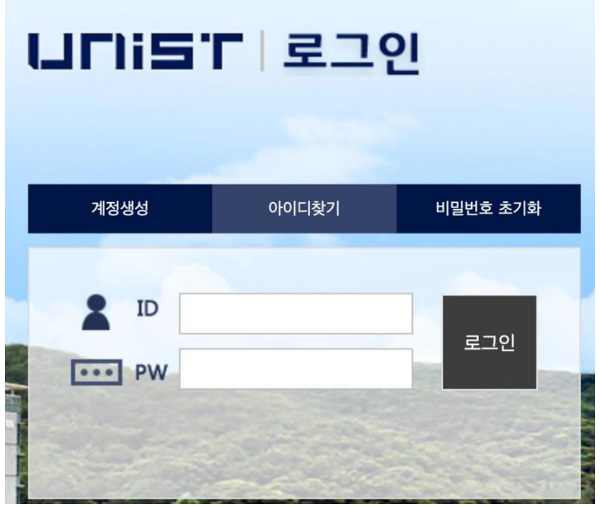
+ **Authentication**: the ability of a computer system to *confirm the sender's identity*

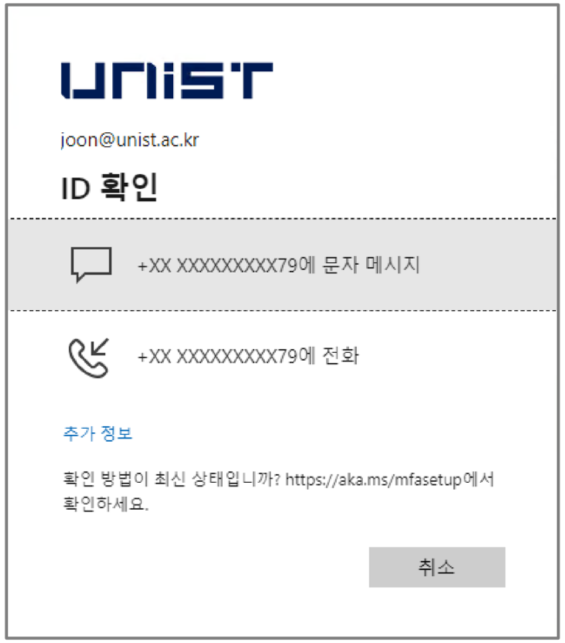
+ **Non-repudiation**: the ability of a computer system to *confirm that the sender can not deny about something sent*

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, …)







joon@unist.ac.kr

ID 확인

+XX XXXXXXXXX79에 문자 메시지

+XX XXXXXXXXX79에 전화

추가 정보

확인 방법이 최신 상태입니까? https://aka.ms/mfasetup에서 확인하세요.

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)”

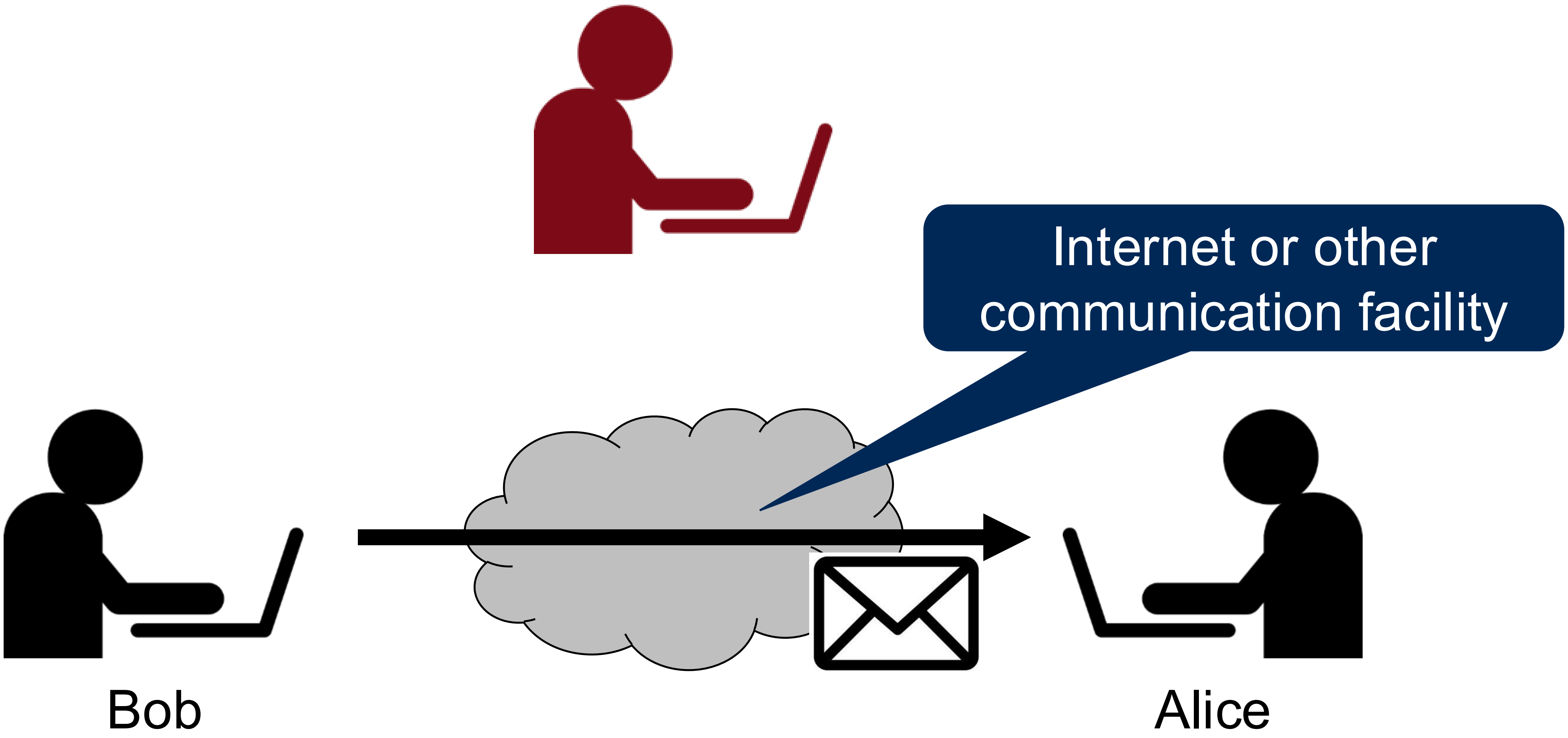
- **Non-repudiation** by secure authentication: authentic statement cannot be denied
  - E.g., digital signature

Aspects of Security

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

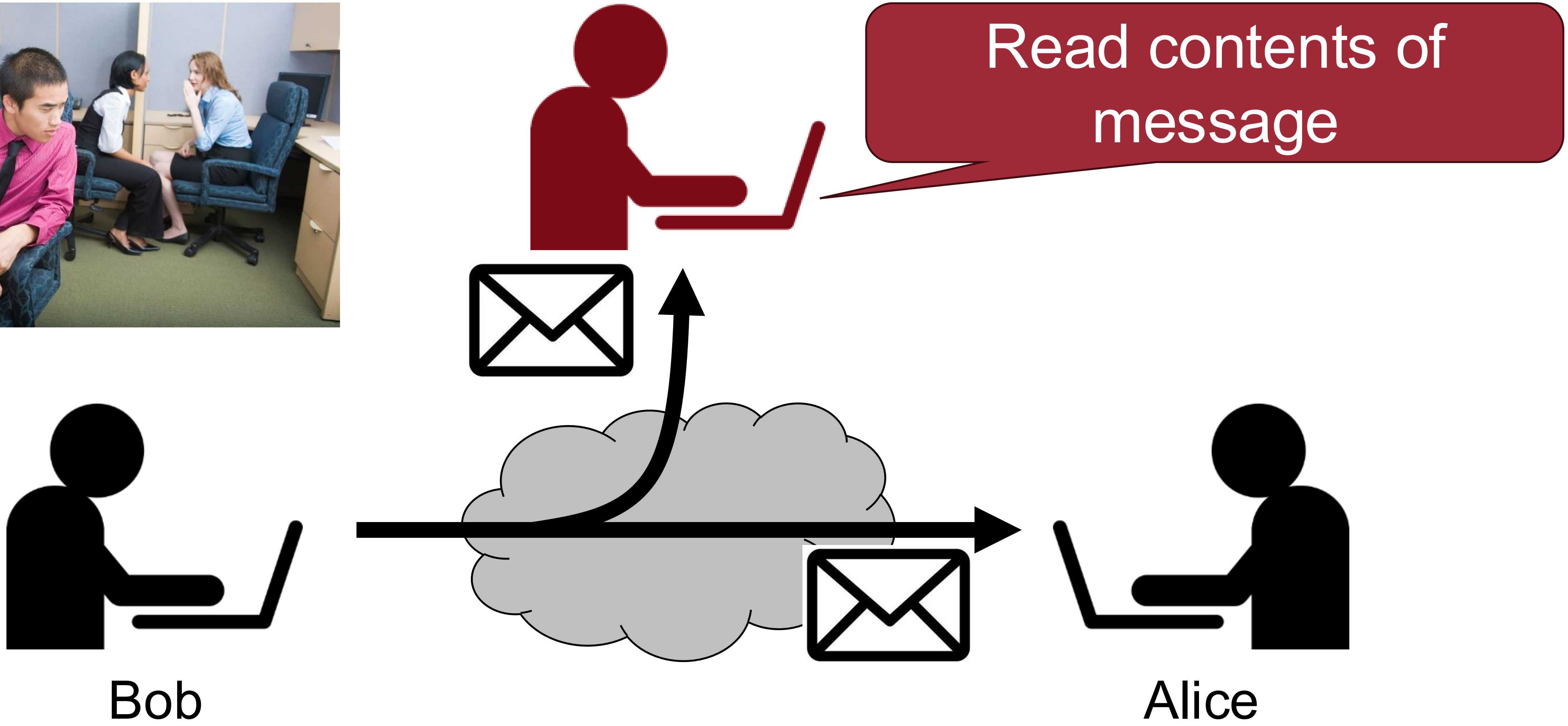
Passive Attacks



Internet or other communication facility

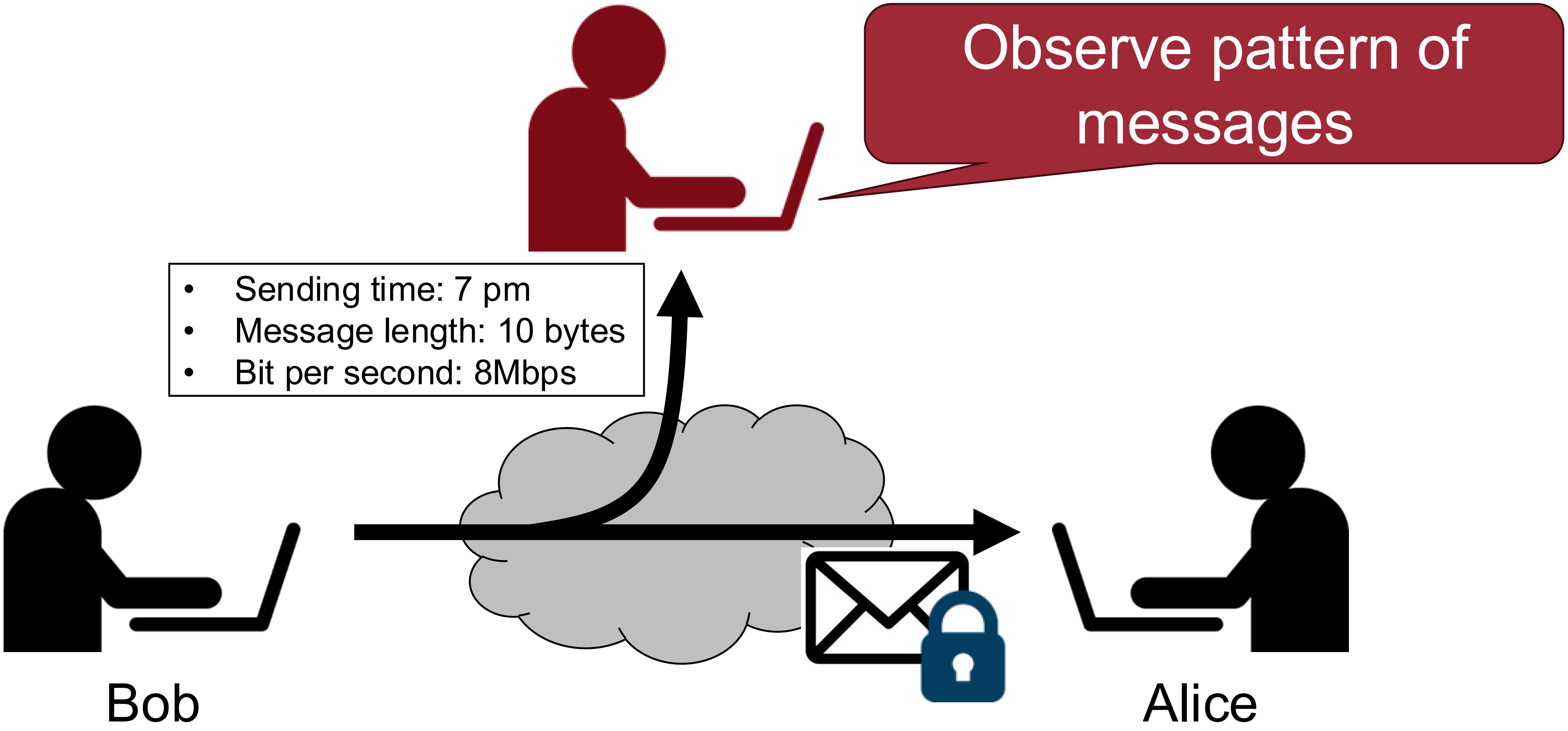
Passive Attacks

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



Passive Attacks

- Traffic analysis

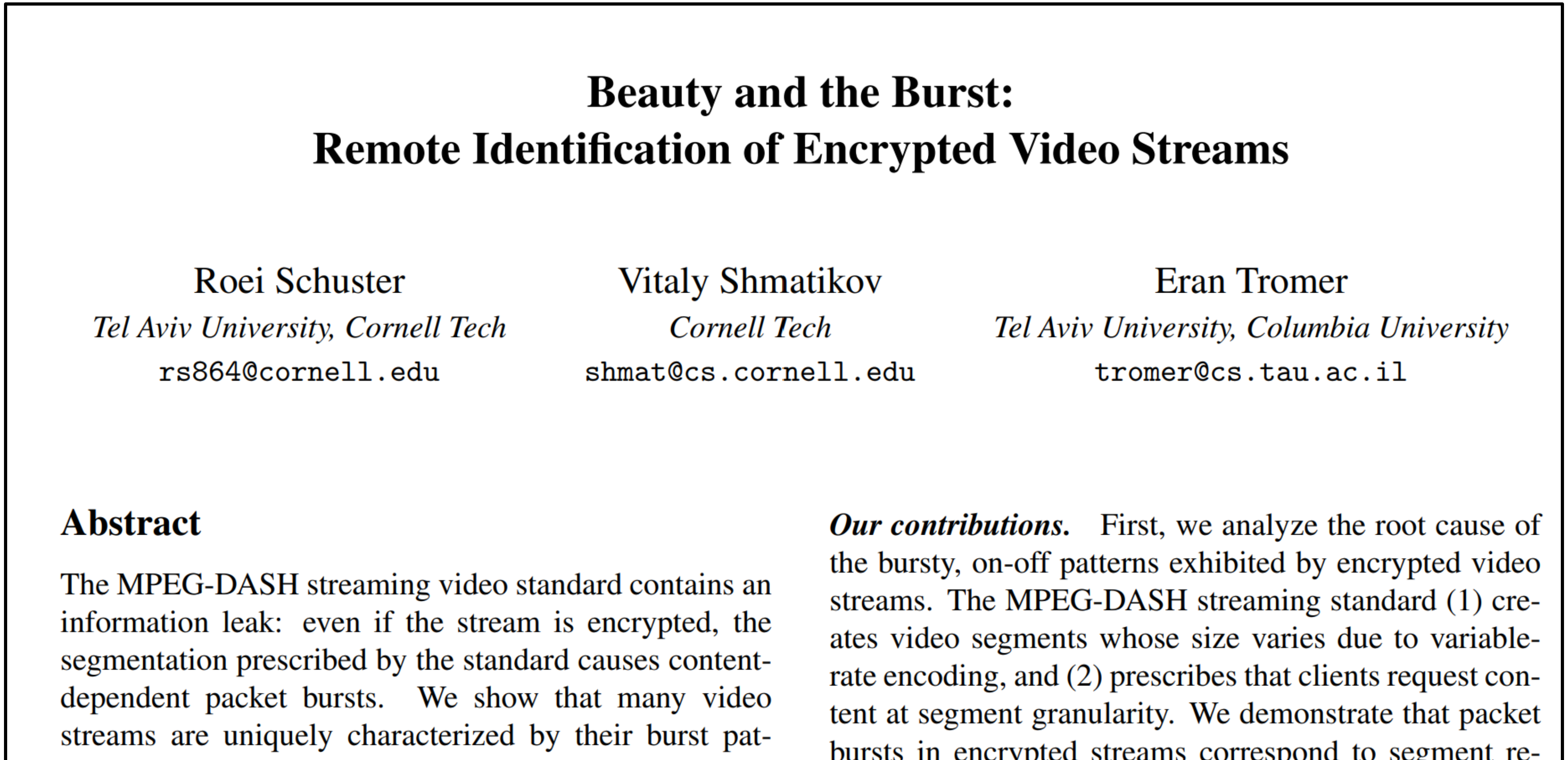


Observe pattern of messages

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

Passive Attack Example

- Beauty and the Burst: Remote Identification of Encrypted Video Streams, ***USENIX SEC'17***



Beauty and the Burst: Remote Identification of Encrypted Video Streams

Roei Schuster
Tel Aviv University, Cornell Tech
`rs864@cornell.edu`

Vitaly Shmatikov
Cornell Tech
`shmat@cs.cornell.edu`

Eran Tromer
Tel Aviv University, Columbia University
`tromer@cs.tau.ac.il`

Abstract

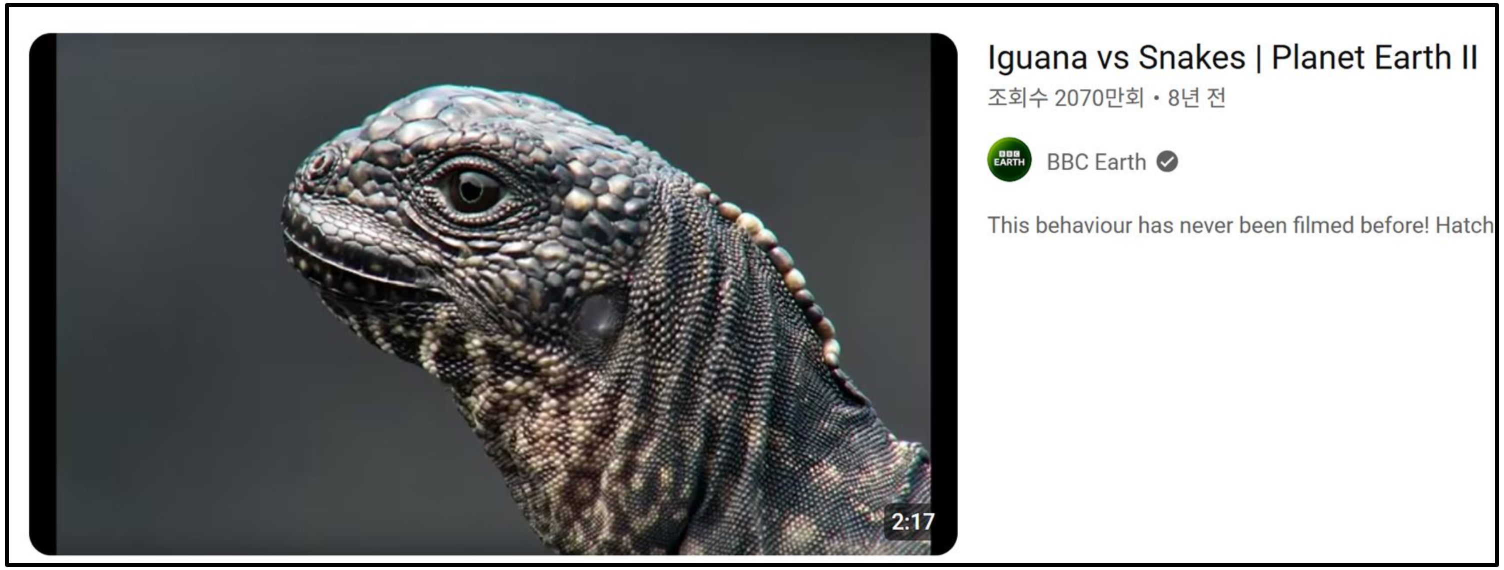
The MPEG-DASH streaming video standard contains an information leak: even if the stream is encrypted, the segmentation prescribed by the standard causes content-dependent packet bursts. We show that many video streams are uniquely characterized by their burst pat-

Our contributions. First, we analyze the root cause of the bursty, on-off patterns exhibited by encrypted video streams. The MPEG-DASH streaming standard (1) creates video segments whose size varies due to variable-rate encoding, and (2) prescribes that clients request content at segment granularity. We demonstrate that packet bursts in encrypted streams correspond to segment re-

Beauty and the Burst, *USENIX SEC '17*

- Observation: Many video streams are uniquely characterized by their ***burst patterns (Fingerprintable patterns)***
  - Even if packets are encrypted at the transport layer (e.g., using TLS), their sizes and times of arrival are visible to anyone watching the network

YouTube KR



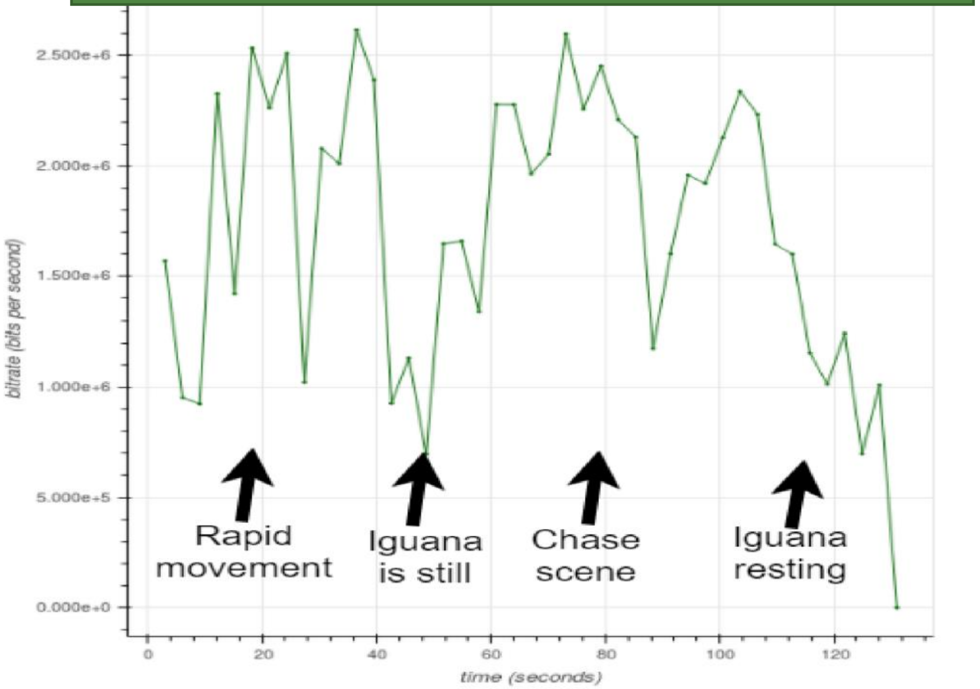
Iguana vs Snakes | Planet Earth II

조회수 2070만회 • 8년 전

BBC Earth

This behaviour has never been filmed before! Hatch

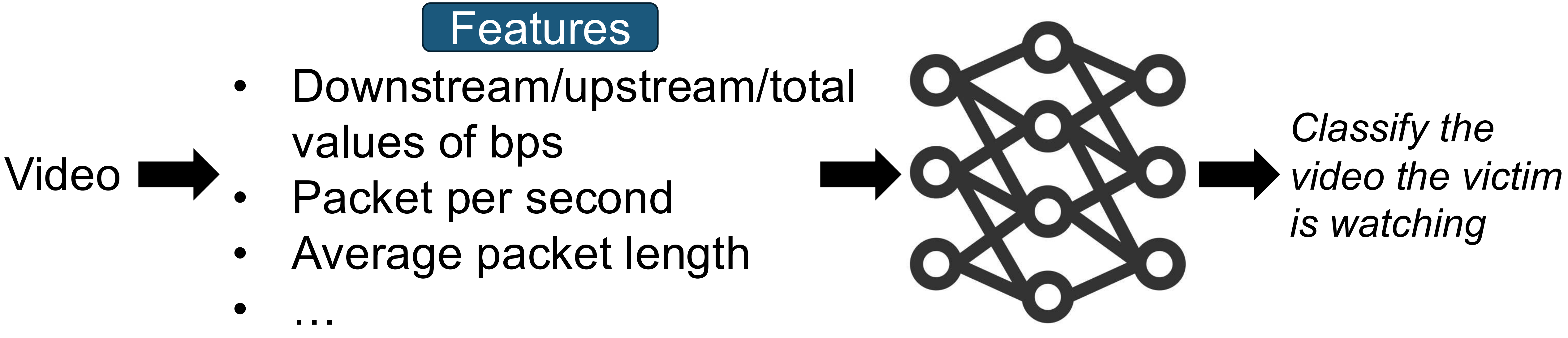
Iguana vs. Snakes bitrate



Scenery, movement, tension rising

Beauty and the Burst, *USENIX SEC '17*

- Observation: Many video streams are uniquely characterized by their ***burst patterns (Fingerprintable patterns)***
  - Even if packets are encrypted at the transport layer (e.g., using TLS), their sizes and times of arrival are visible to anyone watching the network
- Approach: ML-based video fingerprinting



Video

Features

- Downstream/upstream/total values of bps
- Packet per second
- Average packet length
- …

Classify the video the victim is watching

Beauty and the Burst, *USENIX SEC '17*

- Observation: Many video streams are uniquely characterized by their ***burst patterns (Fingerprintable patterns)***
  - Even if packets are encrypted at the transport layer (e.g., using TLS), their sizes and times of arrival are visible to anyone watching the network
- Approach: ML-based video fingerprinting
- Results:
  - Youtube: 0 false positives with 0.988 recall
  - Netflix: 0.0005 false positive rate with 0.93 recall

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

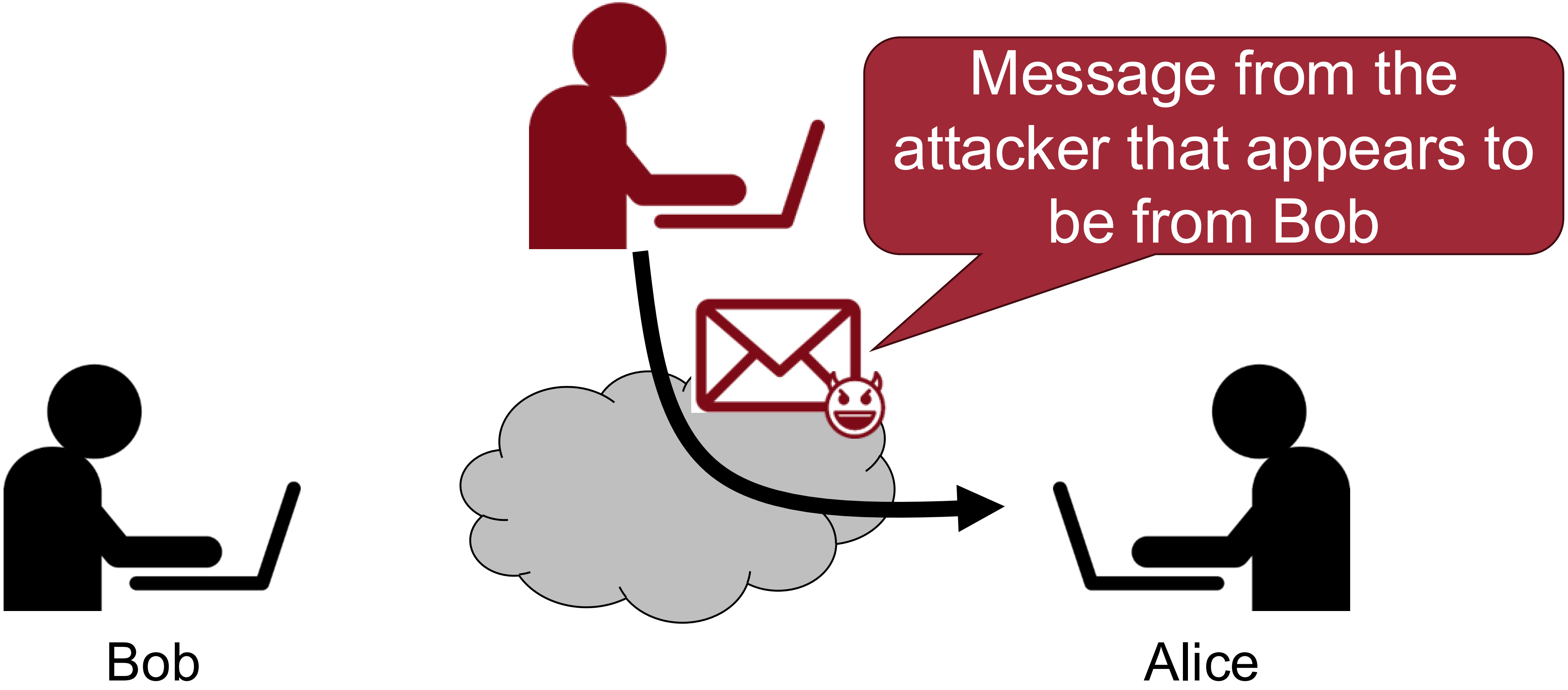
- **Creating illegitimate messages**
  - Masquerade (who)
  - Replay (when)
  - Modification of messages (what)

- **Denying legitimate messages**
  - Repudiation

- **Making system facilities unavailable**

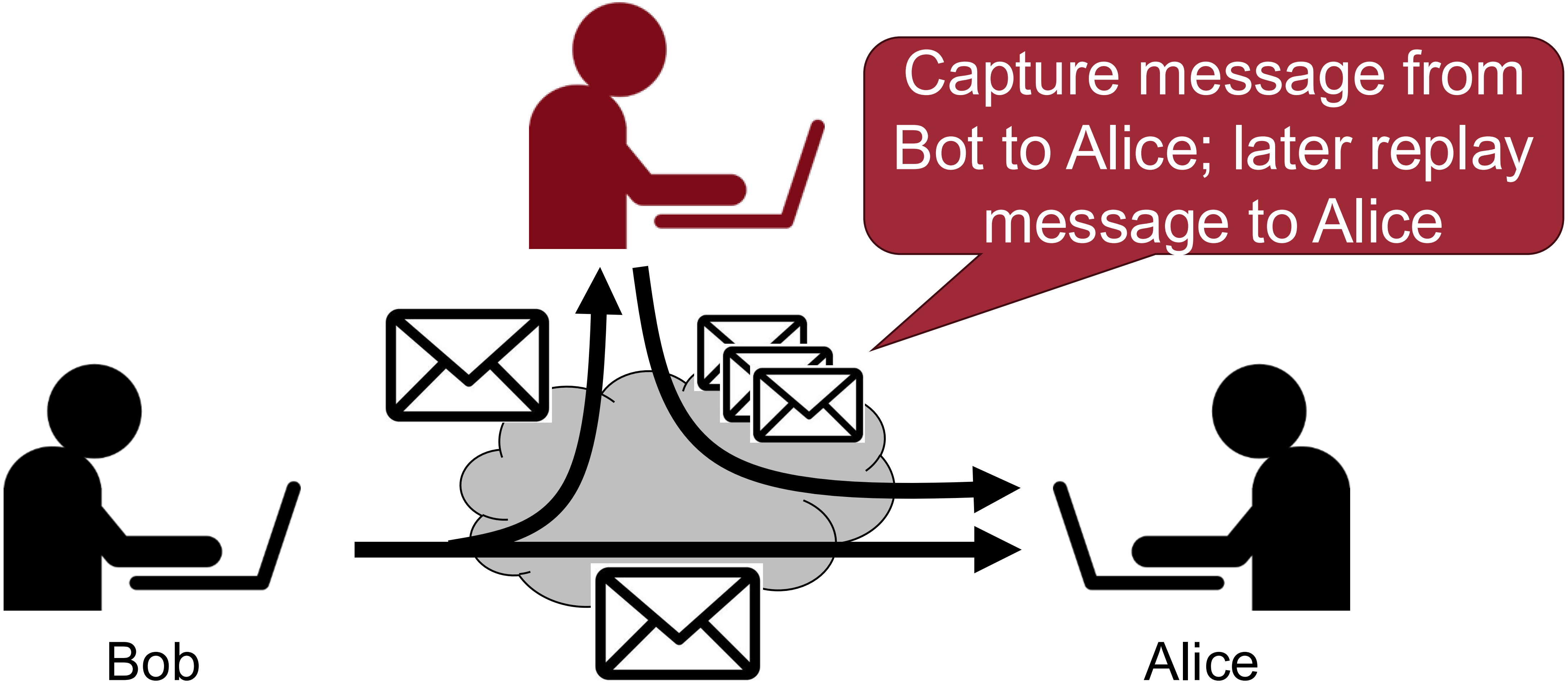
Active Attacks

- Masquerade
  - One entity pretends to be a different entity



Active Attacks

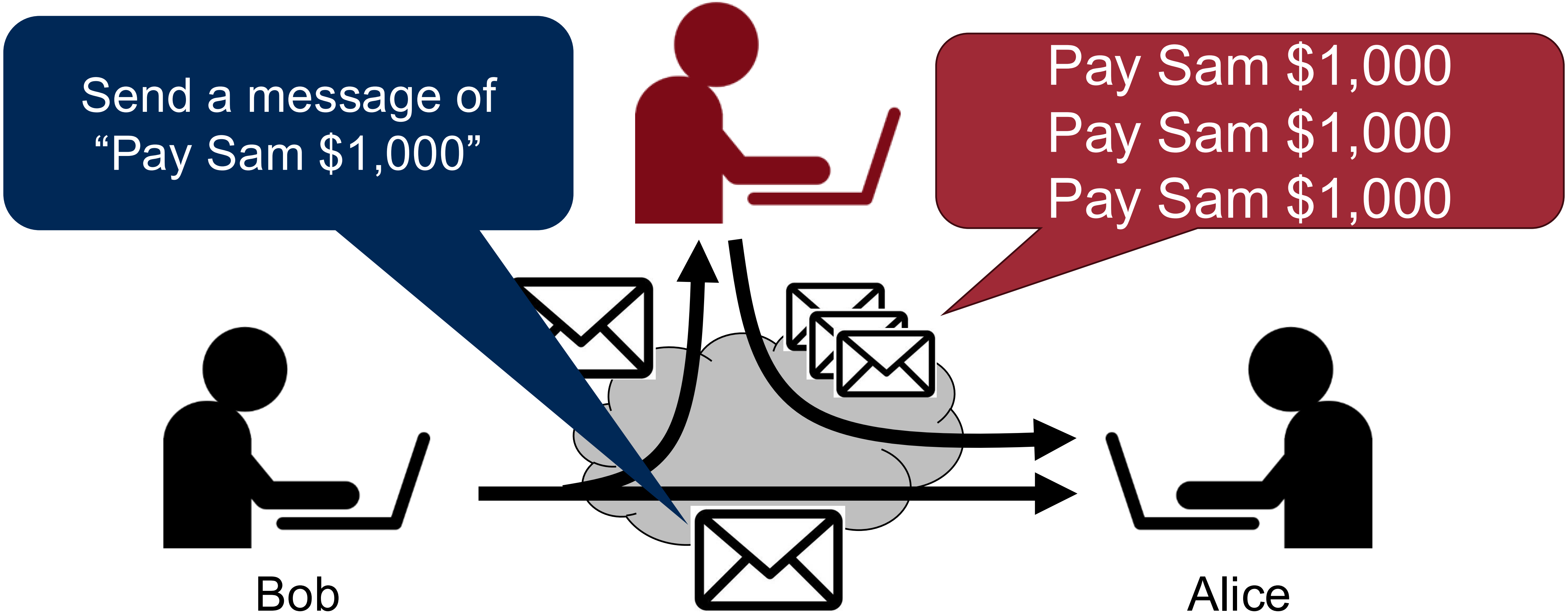
- Replay
  - A message is captured and retransmitted later



Capture message from Bot to Alice; later replay message to Alice

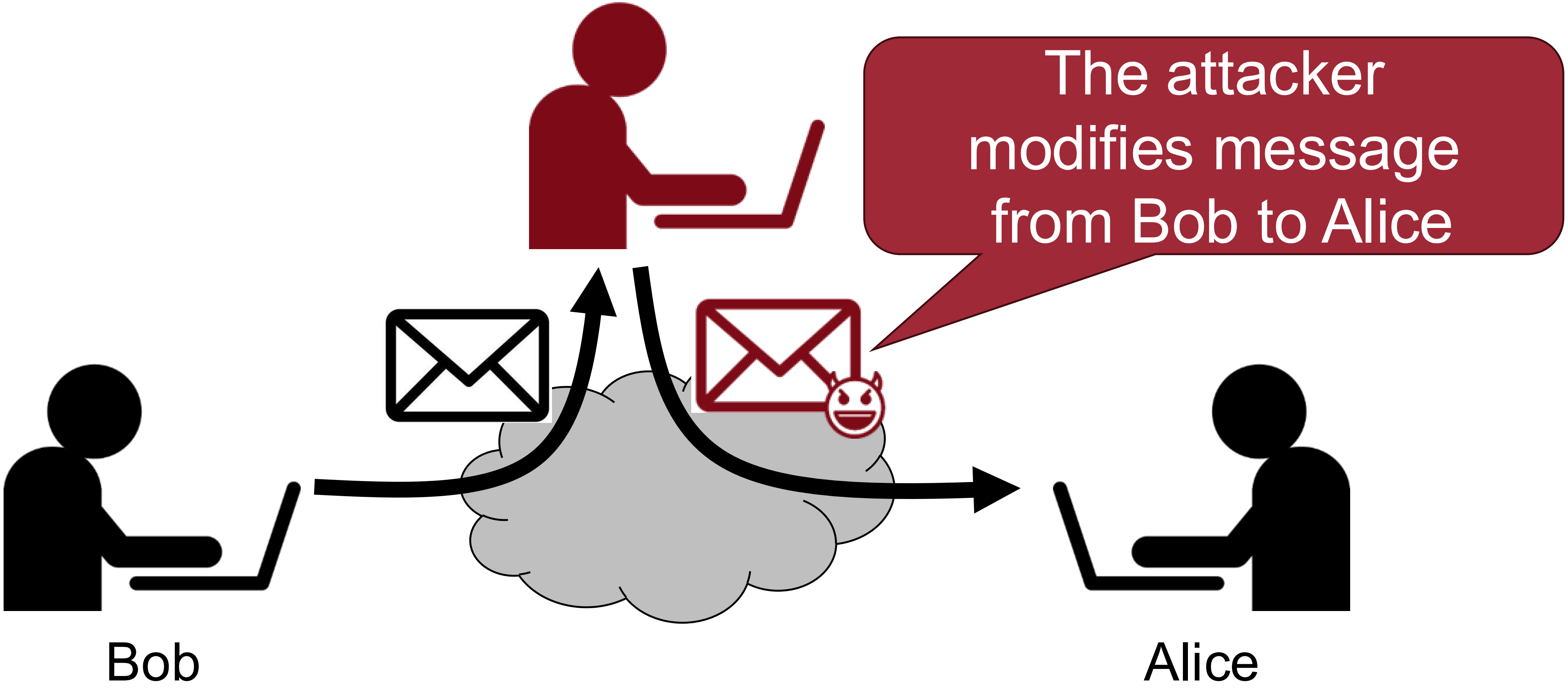
Active Attacks

- Replay
  - A message is captured and retransmitted later



Active Attacks

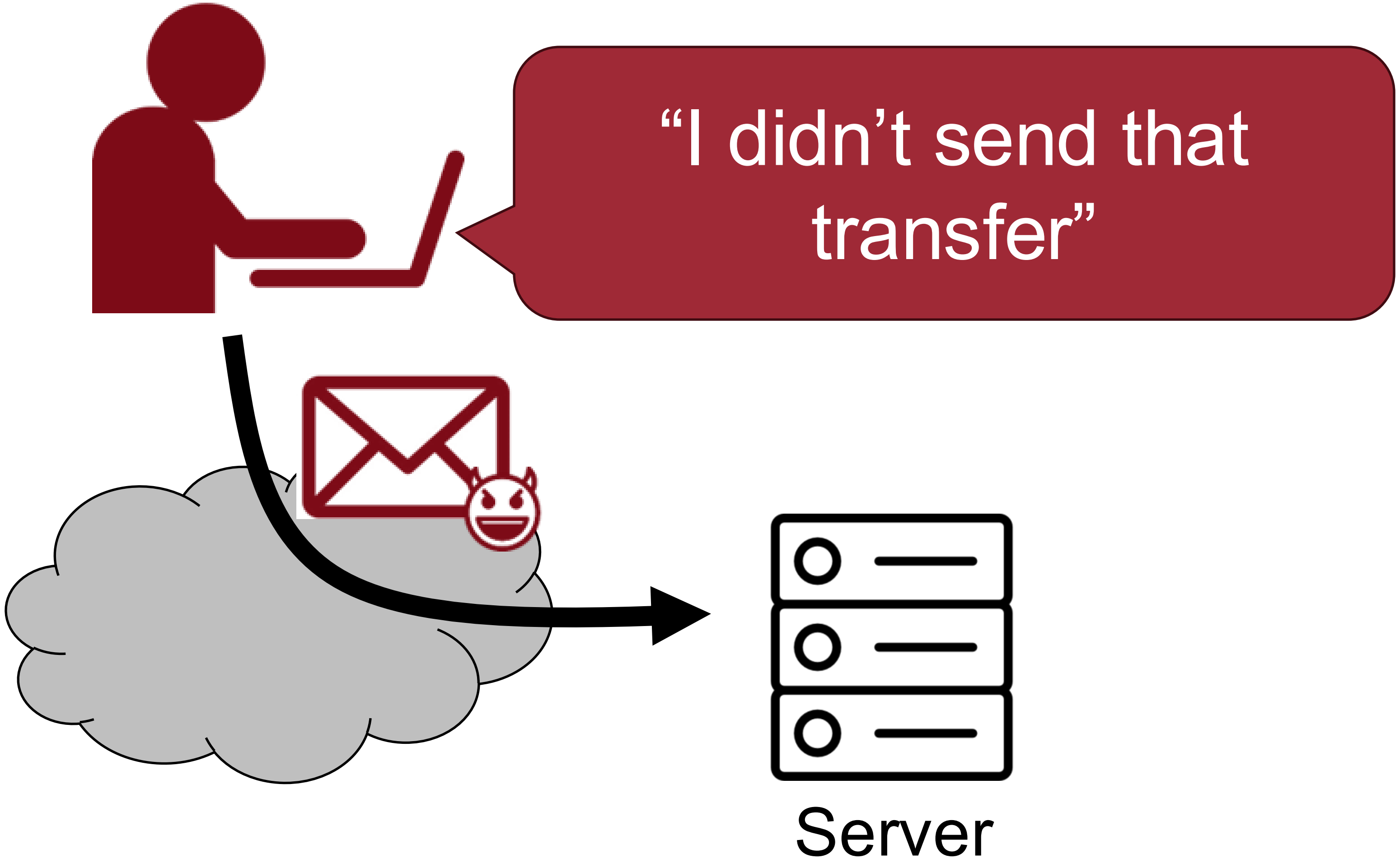
- Modification of messages
  - A message is captured, modified, and transmitted



The attacker modifies message from Bob to Alice

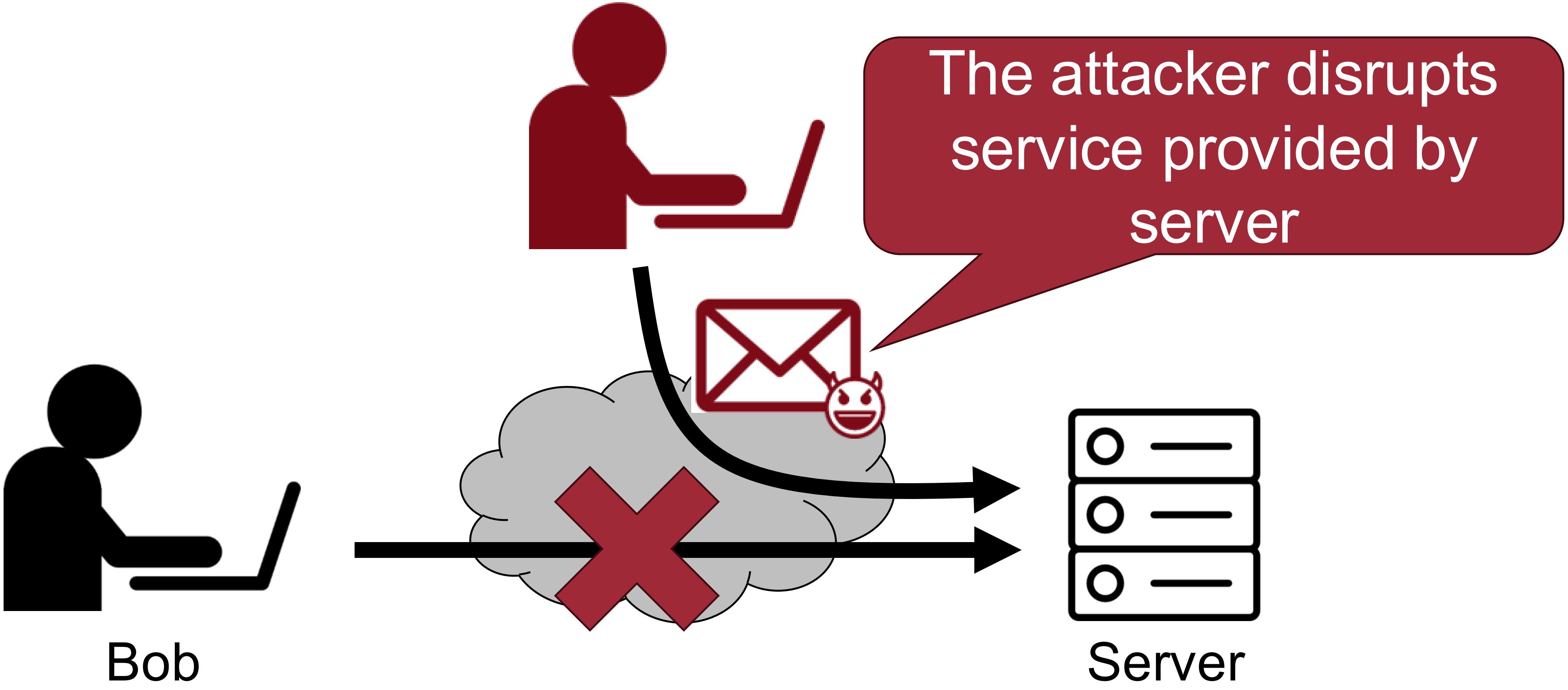
Active Attacks

- Repudiation
  - Denial of sending or receiving messages



Active Attacks

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



The attacker disrupts service provided by server

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**

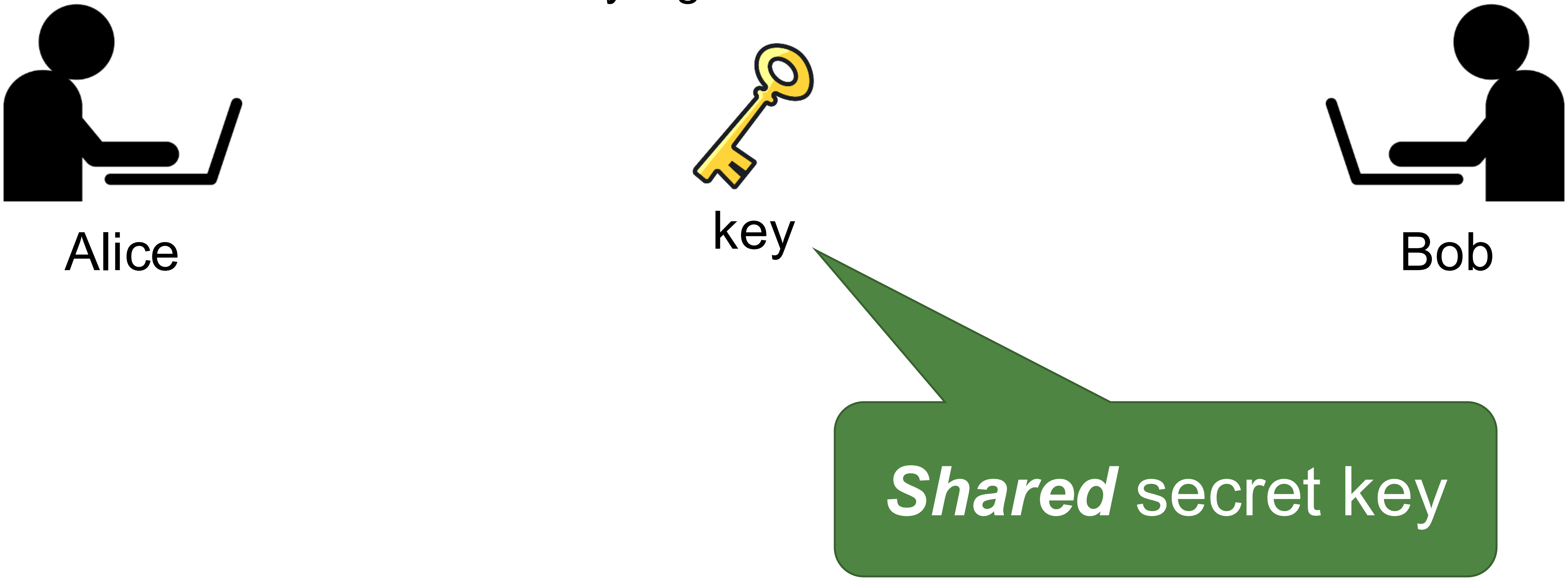
🤔 What about availability?

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

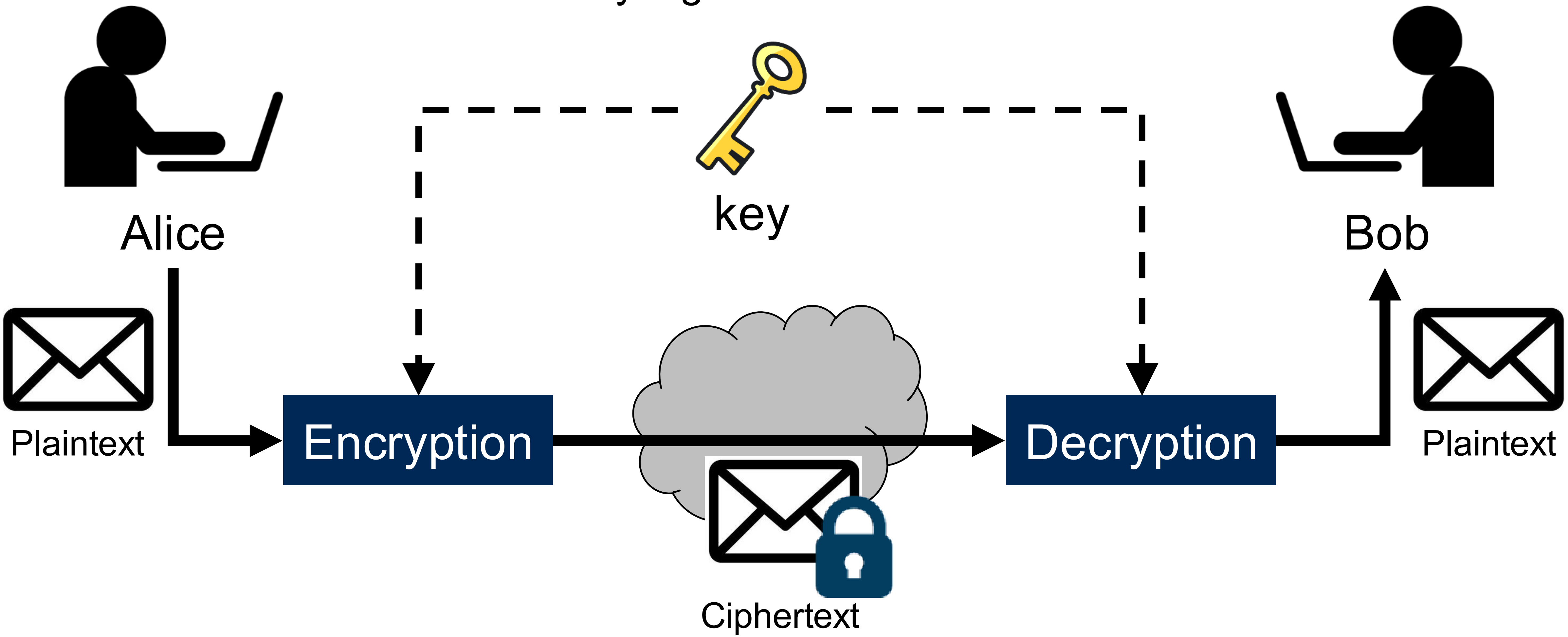
key

Bob

Shared secret key

Symmetric Key Cryptography

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



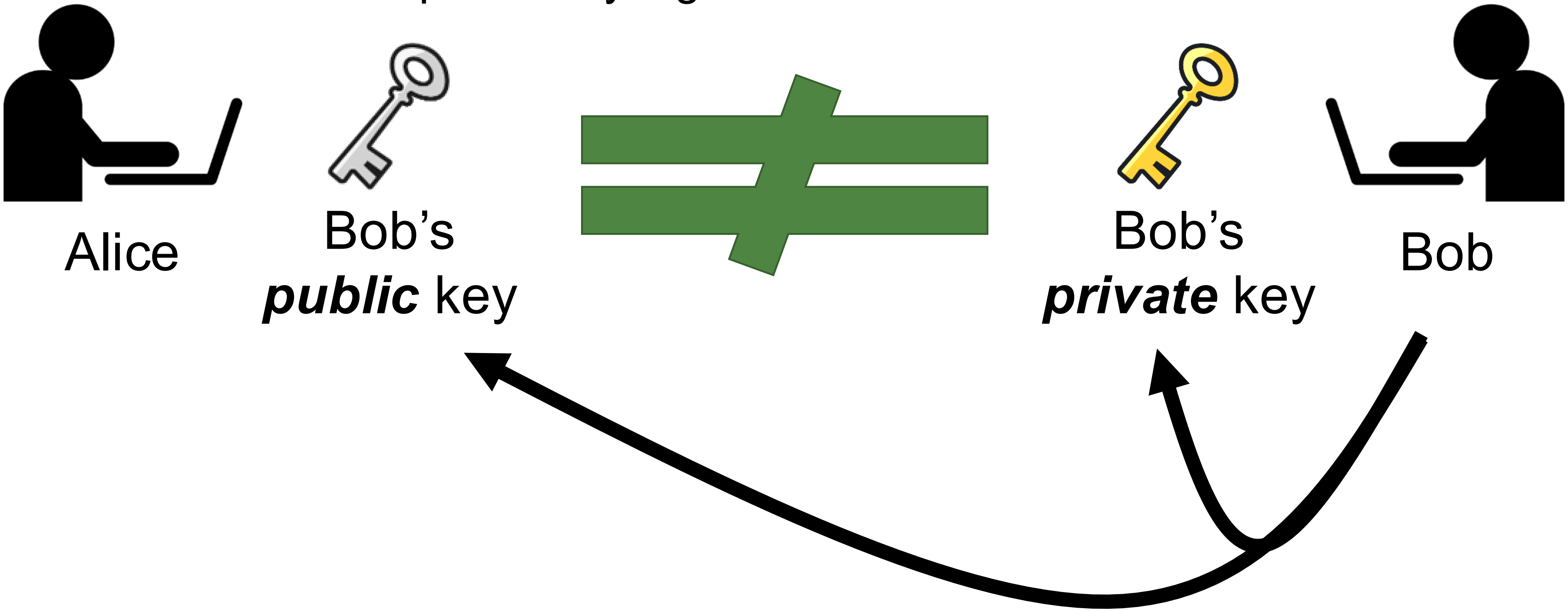
Symmetric Key Cryptography

- 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



Alice

Bob's ***public*** key

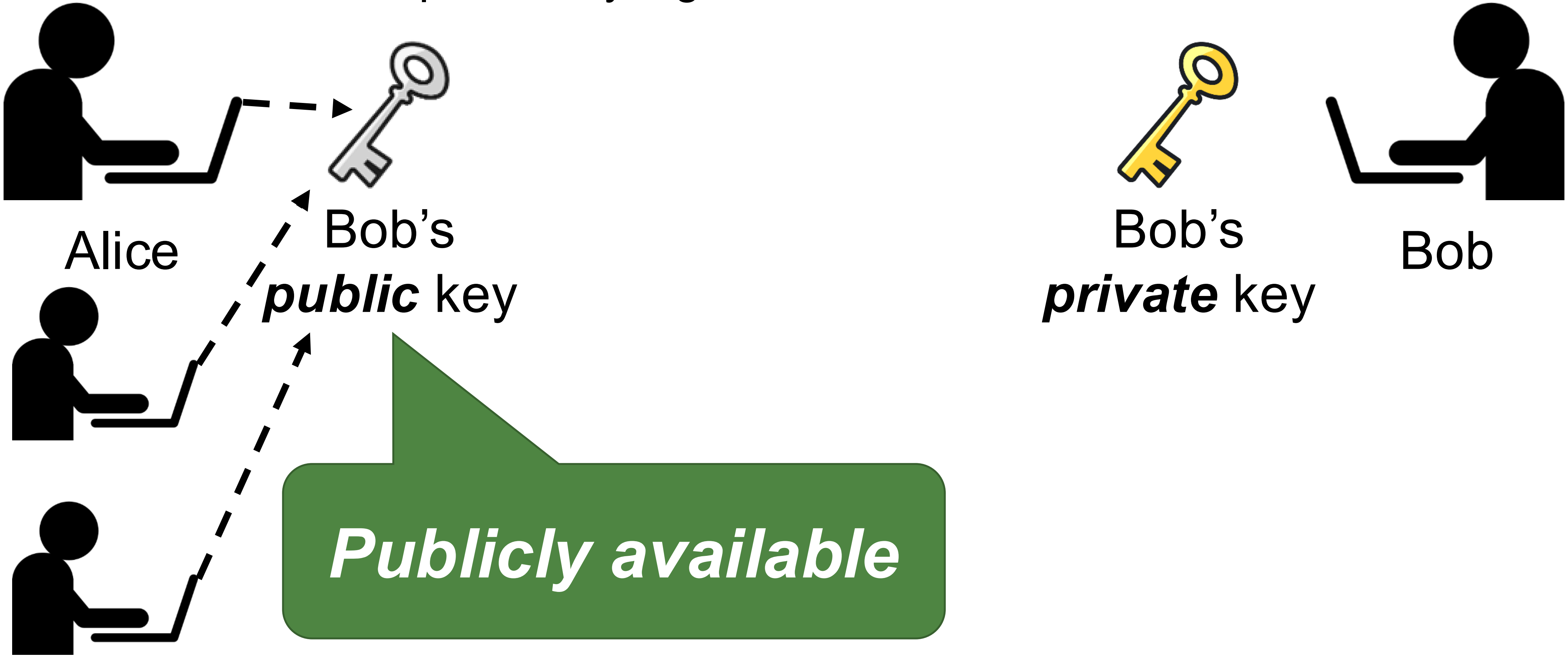
≠

Bob's ***private*** key

Bob

Asymmetric Key Cryptography

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



Alice

Bob's ***public*** key

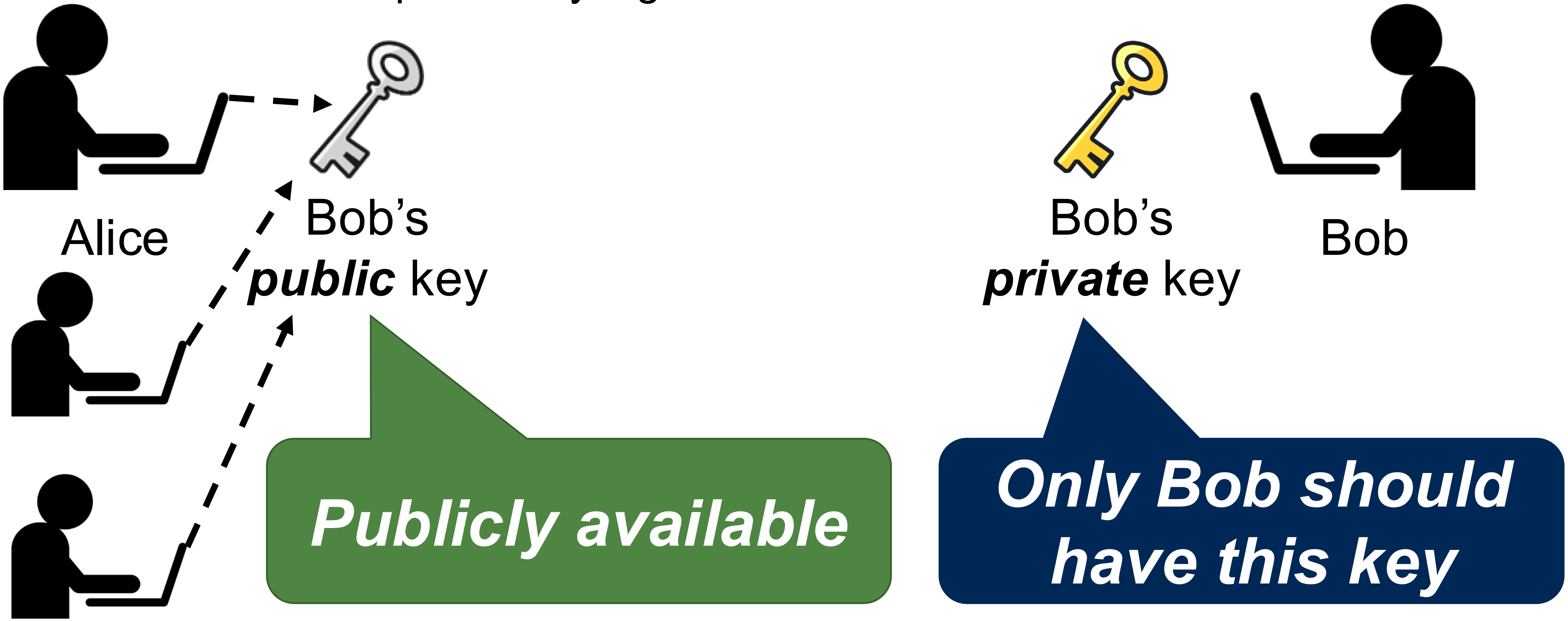
Bob's ***private*** key

Bob

Publicly available

Asymmetric Key Cryptography

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



Alice

Bob's ***public*** key

Bob's ***private*** key

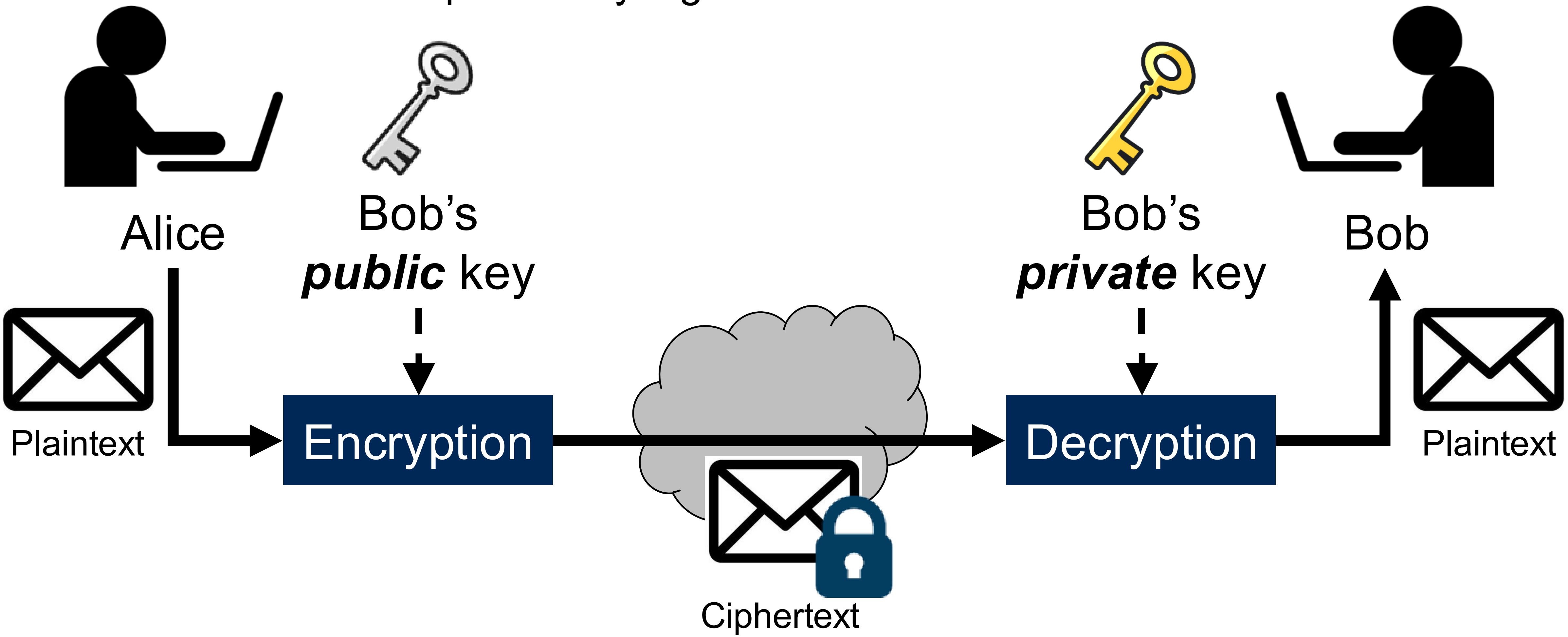
Bob

Publicly available

Only Bob should have this key

Asymmetric Key Cryptography

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

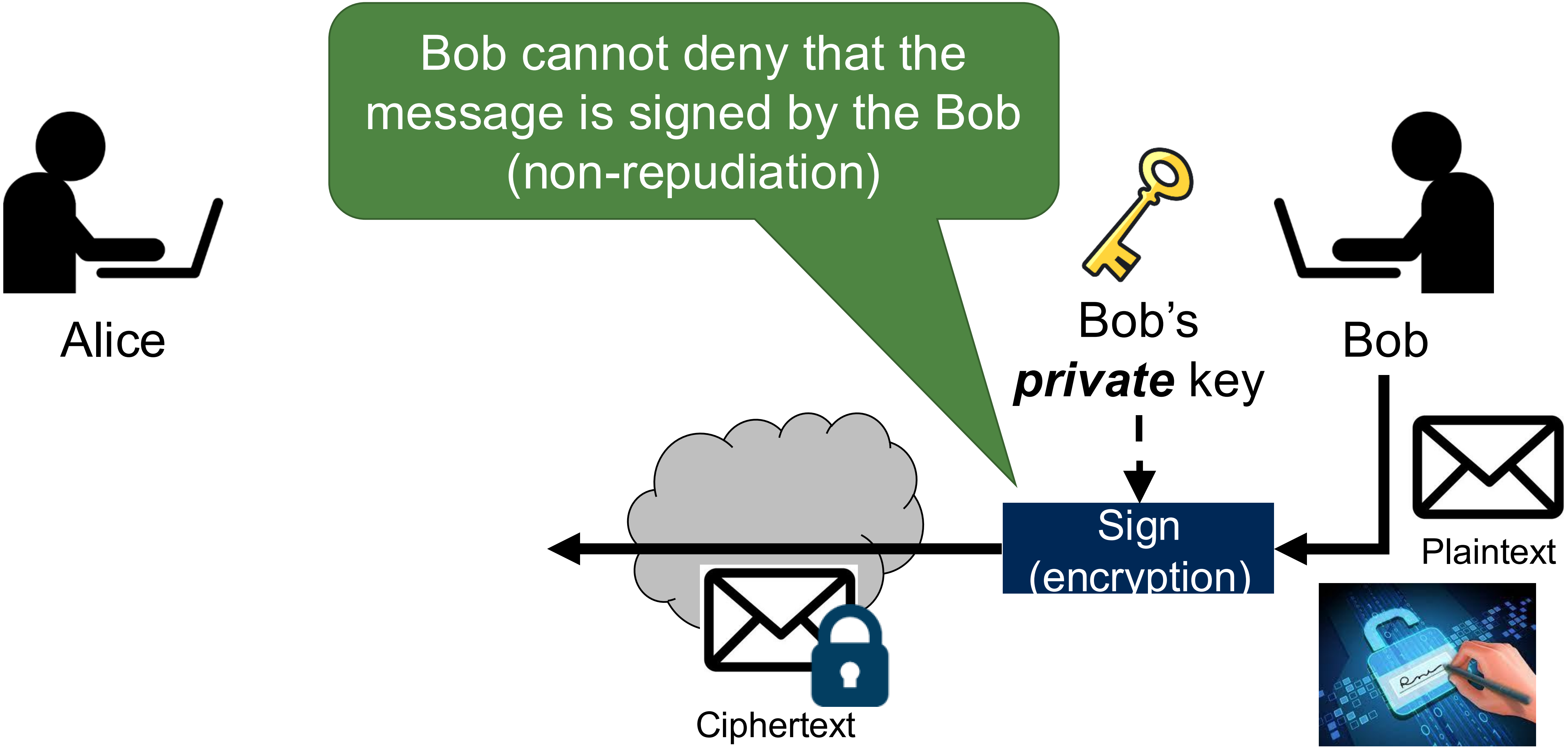


Asymmetric Key Cryptography

- Pros?

- Cons?

Digital Signature



Bob cannot deny that the message is signed by the Bob (non-repudiation)

Alice

Bob's *private* key

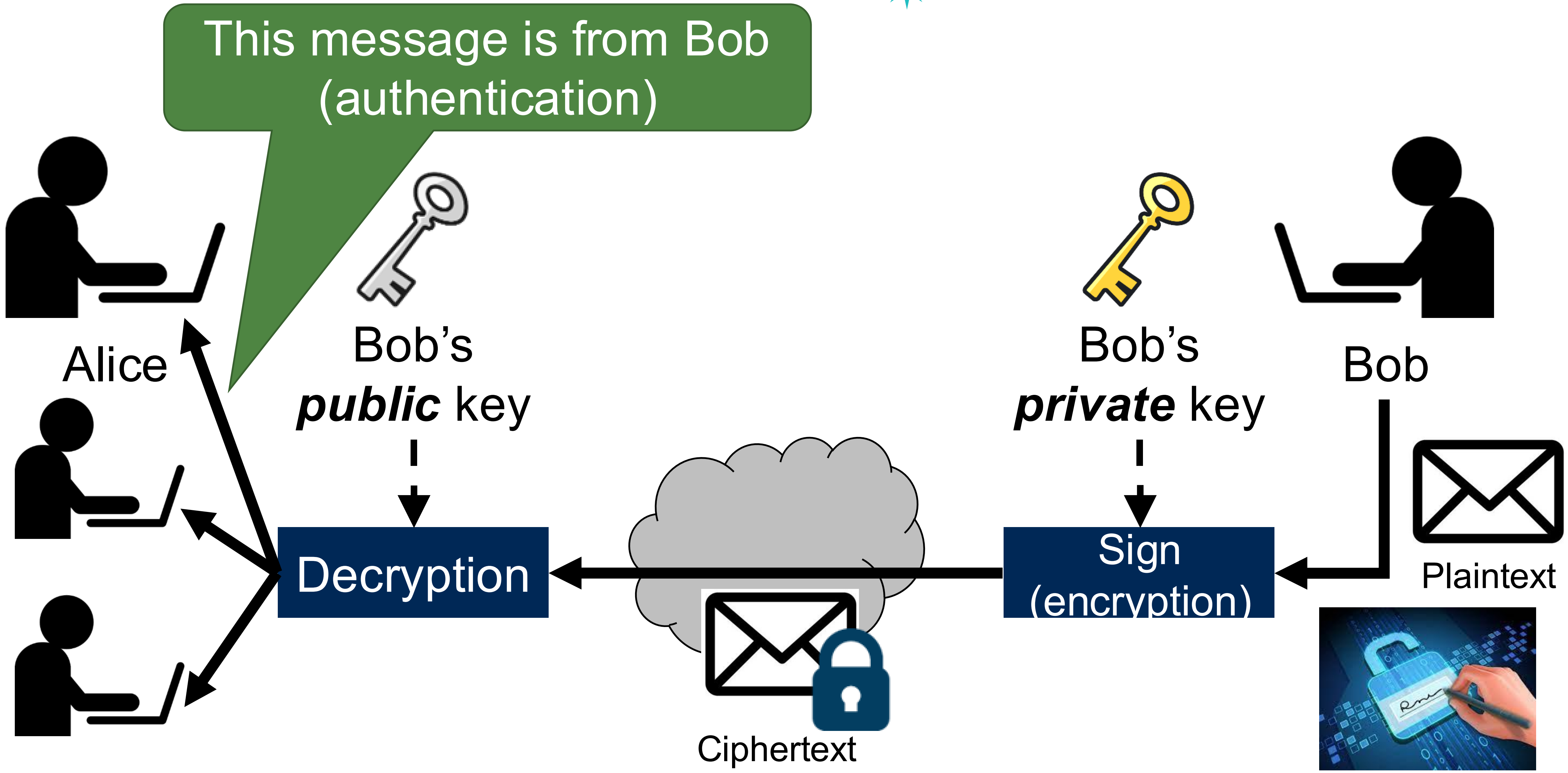
Bob

Sign (encryption)

Plaintext

Ciphertext

Digital Signature



This message is from Bob (authentication)

Alice

Bob's ***public*** key

Decryption

Ciphertext

Sign (encryption)

Bob's ***private*** key

Bob

Plaintext

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?