

하이브리드 암호

2022년 11월 16일 수요일

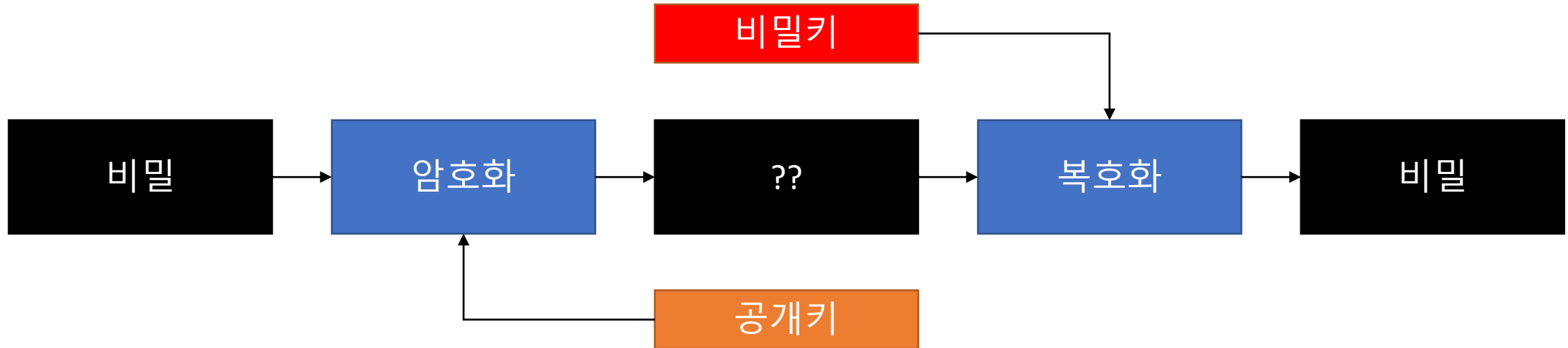
정보보호

충남대학교 정보보호연구실 허강준

- 대칭키암호 → 암호화 했던 키로 복호화가 가능



- 공개키암호 → 암호화와 복호화에 쓰는 키가 다름

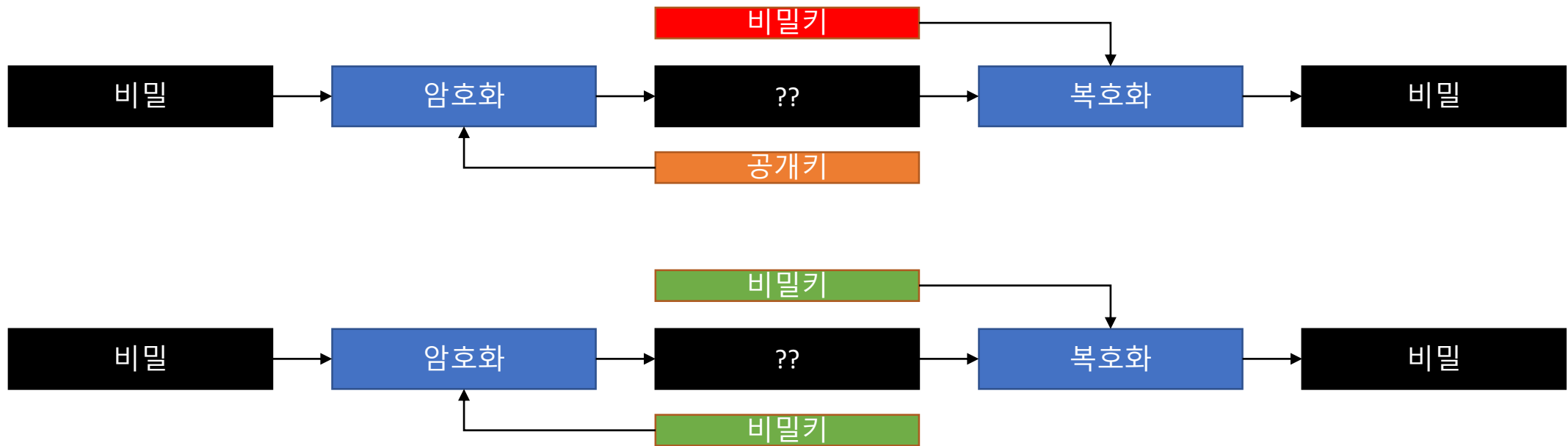


- 공개키암호 vs 대칭키 암호

	공개키암호	대칭키암호
키 종류	2가지 (공개키, 개인키)	1가지 (비밀키; secret)
키 길이 (비트)	1024~8192	128~256
성능	느림	빠름
평문 길이 제한	있음	없음

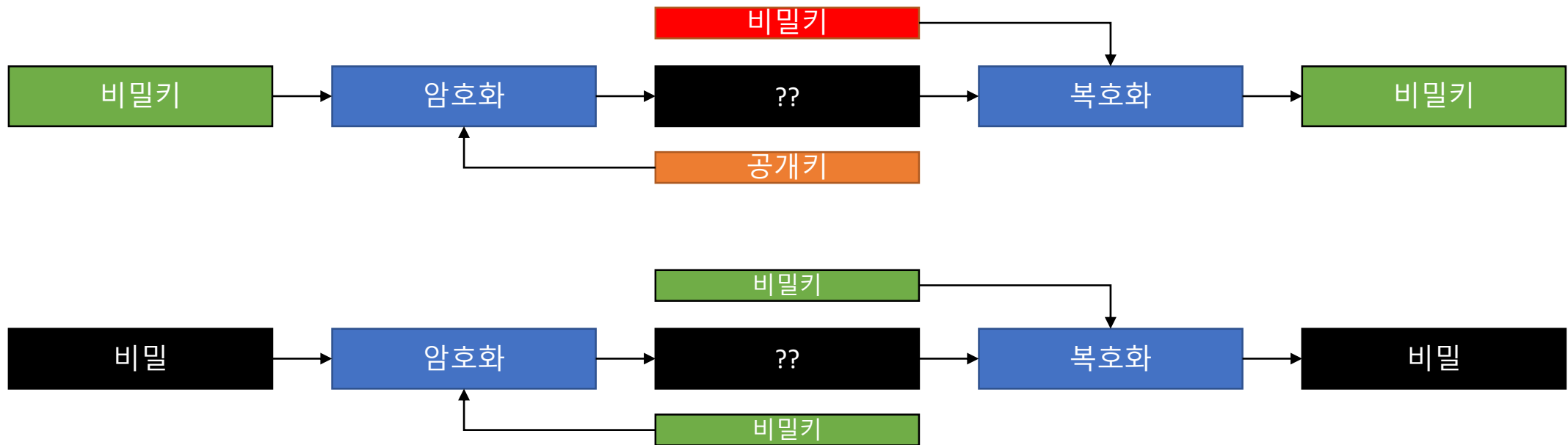
하이브리드 암호

- 공개키암호 → 강력하지만 느림
- 대칭키암호 → 빠르고 다용도로 활용 가능

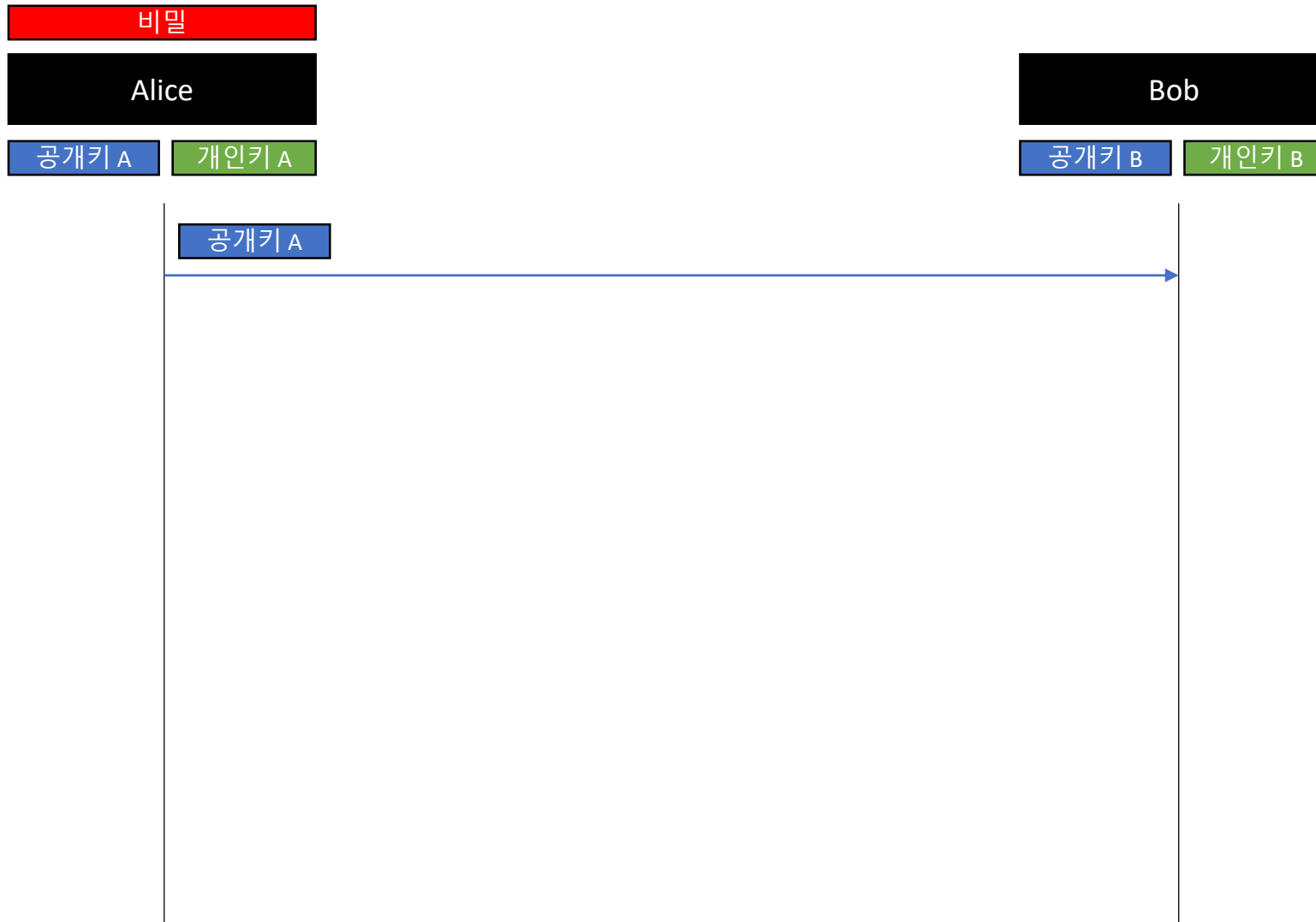


하이브리드 암호

- 공개키암호 → 강력하지만 느림
- 대칭키암호 → 빠르고 다용도로 활용 가능



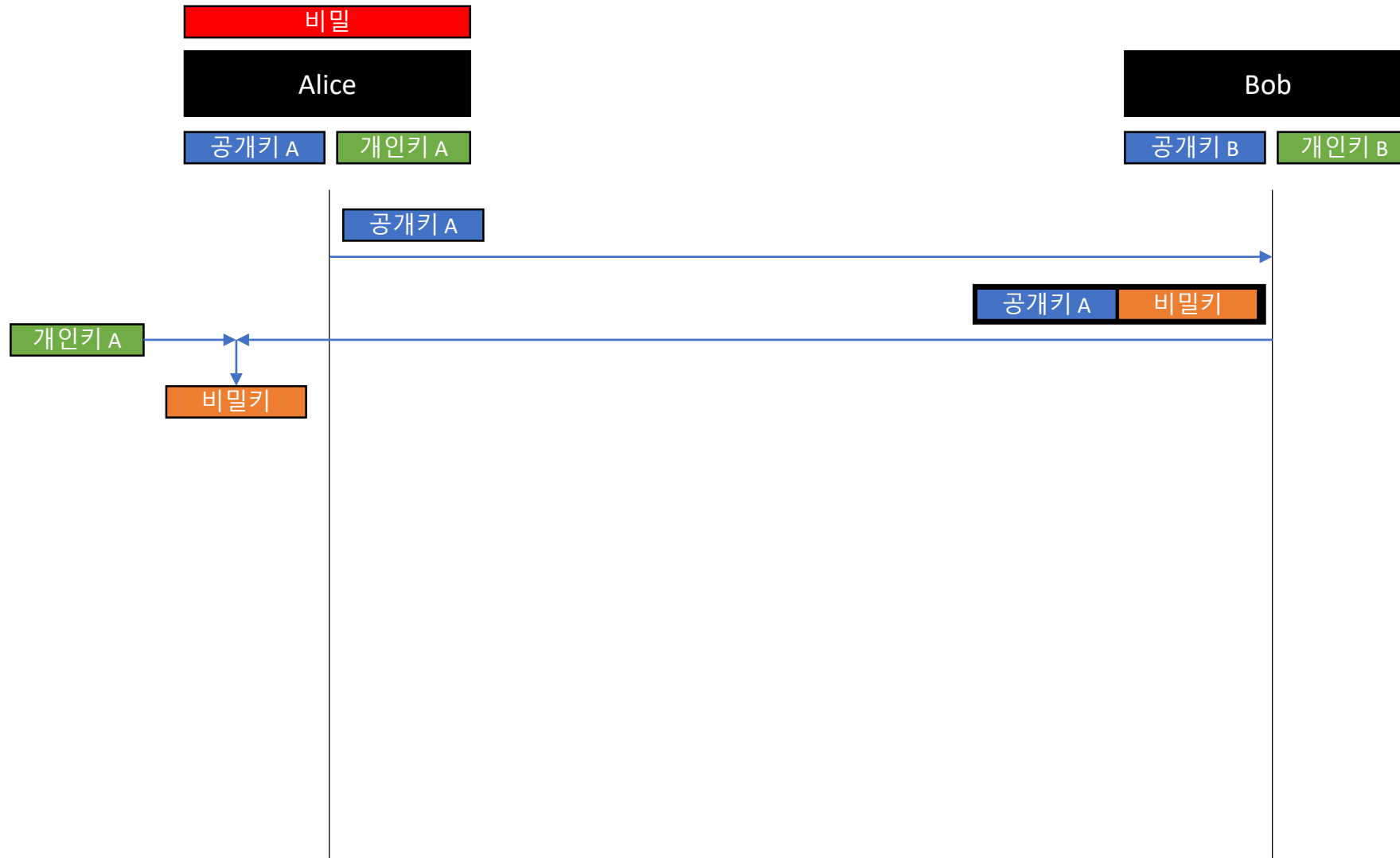
하이브리드 암호



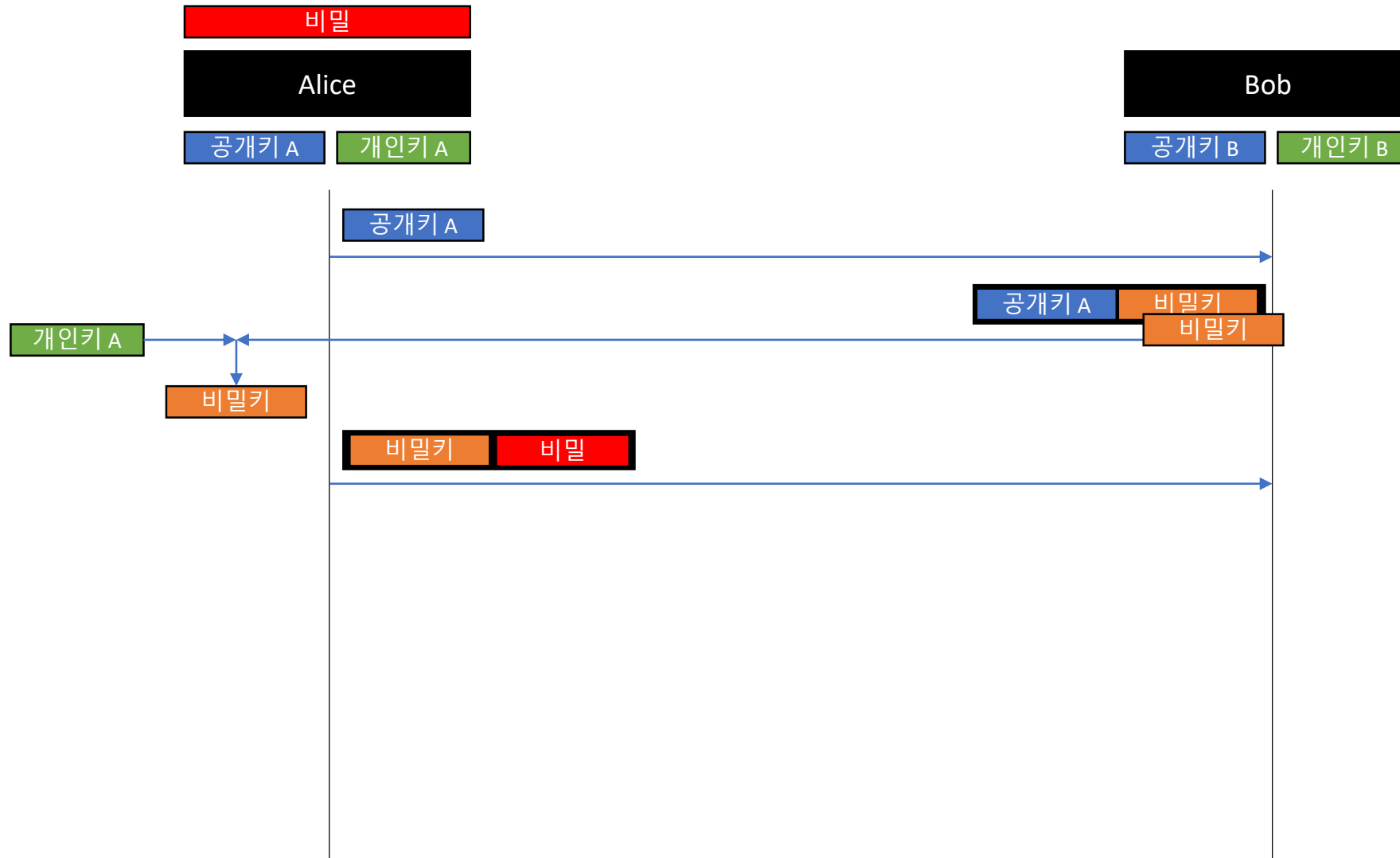
하이브리드 암호



하이브리드 암호



하이브리드 암호



하이브리드 암호



암호채팅 프로그램...

- End-to-End Encryption은 맞았는데...
- 서버가 키를 생성 및 보관

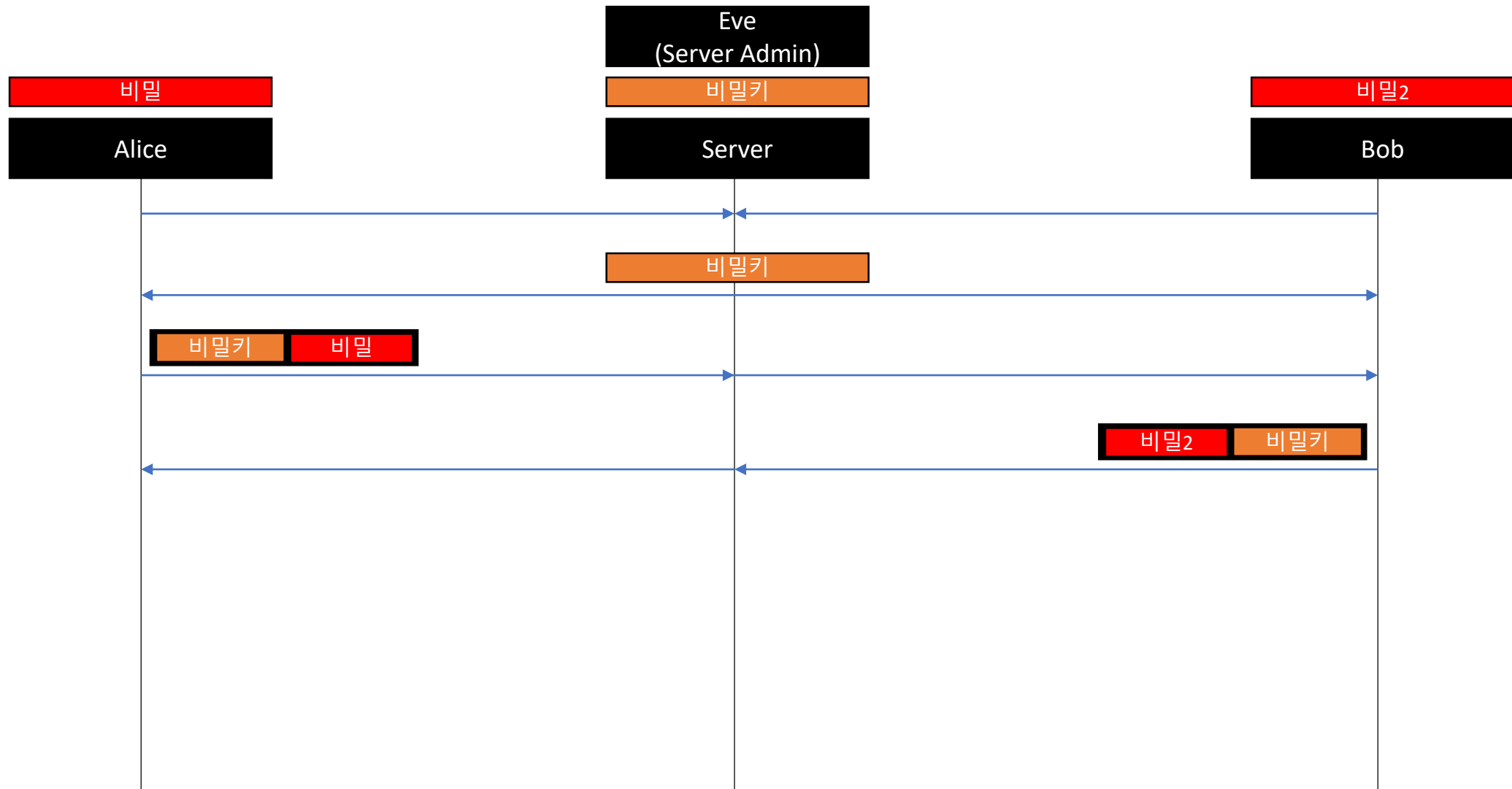
```
PS C:\Users\patche\Documents\GitHub\CipherCommunicator> python server.py
[*] Key generated: b'\xfc\xad\xdb\x73|9\xfd\xab\x93\xae\xee'
[*] Server started on 0.0.0.0:24000
[*] Accepted a connection from ('127.0.0.1', 6239)
[*] Accepted a connection from ('127.0.0.1', 6240)
('127.0.0.1', 6239): b'\xf8\xca0\xdb\xba\xef\xc3\xc5\xa3\xa77b\x9fg\xfo\xfb6b\x1d%\xafb*\x85H\xa9V\x0e\xba\xal\xca"\xc2\xa7b\xcew3\x9ei\x9b\xc1\x90\xc6\xa4Uf'\x1f\xcdjf\x10\xcb\xa1\xec\x97A)\xe9\xa5\x8c\xe4o\x1b'
Broadcast_send: ('127.0.0.1', 6240)
('127.0.0.1', 6240): b'\xef\x84\xc3\x179\x8d\t\xcd\x02o\x88E\xd3\xff\x02\xf9\xa8?_\xc7M\x0b\x98<\xf7\x8c\xa7k\xcf\xc5\xee{g\r00b\x0b\xda\x94\x8f\xf6\x84\x0bw\x08\x1f'
Broadcast_send: ('127.0.0.1', 6239)

PS C:\Users\patche\Documents\GitHub\CipherCommunicator> python client.py
[*] connected to 127.0.0.1:24000, Receiving an encryption key...
[*] Key received: b'\xfc\xad\xdb\x73|9\xfd\xab\x93\xae\xee'
[*] Now a chatting session is starting...
Message: 이건 비밀인데 서버 주인은 절대 모를걸 ㅋㅋ
Me: 이건 비밀인데 서버 주인은 절대 모를걸 ㅋㅋ
Message:
Received: 원데? 나한테만 말해보셈 🤔

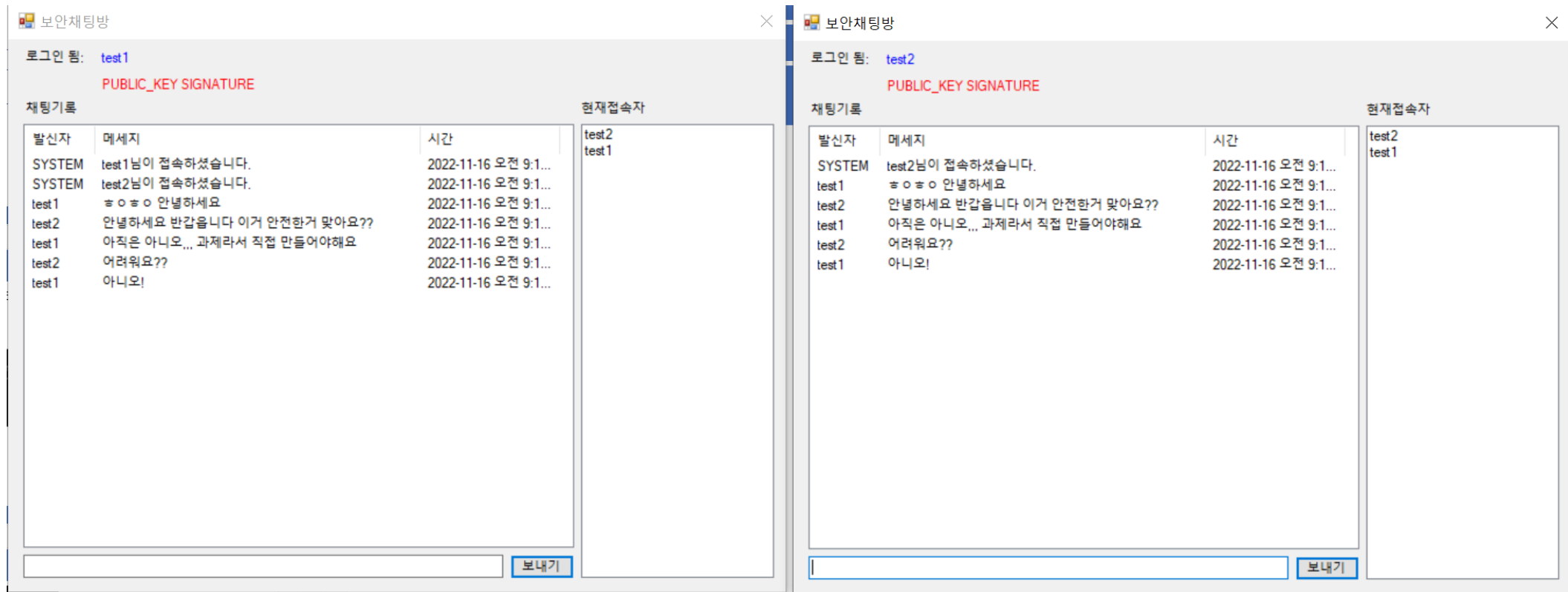
Windows PowerShell

PS C:\Users\patche\Documents\GitHub\CipherCommunicator> python client.py
[*] connected to 127.0.0.1:24000, Receiving an encryption key...
[*] Key received: b'\xfc\xad\xdb\x73|9\xfd\xab\x93\xae\xee'
[*] Now a chatting session is starting...
Message:
Received: 이건 비밀인데 서버 주인은 절대 모를걸 ㅋㅋ
원데? 나한테만 말해보셈 🤔
Me: 원데? 나한테만 말해보셈 🤔
Message: |
```

암호채팅 프로그램...

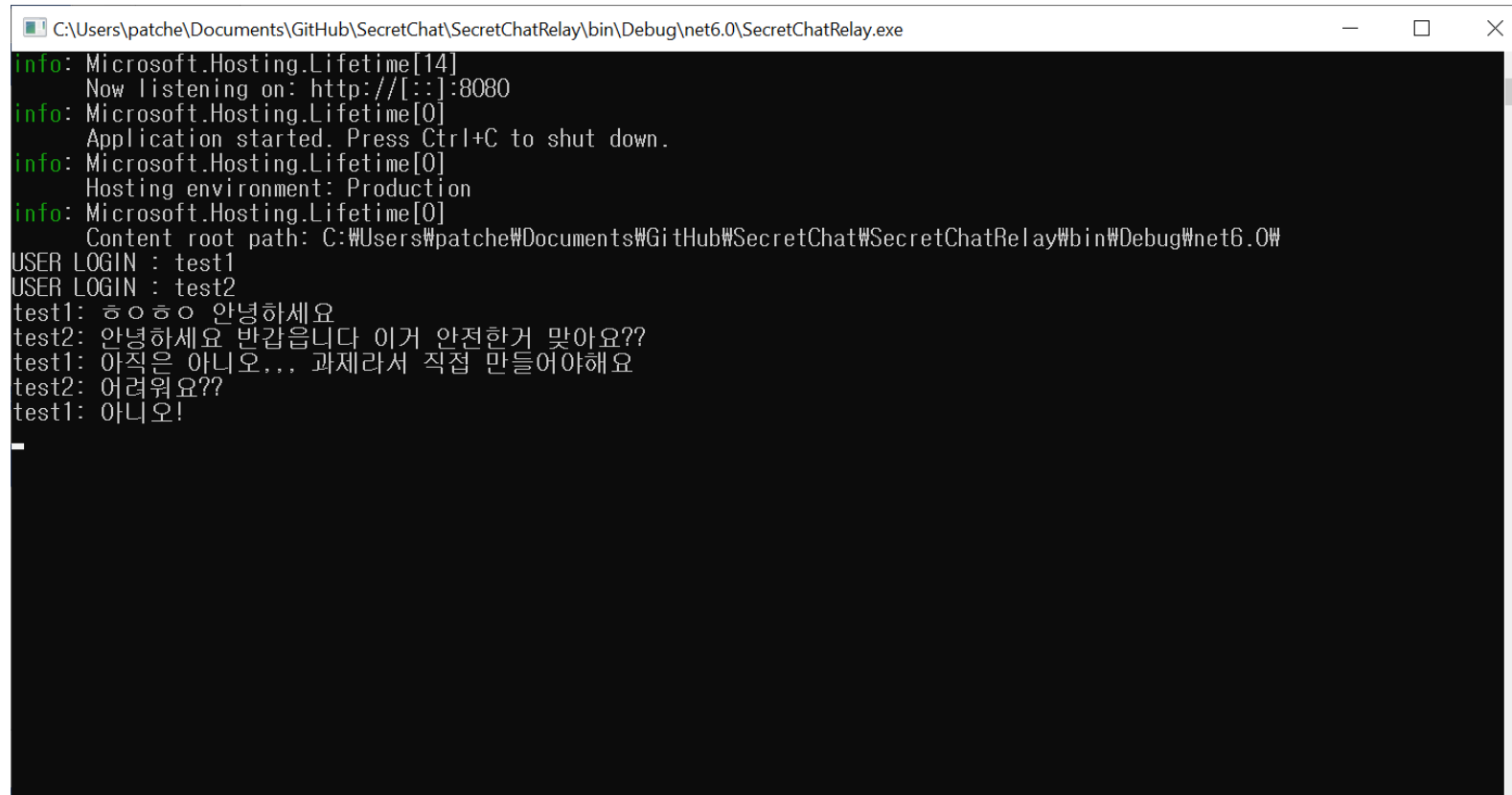


암호채팅 프로그램... (진짜)



암호채팅 프로그램... (진짜)

- 서버에서는 더이상 키를 보관하지 않음!
- 서버 주소는 카카오톡 알림톡으로 전파



```
C:\Users\pathe\Documents\GitHub\SecretChat\SecretChatRelay\bin\Debug\net6.0\SecretChatRelay.exe
info: Microsoft.Hosting.Lifetime[14]
      Now listening on: http://[::]:8080
info: Microsoft.Hosting.Lifetime[0]
      Application started. Press Ctrl+C to shut down.
info: Microsoft.Hosting.Lifetime[0]
      Hosting environment: Production
info: Microsoft.Hosting.Lifetime[0]
      Content root path: C:\Users\pathe\Documents\GitHub\SecretChat\SecretChatRelay\bin\Debug\net6.0\
USER LOGIN : test1
USER LOGIN : test2
test1: ㅎㅎㅎ 안녕하세요
test2: 안녕하세요 반갑습니다 이거 안전한거 맞아요??
test1: 아직은 아니오... 과제라서 직접 만들어야해요
test2: 어려워요??
test1:아니오!
```

암호채팅 프로그램... (진짜)

- 채팅 기본 기능 및 여러 복잡한 기능은 전부 만들어져 있음
- 직접 해야 하는 것들: 키 생성, 암호화, 복호화, 해시 등...

보안채팅: 닉네임을 입력하세요...

조교 허강준

http://[색상바]/chat

로그인

보안채팅방

로그인 됨: test1

PUBLIC_KEY SIGNATURE

채팅기록

발신자	메세지	시간
SYSTEM	test1님이 접속하셨습니다.	2022-11-16 오전 9:1...
SYSTEM	test2님이 접속하셨습니다.	2022-11-16 오전 9:1...
test1	ㅇㅇㅇㅇ 안녕하세요	2022-11-16 오전 9:1...
test2	안녕하세요 반갑습니다 이거 안전한거 맞아요??	2022-11-16 오전 9:1...
test1	아직은 아니오... 과제라서 직접 만들어야해요	2022-11-16 오전 9:1...
test2	어려워요??	2022-11-16 오전 9:1...
test1	아니오!	2022-11-16 오전 9:1...
SYSTEM	test2님이 나가셨습니다.	2022-11-16 오전 9:1...

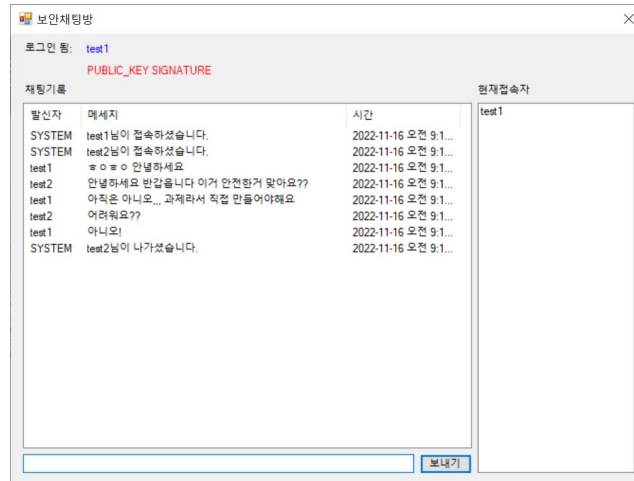
현재접속자

test1

보내기

암호채팅 프로그램... (진짜)

클라이언트: 기본 기능 완성



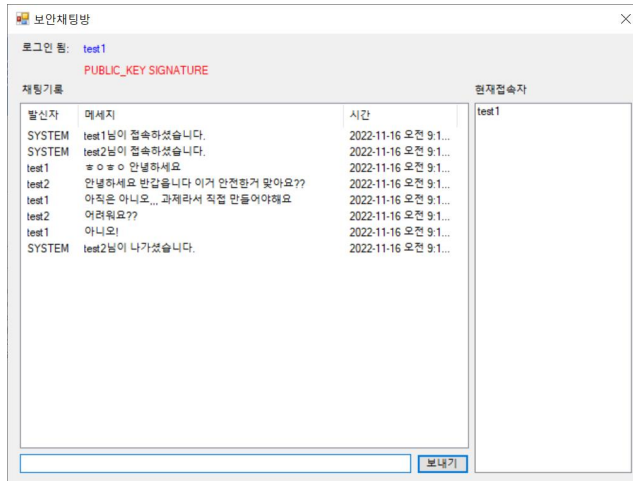
과제로 구현해야 할 것들 (예시)

- python-scripts
- certification
- generate-keys
- hash-mac
- public-key-crypto
- symmetric-key-crypto

서버: 조교가 직접 운영함 별도 실행 필요 없음

```
C:\Users\patche\Documents\GitHub\SecretChat\SecretChatRelay\bin\Debug\net6.0\SecretChatRelay.exe
info: Microsoft.Hosting.Lifetime[14]
      Now listening on: http://[::]:8080
info: Microsoft.Hosting.Lifetime[0]
      Application started. Press Ctrl+C to shut down.
info: Microsoft.Hosting.Lifetime[0]
      Hosting environment: Production
info: Microsoft.Hosting.Lifetime[0]
      Content root path: C:\Users\patche\Documents\GitHub\SecretChat\SecretChatRelay\bin\Debug\net6.0\
USER LOGIN : test1
USER LOGIN : test2
test1: ㅎㅇㅎㅇ 안녕하세요
test2: 안녕하세요 반갑습니다. 이거 안전한거 맞아요??
```

암호채팅 프로그램... (진짜)



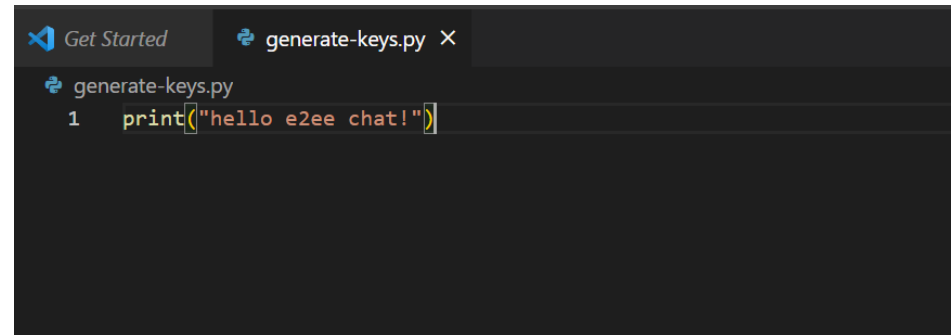
Python 실행

print 로 결과 출력 및 전송

- python-scripts
- certification
- generate-keys
- hash-mac
- public-key-crypto
- symmetric-key-crypto

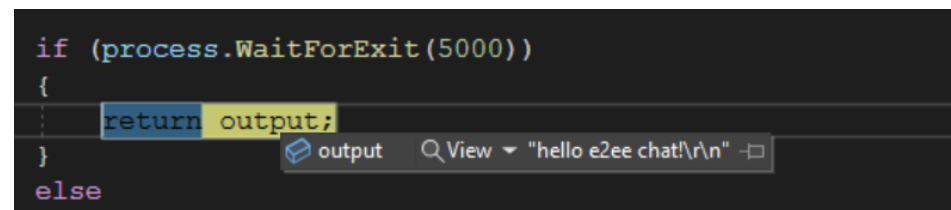
암호채팅 프로그램... (진짜)

파이썬 코드



```
Get Started generate-keys.py X
generate-keys.py
1 print("hello e2ee chat!")
```

채팅 프로그램



```
if (process.WaitForExit(5000))
{
    return output;
}
else
```

output View "hello e2ee chat!\\n"

암호채팅 프로그램... (진짜)

- 13주차까지 완성 목표
- 채팅 프로그램은 소스코드가 공개되어 있음
 - 바로 실행 가능하도록 실행파일도 배포됨
- 매주 구현해야 할 기능 및 스크립트 이름은 레포에 명시
- 이번주:
 - 공개키/개인키, 비밀키 생성
 - 공개키 암호를 이용한 비밀키 암호화 및 복호화
 - 대칭키 암호를 이용한 평문 암호화 및 복호화

주차	실습 주제	과제	날짜
1	오리엔테이션 & 쉘풀기	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	해사	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 암호 기반 암호 통신기 (시작)	11/16
12	난수와 디지털서명	하이브리드 암호 기반 암호 통신기 (2)	11/23
13	메세지 인증	하이브리드 암호 기반 암호 통신기 (3)	11/30
14	통신기 검증 & TLS와 PGP(GPG)	GPG를 이용하여 암호 메일 보내기	12/7
15	기 말 고 사 (12/12)		종강

질문?

- 없으면 자리에서 일어나셔도 좋습니다 :)
- **대학원 입학 문의**는 언제나 환영
 - 블록체인, Web 3, 해킹 관심있거나 유경험자 우대

입학문의

- 류재철 교수님 (jcryou [at] cnu.ac.kr)
- 허강준 조교 (knowledge [at] o.cnu.ac.kr)