정보보호

채팅 프로그램

정보보호 연구실

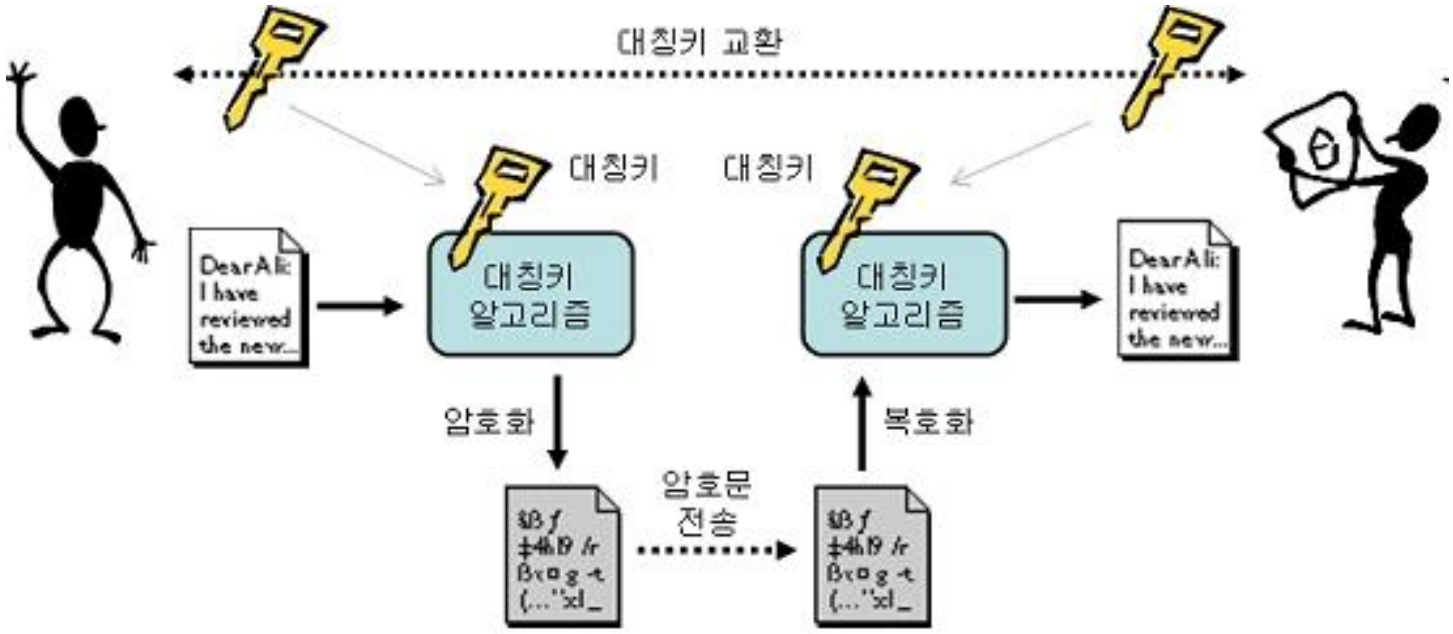
이동섭

ISLAB
INFORMATION SECURITY LABORATORY CNU

대칭키

■ 대칭키 암/복호화 방식

▶ 암호화에 사용되는 키와 복호화에 사용되는 키가 같음



실습 과제

1:1 통신

■ 예시 화면

▶ 서버

– 방 생성 및 키 전송

▶ 클라이언트

– 방 입장

```
(base) dajaba@dajaba:~/lab/04$ python server.py
key exchange Success
iv exchange Success
Connection from: ('127.0.0.1', 60072)
Recieved from user2 : hi
 -> hihi
Recieved from user2 : how are you today
 -> i;m good
Recieved from user2 : okey
 -> good
(base) dajaba@dajaba:~/lab/04$
```

```
(base) dajaba@dajaba:~/lab/04$ python client.py
key : thisisbadkeyokeythisisbadkeyokey
iv  : ivisinitialvetor
 -> hi
Received from user1 : hihi
 -> how are you today
Received from user1 : i;m good
 -> okey
Received from user1 : good
 -> bye
```

실습 과제

1:1 통신

■ 코드 : server.py

```python
import socket


def server_program():
    host = '127.0.0.1'
    port = 5462

    key = 'thisisbadkeyokeythisisbadkeyokey'
    iv = 'ivisinitialvetor'

    server_socket = socket.socket()
    server_socket.bind((host, port))

    server_socket.listen(2)
    conn, address = server_socket.accept()
    conn.send(key.encode())
    print(conn.recv(1024).decode())
    conn.send(iv.encode())
    print(conn.recv(1024).decode())

    print("Connection from: " + str(address))


    while True:
        rdata = conn.recv(1024)
        if not rdata:
            break
        data = rdata.decode()
        print("Recieved from user2 : " + str(data))
        data = input(' -> ')
        conn.send(data.encode())

    conn.close()


if __name__ == '__main__':
    server_program()
```

실습 과제

1:1 통신

■ 코드 : client.py

```python
import socket

def client_program():
    host = '127.0.0.1'
    port = 5462

    keyRecive = False
    client_socket = socket.socket()
    client_socket.connect((host, port))

    if(keyRecive == False):
        key = client_socket.recv(1024).decode()
        print('key : ' + key)
        client_socket.send('key exchange Success'.encode())
        iv = client_socket.recv(1024).decode()
        print('iv  : ' + iv)
        client_socket.send('iv exchange Success'.encode())
        keyRecive = True


    if(keyRecive):
        message = input(" -> ")
        while message.lower().strip() != 'bye':
            client_socket.send(message.encode())
            data = client_socket.recv(1024)
            data = data.decode()
            print('Received from user1 : ' + data)

            message = input(" -> ")
    client_socket.close()


if __name__ == '__main__':
    client_program()
~
```

실습 과제

1:1 통신

■ 코드 : MCipher.py

```
from Crypto.Cipher import AES

BS =
pad =
unpad =

def setAES(key, iv):
    #TODO SET AES

    return

def AES_Encrypt(cipher, data):
    #TODO DATA ENCRYPT

    return

def AES_Decrypt(cipher, data):
    #TODO DATA DECRYPT

    return
```

제출 요령

- **보고서 (*.pdf)**
  - 문서는 PDF로 변환하여 제출
  - 과제 해결 과정
    - 과제를 어떻게 이해했는지
    - 어떻게 해결했는지

- **소스코드 (*.py)**
  - 과제 해결에 작성한 코드

❖ 소스코드

1) 실습 부분 코드

- 코드 분석

- 1:1 암호화 통신