Computer Security

- Introduction to Cryptography and Security

Howon Kim

2019.3.6

About this course…

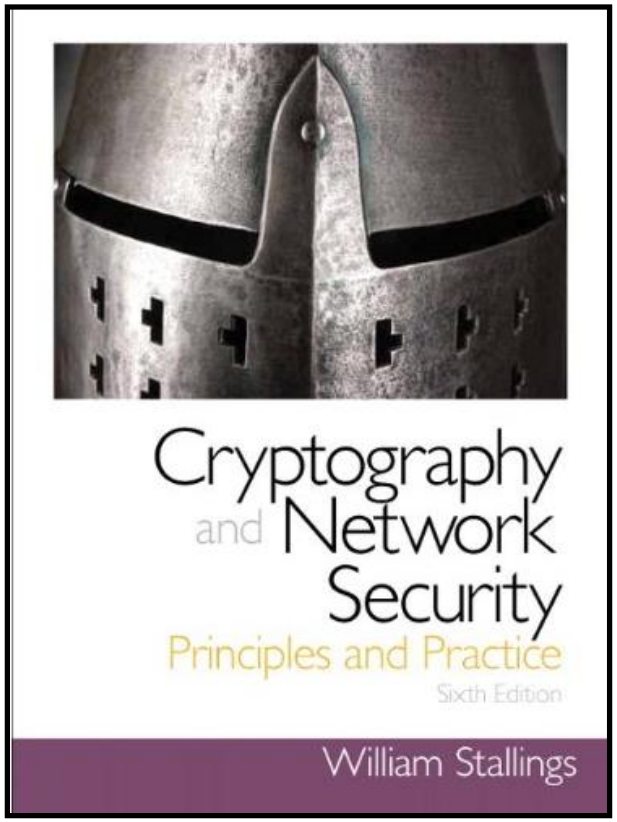
- Course name : computer security (CA24158)
  - Study the basics on cryptography & security
  - Study about the number theory (finite fields, ring, arithmetic), which is the fundamental knowledge for the cryptography & security
  - Study about the private key cryptography such as DES, AES, etc.
  - Study about the basic mechanism of the public key cryptography. RSA and ECC will be introduced
  - Study about the quantum cryptography.
  - Study about the applications of the cryptography. That is, about the security protocols (authentication protocol)
  - Understanding the cryptography and security issues in practical IT applications

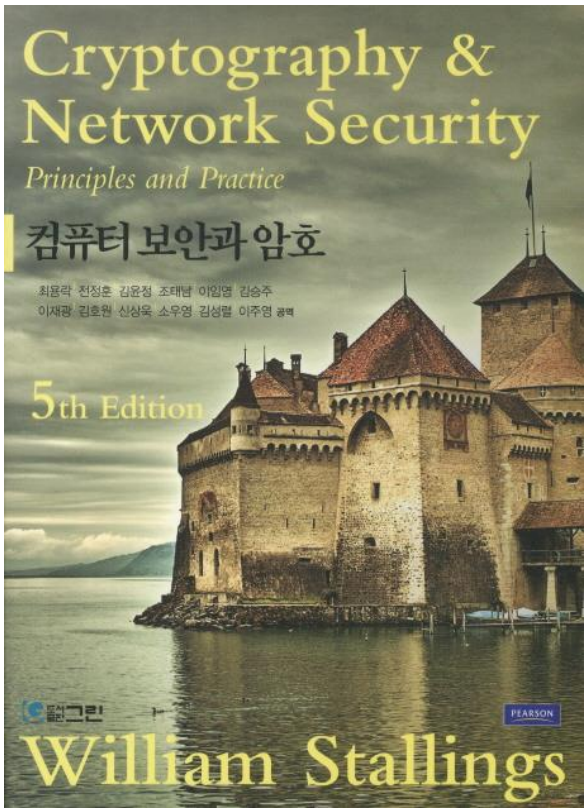
About this course…

- About me…
  - Office : A06-6503
  - Office hours : Monday & Wednesday, 13:00~14:00
  - Email: howonkim@pusan.ac.kr
  - Phone: 010-8540-6336
  - http://infosec.pusan.ac.kr
- Current Major Interests
  - Cryptography & Security
  - Blockchain & Its Security Issues
  - AI, Deep Learning, Digital Twin
  - FPGA & ASIC chip design
  - 과기정통부 사물인터넷 연구센터
  - 과기정통부 블록체인 보안 전문연구실
  - 과기정통부 양자컴퓨터 보안
  - 국가보안기술연구소, ETRI, KISA, Virginia Tech과 국제공동연구

About this course…

- Textbook (International edition is also available)
  - "Cryptography & Network Security: principles and practices" (6th Ed), William Stallings, Pearson Education Inc. 2013.



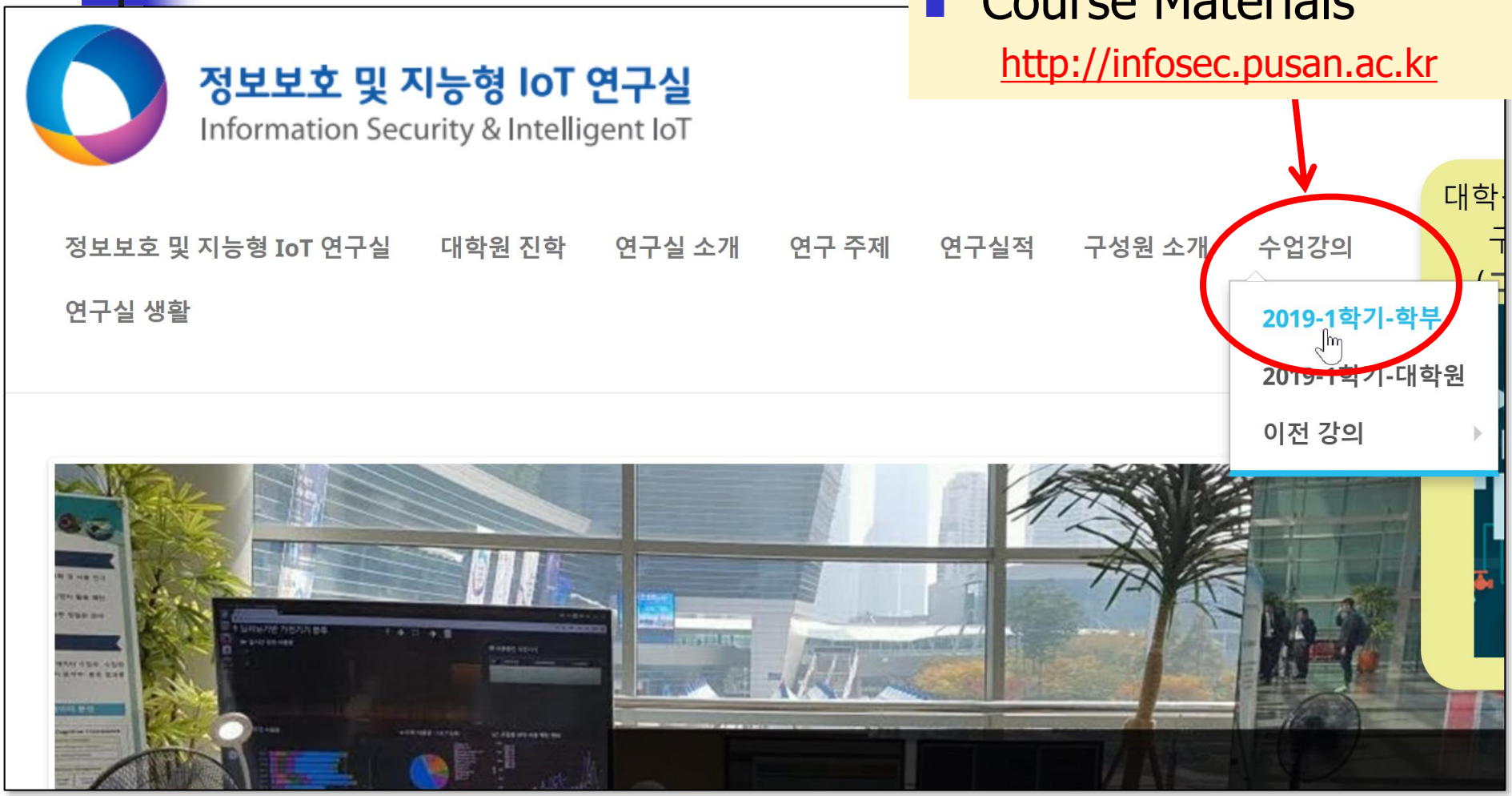


About this course…

- Time & Classroom
  - 10:30 ~ 11:45 AM (Monday, Wednesday)
- References
  - Handbook of Applied Cryptography, available at http://www.cacr.math.uwaterloo.ca/hac/
  - Cryptography in C and C++(2nd edition) by Michael Welschenbach, Apress, 2005.
  - Modern Cryptography: Theory and Practice(1st edition) by Wenbo Mao, Prentice Hall PTR, 2003

About this course…

- Course Materials
  http://infosec.pusan.ac.kr



About this course…

Detailed schedule

주	학습내용	교재	활동사항
1	Introduction of Cryptography and Security (1)	CH1	
2	Introduction of Cryptography and Security (2)	CH1	
3	Classical Encryption Techniques	CH2	
4	Block Ciphers and DES	CH3	
5	Modular Arithmetic and Finite Fields	CH4	
6	AES	CH5	
7	Symmetric Ciphers and Stream Ciphers	CH6,7	
8			Midterm exam.
9	Introduction to Number Theory (이산수학 II ?)	CH8	
10	Public Key Cryptography and RSA	CH9	
11	Key Management Scheme	CH10	
12	Message Authentication and Hash Functions	CH11,12	
13	Digital Signatures and Authentication Protocols	CH13	
14	Practical Security(virus, hacking, etc.) & Quantum Cryptography	-	
15			Final exam.

About this course…

- Grading Policy

항 목	점 수
Attendance	5
Midterm	40
Final	40
Homework	15
Total	100

Attacks and Countermeasures: Motivation

- Threaten the user
  - physical or social attack (e.g., rubber hose attack, psychological attack)

  ➡ How can we prevent this?

- Forge the certificate

  ➡ Countermeasure: Make a secure algorithm to protect a certificate

  Theory: cryptography

- Hack into the user's computer

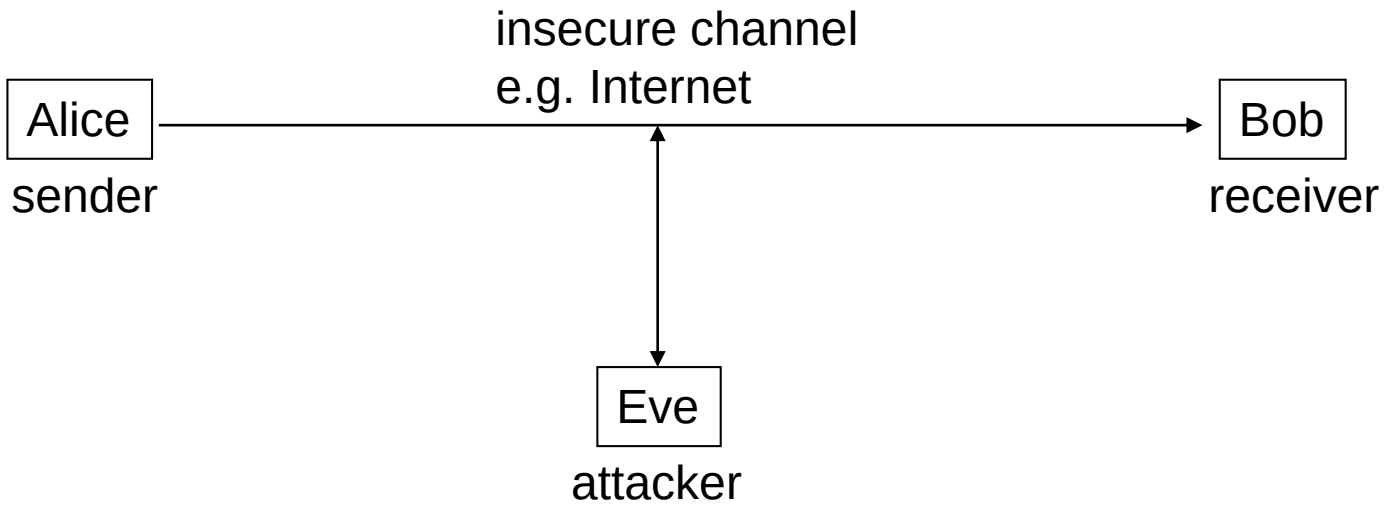
  ➡ Countermeasure:
  Make a secure system and a secure communication channel.

  Practice: system and communication security

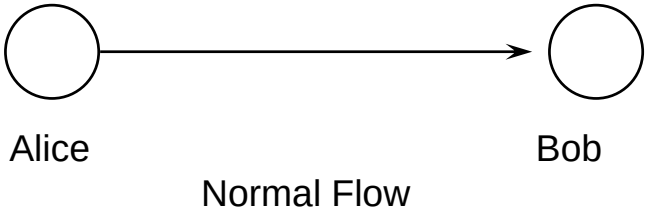
Cryptology

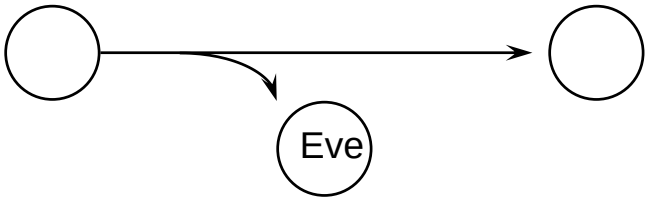
- Cryptology
  - Cryptography
    - designing systems to do secure communication over insecure channels
  - Cryptanalysis
    - breaking such systems

Basic Communication Scenario for Cryptography

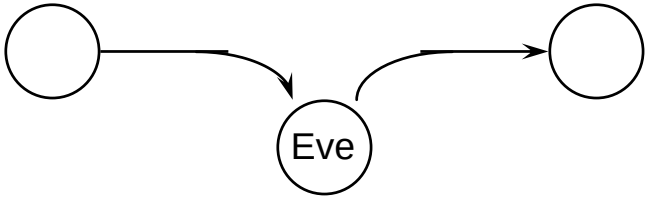


Threats

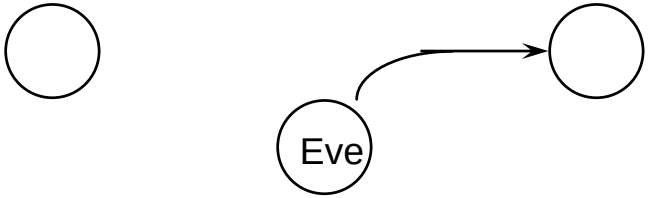




Eavesdropping ⇒ Confidentiality(기밀성으로 방지)



Modification ⇒ Integrity (무결성으로 방지 혹은 확인)



Impersonation ⇒ Authentication(인증으로 확인)

Security Services

- Confidentiality (or Privacy) 기밀성
  - Eve should not be able to read Alice's message to Bob.
- (Data) Integrity 무결성
  - Bob wants to be sure that Alice's message has not been altered.
  - i.e., contain no modification, insertion or deletion
- Authentication 인증
  - Bob wants to be sure that his communication partner is Alice.
- Non-repudiation 부인방지
  - Alice cannot claim that she did not send the message, if she actually sent it.
  - This service is particularly important in electronic commerce applications, where it is important that a consumer cannot deny the authorization of a purchase.

Security Services

- Access Control 접근제어
  - Prevention of unauthorized use of a resource
  - This service controls
    - who can have access to a resource,
    - under what conditions access can occur,
    - and what those accessing the resource are allowed to do.
- Availability 가용성
  - A system or a system resource should be accessible and usable
    - upon demand by an authorized system entity,
    - according to performance specifications for the system.

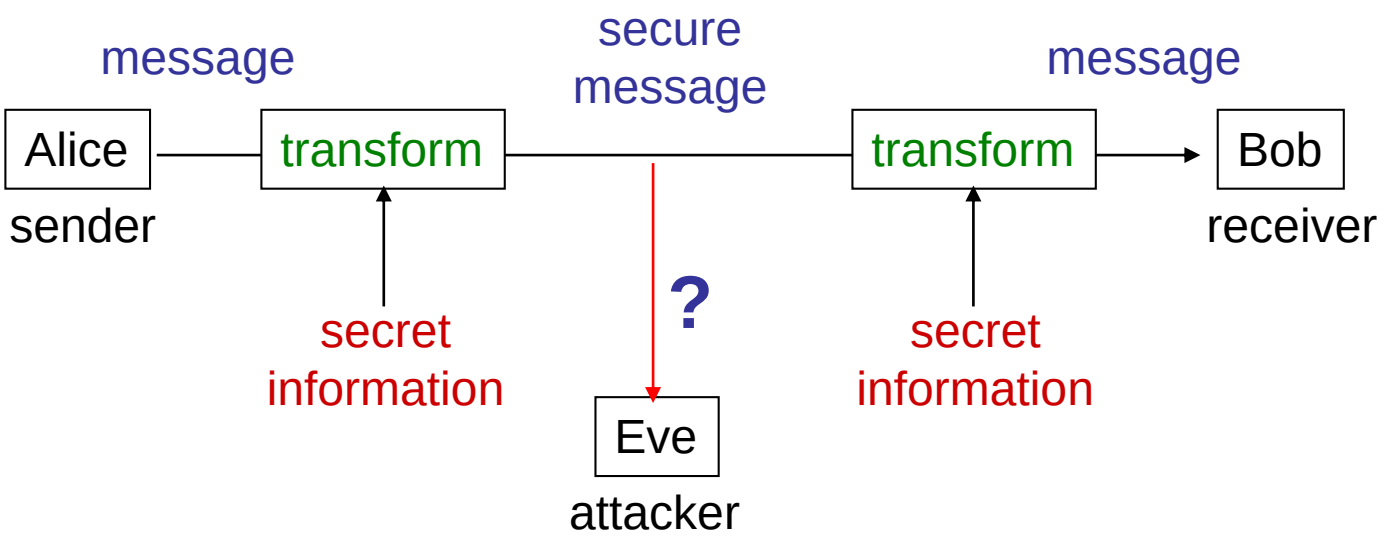
Cryptographic Mechanisms

Confidentiality → Encryption algorithm 암호알고리즘
- Classical cryptosystems
- Symmetric key algorithms (DES, AES)
- Public key algorithms (RSA, ElGamal)

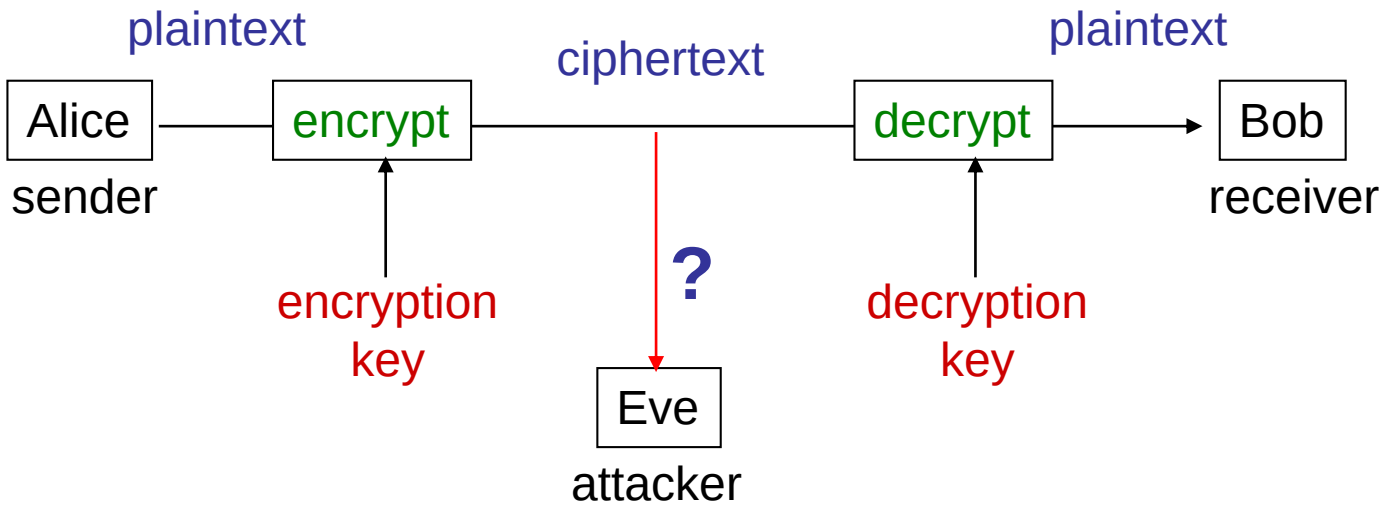
Integrity
Authentication → Digital Signature 전자서명
- RSA signature
- DSA

Message Authentication Code 메시지인증코드

Confidentiality Model



Confidentiality Model



plaintext: 평문 ciphertext: 암호문

encrypt: 암호화 decrypt: 복호화

Cryptography vs. Steganography

- Cryptography
  - The existence of the message itself is not disguised, but the meaning is obscured.
  - Even the encryption method is also assumed to be known to an attacker.
  - What keeps the message secret is a **key**.
- Steganography
  - No one apart from the intended recipient knows of the existence of the message.
  - Example [Herodotus (485 ~ 525 BC, the first Greek historian), “The Histories of Herodotus”]
    - Histaeus shaved the head of his most trusted slave and tatooed a message on his head.
    - After his hair had grown the message was hidden.

Example of Steganography

A GIF carrier file containing the airport map

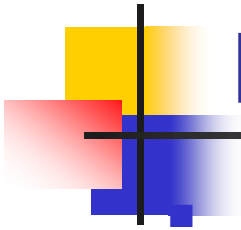
< GIF image of the Washington DC mall at night >

예: GIF-it-up 프로그램을 사용한 steganography 수행

Hides information in GIF files using least significant bit substitution !

< airport map, Burlington, Vermount>

http://www.garykessler.net/library/fsc_stego.html



Next…

- Introduction of Cryptography and Security (2)
  - Basics on
  - classical encryption technique
  - private key cryptography
  - public key cryptography
  - security protocols
  - network security & Internet security
  - Etc.

Homework #1

- Sage 패키지 사용환경 설치 **(http://www.sagemath.org/)**
  - Windows상에서 VirtualBox 설치(무료)
  - Sage가상 이미지 파일 다운로드 후, VirtualBox로 설치
  - http://ftp.kaist.ac.kr/sage/win/index.html에서 sage-7.4.ova 파일 다운로드

- Sage 사용법 익히기

- HW #1 제출 내용:
  - Sage를 사용하여 Euclidean 알고리즘을 사용하여,임의의 두 정수의 gcd를 구하는 프로그램 작성 후, 제출(3월 13일 월요일 수업시간에 제출)


Q&A