CNU 충남대학교 CHUNGNAM NATIONAL UNIVERSITY

REPORT

정보보호 00 반

채팅 프로그램

이름	정진욱
학과	컴퓨터공학과
학번	201602071
과목	정보보호
교수님	류재철 교수님

1. 과제 이해

이번 과제는 자난 과제에서 이용했던 pycrypto 모듈의 AES 를 사용하여 네트워크를 통한 메시지 발신/수신 시 CBC 암호/복호화를 수행하는 것입니다.

AES_CBC 는 블록 암호 방식의 암호화/복호화를 진행하므로 짧은 메시지를 암호화/복호화하기에 알맞습니다.

2. 과제 구현

a. Server 및 Client

```python
#!/usr/bin/python3
import socket
import MCipher as MCipher

def server_program():
 host = '127.0.0.1'
 port = 5461

 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())
 cipher = MCipher.setAES(key, iv)

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

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

 conn.close()


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

```python
#!/usr/bin/python3
import socket
import MCipher as MCipher

def client_program():
 host = '127.0.0.1'
 port = 5461

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

 if(keyReceive == 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())
  keyReceive = True
  cipher = MCipher.setAES(key, iv);

  if(keyReceive):
   message = input(' -> ')
   while message.lower().strip() != 'bye':
    client_socket.send(MCipher.AES_Encrypt(cipher, message))
    data = client_socket.recv(1024)
    data = MCipher.AES_Decrypt(cipher, data).decode()
    print('Received from user1 : ' + data)

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

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

Server 및 Client 파일입니다. Server 및 Client 에서 각각 전송 시 암호화, 수신 시 복호화 처리를 해 두었습니다.

b. MCipher

```python
#!/usr/bin/python3
from Crypto.Cipher import AES

BS = 16
pad = lambda s : s + (BS - len(s) % BS) * chr(BS - len(s) % BS)
unpad = lambda s : s[:-ord(s[len(s)-1:])]

def setAES(key, iv):
 cipher = AES.new(key, AES.MODE_CBC, iv)#counter = lambda :
 return cipher

def AES_Encrypt(cipher, data):
 message = pad(data)
 return cipher.encrypt(message)

def AES_Decrypt(cipher, data):
 return unpad(cipher.decrypt(data))
```

MCipher는 암호화/복호화를 담당하는 파이썬 모듈로, AES 객체를 만들고, 해당 객체를 받아서 Encrypt, Decrypt 하는 역할을 수행합니다.

3. 실행 결과