

# 오리엔테이션

2022년 9월 7일 수요일

정보보호

충남대학교 정보보호연구실 허강준

- 강의 소개
- 실습 소개
- 추후 일정
- 과?제공지

# 강의 소개

- 담당 교수님: 류재철 교수님
- TA: 허강준 @ 정보보호연구실 (공5629)
- 연락 혹은 질문이 필요한 경우 [kheo@islab.work](mailto:kheo@islab.work) 로
  - 너무 답장이 없다 싶으면 [knowledge@o.cnu.ac.kr](mailto:knowledge@o.cnu.ac.kr) 로 다시 보내주시길...
  - 랩실로 찾아와도 됩니다만 자리에 없을수도...
- 이론/실습 각각 1주일에 2시간씩
- 이론: **월요일 10:00 ~ 12:00**
- 실습: **수요일 10:00 ~ 12:00**

	월	화	수	목	금
9					
10					
11					
12					

# 강의 소개 – 앞으로 사용하게 될 교재

알기 쉬운 정보보호개론 : 흥미로운 암호 기술의 세계, 3판,  
히로시 유키 지음, 이재관, 전태일, 조재신 공역, 인피니티북스



暗号技術入門 秘密の国のアリス 第3版  
結城 浩 著, SBクリエイティブ



## 강의 소개 – 성적은 이렇게 나갑니다.

- 중간고사 30%
- 기말고사 30%
- 과제 30%
- 출석 10%

### 주의사항

- 출석 시수가 전체 시수의  $\frac{3}{4}$ 에 미달하는 경우 F입니다.
- 시험 부정 행위는 F입니다.
- 과제 부정 행위는 가담자 전원 해당 주차 과제 점수를 0점 처리합니다.
- 기한 경과 후 제출 과제는 1일마다 0.5점씩 감점됩니다.

## 강의 소개 – 시험?

- 8주차 중간고사, 15주차 기말고사 (와 동시에 종강)
- 이론과 실습에서 각각 50%씩 출제 (6~8문제 정도)
  - 얘기하지 않은 내용은 **절대로 나오지 않습니다**
  - 안낸다고 한 내용도 **절대로 나오지 않습니다**
  - 아무튼 그냥 **즐기시면 됩니다**

## • 작년... 그리고 올해 예정했던 실습

2021 정보보호

E2EE Chat Docs

로그인

### End-to-End Encryption Chat Protocol (3E) Specification

최종 업데이트: ver 1.0, 2021-10-07

이 문서는 충남대학교 2021학년도 학부 정보보호과목의 실습 진행을 위하여 서버 접근 정보 및 프로토콜에 대해 명세하고 있습니다.

자료 참조에 문제가 있는 경우 [메일보기](#)를 통해 조교에게 연락하시기 바랍니다.

#### 개요

End-to-End Encryption Chat Suite (이하 E2EECS)는 TCP 소켓 통신 기반의 보안 채팅 솔루션입니다. 각 사용자 간에 송/수신되는 모든 메시지는 암호화되어야 하며 별다른 조치가 없는 경우 서버 상에서 평문을 확인할 수 없어야 합니다. 본 문서는 E2EECS의 클라이언트 개발자가 E2EE 클라이언트(이하 E2C)를 개발하는데 있어 필요한 내용을 담고 있으며 다음과 같이 구성되었습니다:

- 프로토콜 기본 구조
- 서버 연결 및 종료 절차
- 키 교환 절차
- 메시지 처리 절차

본 문서에서는 서버와 클라이언트가 주고받는 메시지를 색상으로 구분합니다.



무슨 일이 있었는지는...: <https://github.com/CNUCSE-InformationSecurity-2021-Fall>

# 실습 소개

- 4학년 2학기인데 내가 너무했던게 아닐까?

교수님의 강의는 매우 훌륭하였지만 실습조교가 미달이었다고 생각이 듭니다. 실습과제위주의 시험문제제출로 인해 이론강의에 대한 평가가 제대로 이뤄지지 않은 것 같고 실습과제의 난이도에대한문제가 심각하고 제대로된 실습과 과제의 유도과정이 생략되어 많은 학우들이 어려움을 겪음.

실습 휴강을 당일에 알려준다  
실습을 많이 안한다  
과제의 난이도 차이가 심하다  
문제도 교수님의 수업과 어긋난다

채팅 프로그램 실습 난이도가 높아서 약간 개선되었으면 좋겠고 이외는 모두 만족했습니다

실습 과제가 너무 어려웠습니다.



# 실습 소개

- 그래서...



# 실습 소개

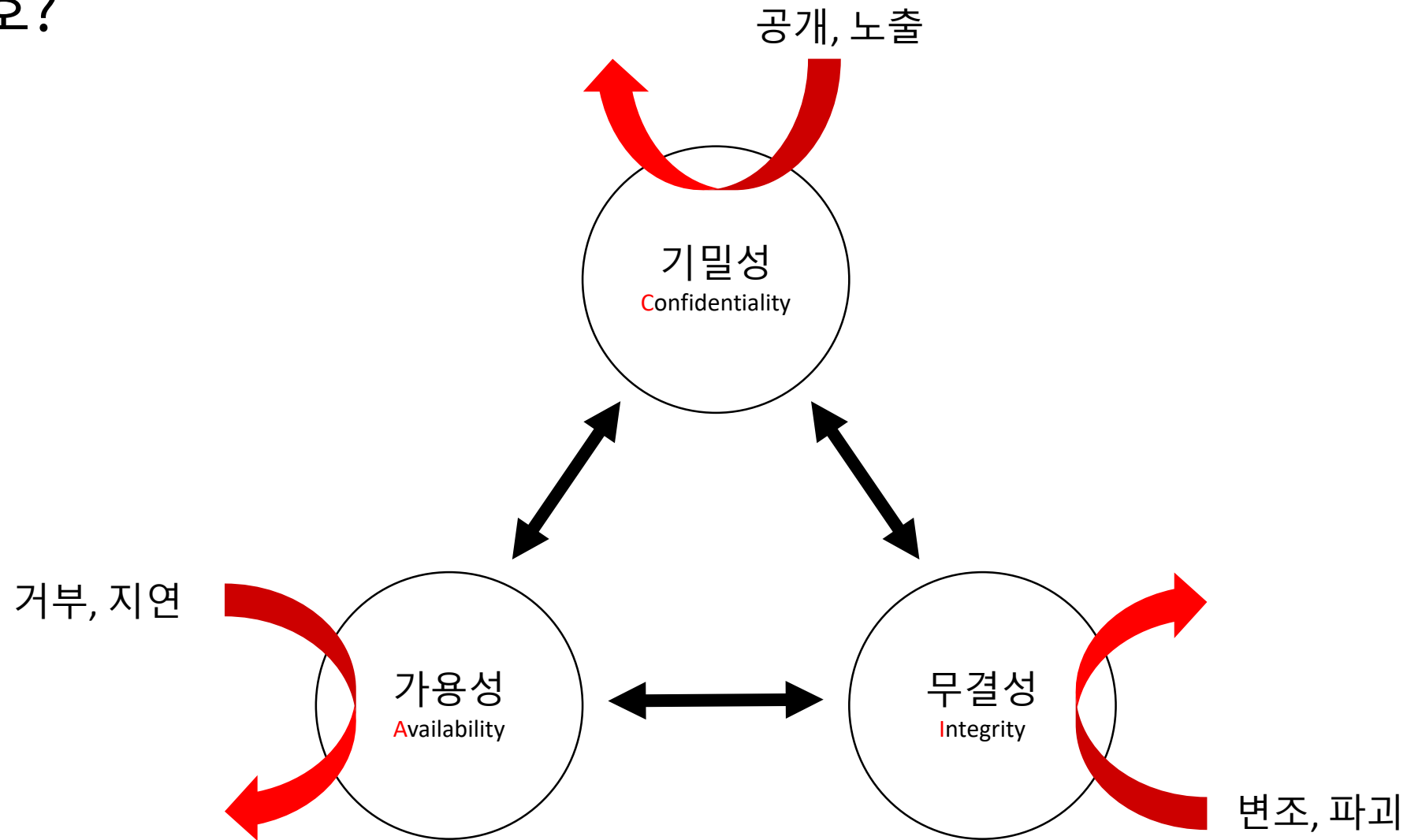
- 매주 이론 수업과 관련된 실습 진행
- 실습 관련 자료
  - <https://github.com/CNUCSE-InformationSecurity-2022-Fall>
- 매주 새로운 과제
- 언어는 **Python** 으로 진행합니다
- 인터넷 참고 가능, 그러나 복사는 0점
- 과제 제출 == 출석 인정
- 보고서 없음!

부정행위 절대엄금



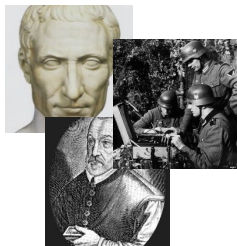
# 강의 소개 – 그래서 뭘 공부하나요?

- 정보보호?

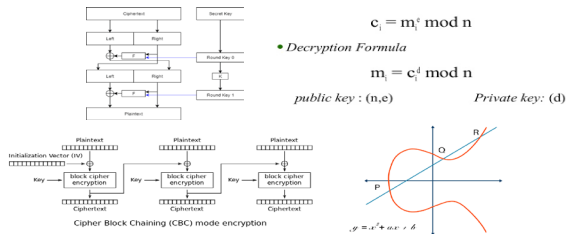


# 강의 소개 – 그래서 뭘 공부하나요?

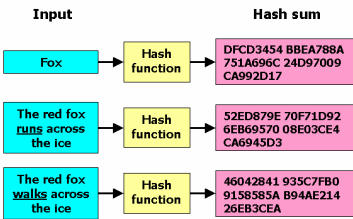
- 각종 암호 기술을 맛봅니다.



“고전암호”



“대칭 암호 vs 공개키 암호”



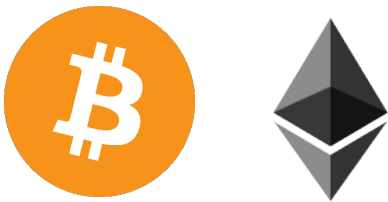
“해시”



“전자서명, 인증서”

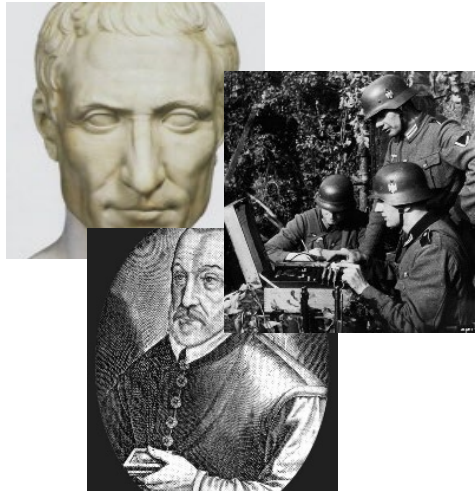


“키, 난수”



“블록체인”

# 강의 소개 – 그래서 뭘 공부하나요?

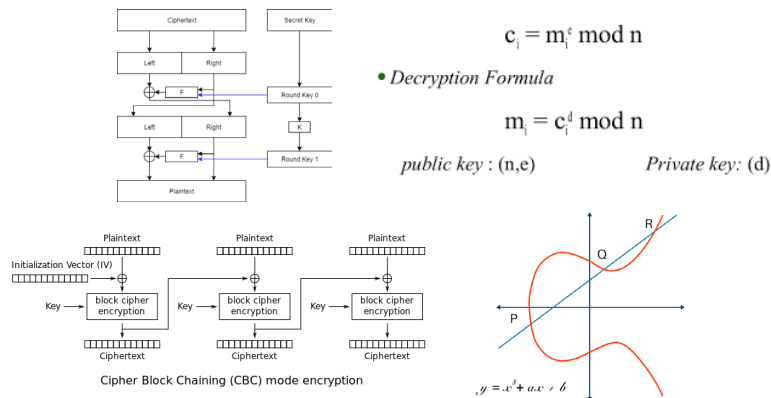


- 고전암호
- 옛날 사람들은 어떻게 암호를 만들고 썼나
- 지피지기면 백전불태 – 전쟁에 활용
- 이동암호, 치환암호
- 카이사르암호(시저암호), 비즈네르 암호

부록: ENIGMA

# 강의 소개 – 그래서 뭘 공부하나요?

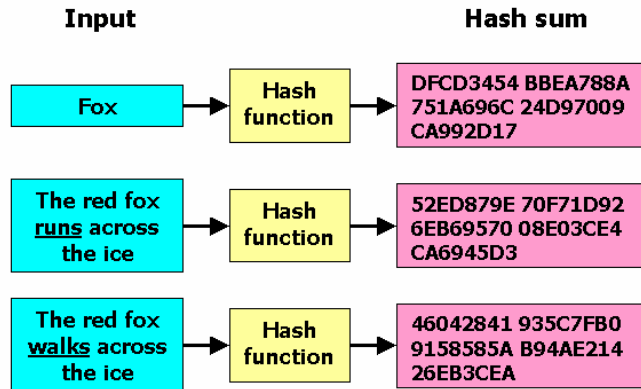
- 대칭키와 공개키 암호
- XOR암호와 One Time Pad
- DES, AES 블록 암호 – Feistel 구조와 S-Box
- 대칭키 암호 알고리즘의 운영 모드
- RSA, ECC 등 용도에 따라 키가 다른 공개키 암호



부록: **K-암호체계**(SEED, ARIA, ...), 랜섬웨어

# 강의 소개 – 그래서 뭘 공부하나요?

- 해시 알고리즘



- 데이터에 대한 특정한 단방향 연산
- 일정한 길이로 출력
- 비밀번호나 무결성 검증에 이용
- MAC을 이용한 메시지 인증
- 무결성 검증에 인증 같은걸 끼었나?

부록: 왜 MD5를 쓰면 안되나?

# 강의 소개 – 그래서 뭘 공부하나요?

- 전자서명과 인증서
- 이 정보는 내가 작성했습니다 (부인방지)
- 나만 아는 “개인키”로 암호화 하면?
- 그럼 이 “공개키”는 누구의 것?
- 신뢰 가능한 기관(CA)이 보증
- 인증서의 모습 – X.509



부록: 공인인증서



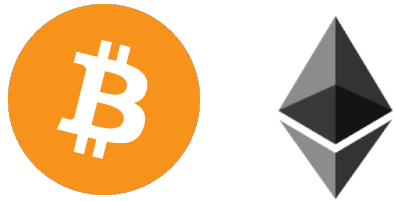
# 강의 소개 – 그래서 뭘 공부하나요?



- 키(Key)
- 암호를 더 안전하게 하기 위해
- 어떻게 관리해야?
- 난수
- 컴퓨터가 주사위를 던지는 방법
- 안전한 난수?

부록: QRNG

# 강의 소개 – 그래서 뭘 공부하나요?



- 블록체인
- 분산 아키텍처 기반의 탈중앙화 데이터베이스
- P2P 기반 네트워크
- 트랜잭션과 채굴
- 기깔나게 무결성을 검증하는 방법: 머클트리?

주차	실습 주제	과제	날짜
1	오리엔테이션 & 썰풀기	과제를 위한 GitHub 설정	9/7
2	카이사르&비즈네르 암호	ENIGMA	9/14
3	XOR과 블록암호	Simplified DES 구현하기	9/21
4	여러가지 블록암호	블록암호를 이용하여 암호통신기 완성하기	9/28
5	블록암호 운용모드	S-DES-CBC, S-DES-ECB 구현하기	10/5
6	RSA	RSA 구현하기, 저강도 RSA 크랙하기	10/12
7	해시	암호통신기에 무결성 검증 기능 추가하기	10/19
8	중 간 고 사 (10/24)		공강
9	메세지 인증코드(MAC)	HMAC 구현하기	11/2
10	디지털 서명	사실인증서 생성 및 프로그램 코드 서명	11/9
11	하이브리드 암호	하이브리드 기반 암호 통신기	11/16
12	난수	시드값 추측을 이용한 암호문 크랙	11/23
13	블록체인과 머클 트리	머클트리 구현하기	11/30
14	TLS와 PGP(GPG)	GPG를 이용하여 암호 메일 보내기	12/7
15	기 말 고 사 (12/12)		종강

# 금주 과?제

- GitHub 레포지토리 설정하기
- 안하면 이후 실습 죄다 0점!!!

Create a new repository


A repository contains all project files, including the revision history. Already have a project repository elsewhere? [Import a repository.](#)

Repository template

Start your repository with a template repository's contents.

No template ▾

Owner \*      Repository name \*

 0x0000FF ▾ / information-security-2022 ✓

Great repository names are short and memorable. Need inspiration? How about [sturdy-doodle?](#)

Description (optional)

정보보호 2022 실습용 레포지토리

☒ Public  
Anyone on the internet can see this repository. You choose who can commit.

☐ Private  
You choose who can see and commit to this repository.

ts   Actions   Projects   Wiki   Security   Insights   Settings

General

Access

Collaborators

Moderation options ▾

Code and automation

Actions ▾

Webhooks

Environments

Pages

Security

Code security and analysis

Deploy keys

Secrets ▾

Integrations

GitHub apps

Email notifications

Who has access

PUBLIC REPOSITORY

This repository is public and visible to anyone.

Manage

DIRECT ACCESS

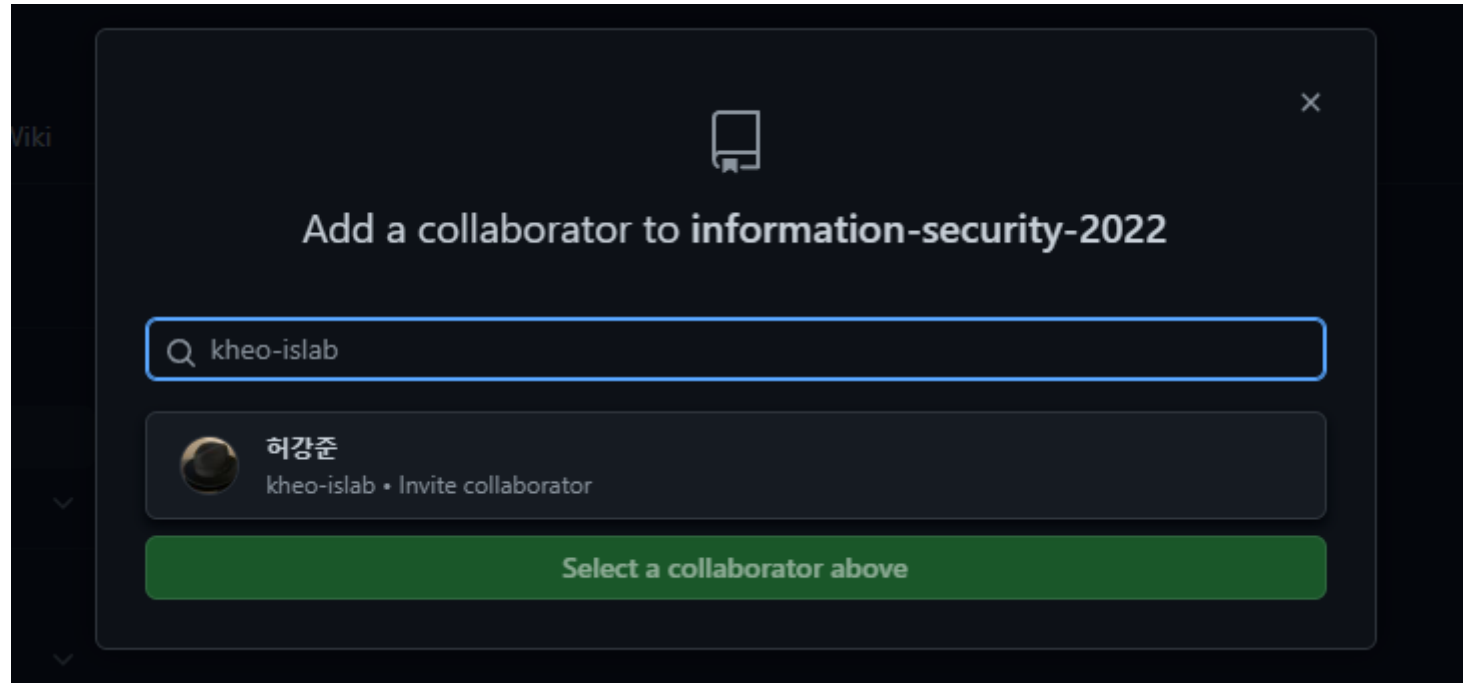
0 collaborators have access to this repository. Only you can contribute to this repository.

Manage access

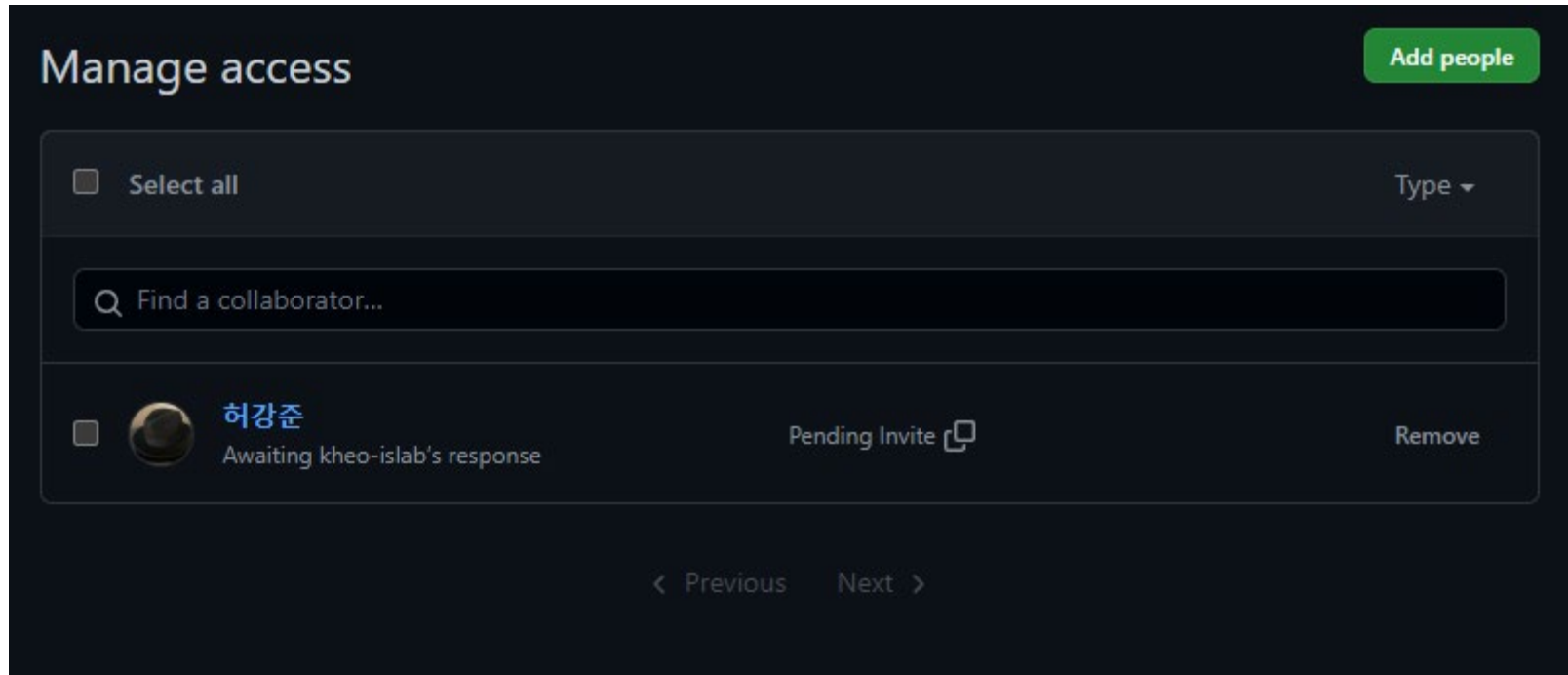
You haven't invited any collaborators yet

Add people

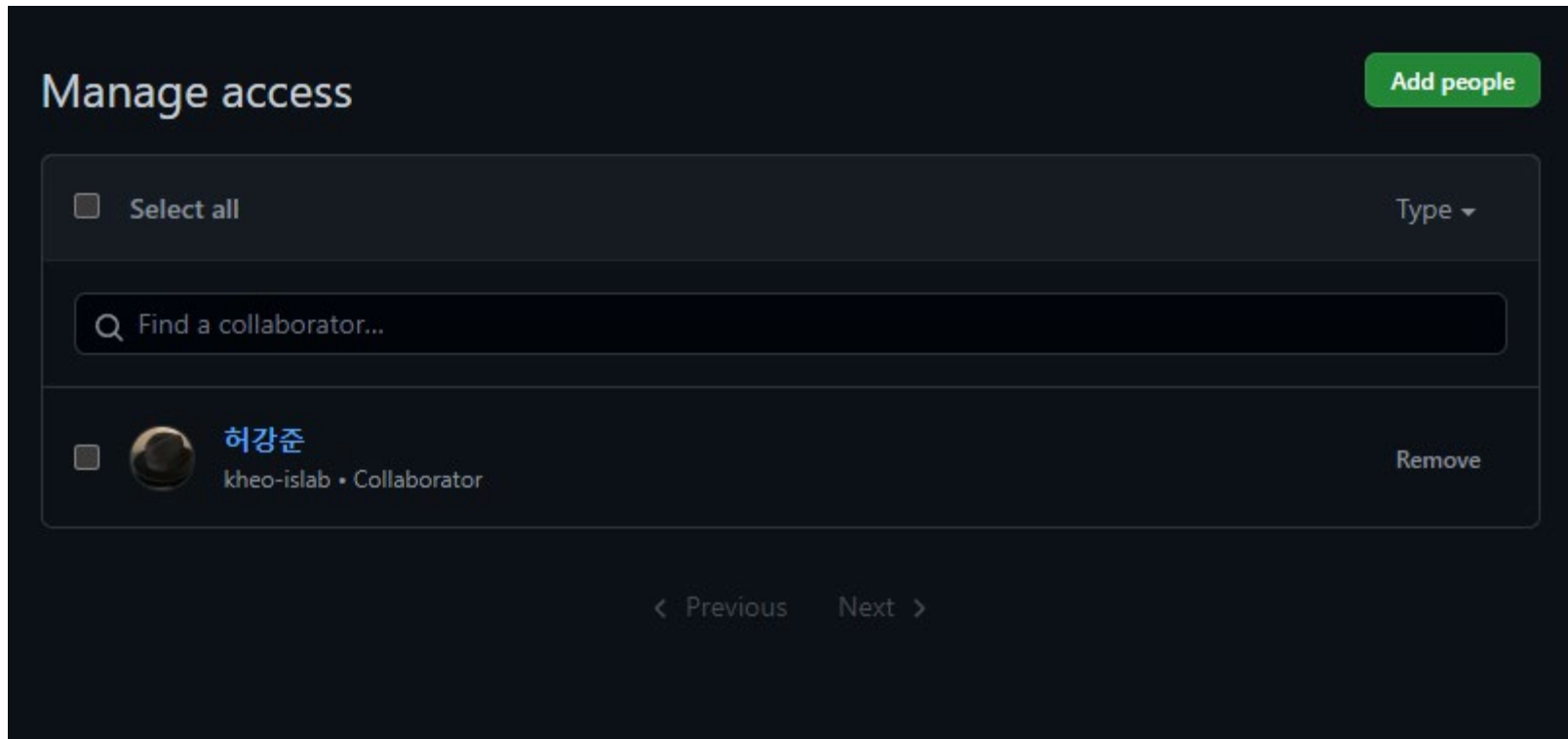
- GitHub 레포지토리 설정하기



- GitHub 레포지토리 설정하기



- GitHub 레포지토리 설정하기



## 질문?

- 없으면 자리에서 일어나셔도 좋습니다 :)
- 대학원 입학 문의는 언제나 환영