CNU 충남대학교 CHUNGNAM NATIONAL UNIVERSITY

REPORT

정보보호 00 반

블록암호

이름	정진욱
학과	컴퓨터공학과
학번	201602071
과목	정보보호
교수님	류재철 교수님

1. 과제 이해

이번 과제는 pycrypto 모듈의 AES 를 이용하여 CBC, CTR 암호/복호화를 구현하는 것입니다.

AES_CBC 는 iv 및 key 를 이용하고, AES_CTR 은 counter 및 key 를 이용한다는 점에서 다르며,

CBC 의 경우 블록 암호 방식의 암호화/복호화를 진행하지만 CTR 의 경우 카운터 방식을 사용하여 블록 암호를 스트림 암호로 바꿉니다.

2. 과제 구현

a. AES_CBC

```
def crypto(mode, fileName):
 keyValue = ''
 iv = 'fdasafdsfdasfdas'
 key = 'thisisbadkeyokey'
 outputFileName = 'encrypt.txt'
 if mode[0] is 'd':
  outputFileName = 'decrypt.txt'

 translated = ''
 outputFile = open(outputFileName, 'wb')

 inputFile = open(fileName, 'rb')
 message = inputFile.read()
 ######
 obj = AES.new(key, AES.MODE_CBC, iv)
 translated = b''
 if mode[0] is 'e':
  translated = obj.encrypt(message)
 elif mode[0] is 'd':
  translated = obj.decrypt(message)
 ######
 outputFile.write(translated)
 outputFile.close()
 inputFile.close()
 print('En(De)cryption complete')
```

AES_CBC 의 crypto 함수는 위와 같이 만들었습니다.

Pycrypto 모듈의 AES 를 이용하여(from Crypto.Cipher import AES) ‘e’일 경우 encrypt, ‘d’일 경우 decrypt 하였습니다.

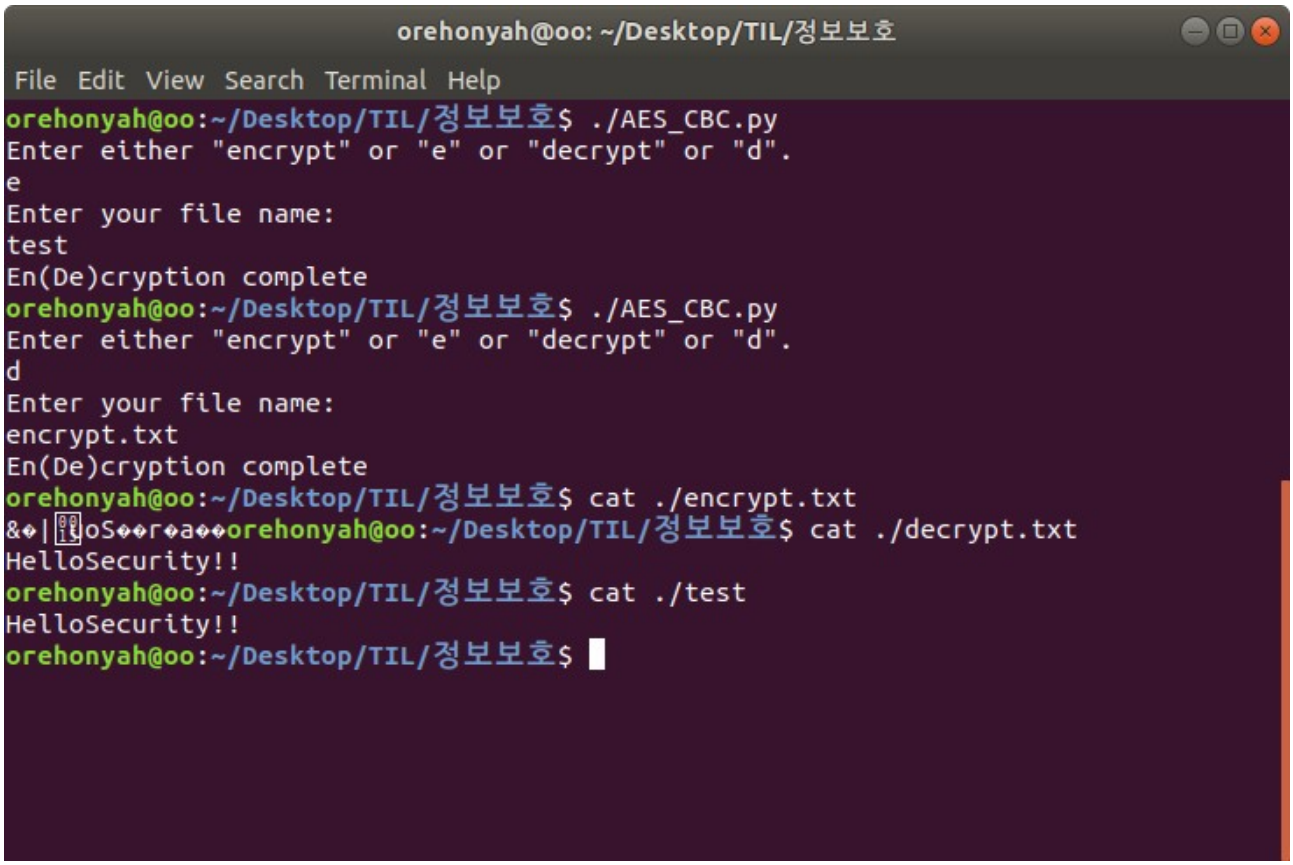
b. AES_CTR

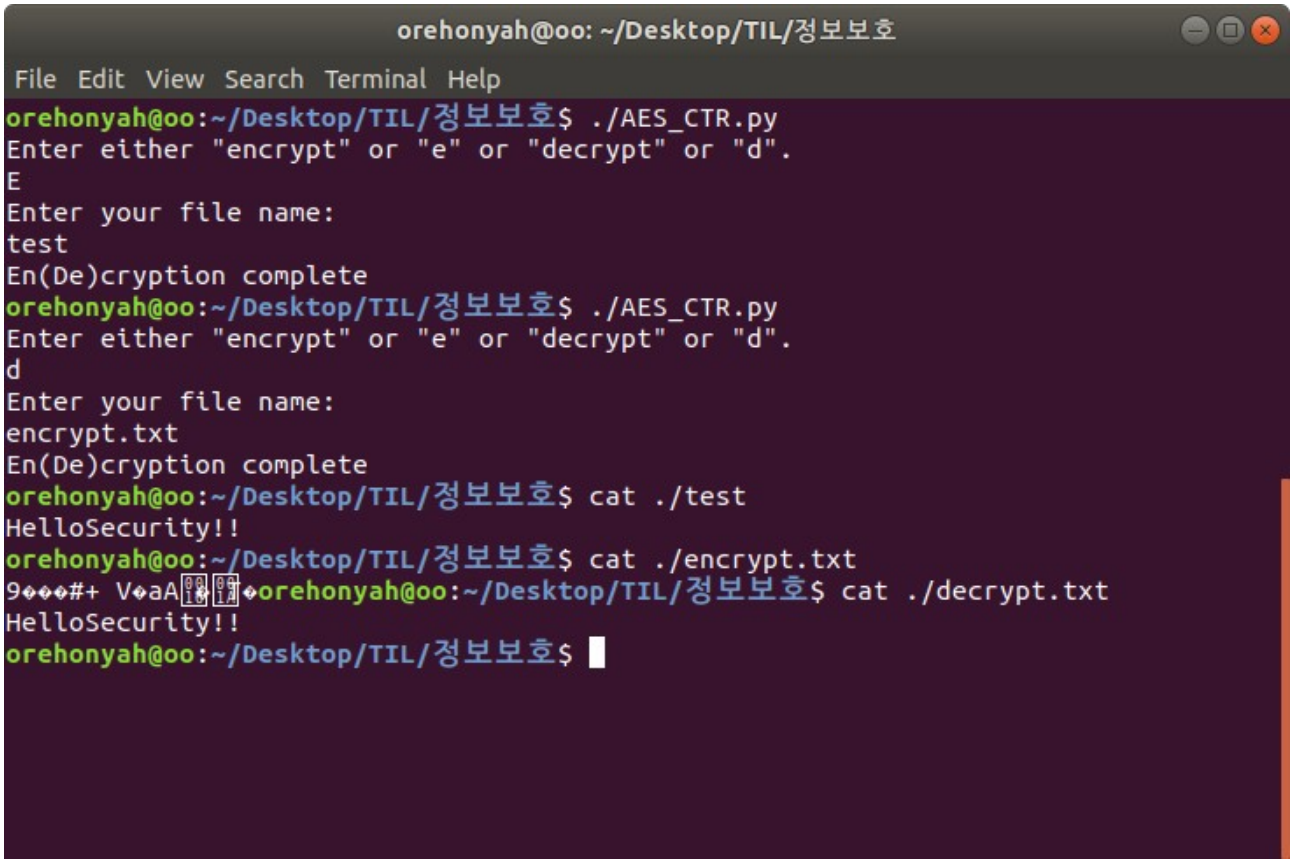
AES_CTR 의 경우 counter 를 써야 합니다.

```
def crypto(mode, fileName):
 keyValue = ''
 iv = b'fdasafdsfdasfdas'
 key = 'thisisbadkeyokey'
 outputFileName = 'encrypt.txt'
 if mode[0] is 'd':
  outputFileName = 'decrypt.txt'

 translated = ''
 outputFile = open(outputFileName, 'wb')

 inputFile = open(fileName, 'rb')
 message = inputFile.read()
 ######
 obj = AES.new(key, AES.MODE_CTR, counter = lambda : iv)
 translated = b''
 if mode[0] is 'e':
  translated = obj.encrypt(message)
 elif mode[0] is 'd':
  translated = obj.decrypt(message)
 ######
 outputFile.write(translated)
 outputFile.close()
 inputFile.close()
 print('En(De)cryption complete')
```

따라서 iv 를 함수 형태로 변환시켜 넣어주었습니다.

3. 실행 결과


orehonyah@oo: ~/Desktop/TIL/정보보호
File Edit View Search Terminal Help
orehonyah@oo:~/Desktop/TIL/정보보호$ ./AES_CBC.py
Enter either "encrypt" or "e" or "decrypt" or "d".
e
Enter your file name:
test
En(De)cryption complete
orehonyah@oo:~/Desktop/TIL/정보보호$ ./AES_CBC.py
Enter either "encrypt" or "e" or "decrypt" or "d".
d
Enter your file name:
encrypt.txt
En(De)cryption complete
orehonyah@oo:~/Desktop/TIL/정보보호$ cat ./encrypt.txt
&|oS r a orehonyah@oo:~/Desktop/TIL/정보보호$ cat ./decrypt.txt
HelloSecurity!!
orehonyah@oo:~/Desktop/TIL/정보보호$ cat ./test
HelloSecurity!!
orehonyah@oo:~/Desktop/TIL/정보보호$


orehonyah@oo: ~/Desktop/TIL/정보보호
File Edit View Search Terminal Help
orehonyah@oo:~/Desktop/TIL/정보보호$ ./AES_CTR.py
Enter either "encrypt" or "e" or "decrypt" or "d".
E
Enter your file name:
test
En(De)cryption complete
orehonyah@oo:~/Desktop/TIL/정보보호$ ./AES_CTR.py
Enter either "encrypt" or "e" or "decrypt" or "d".
d
Enter your file name:
encrypt.txt
En(De)cryption complete
orehonyah@oo:~/Desktop/TIL/정보보호$ cat ./test
HelloSecurity!!
orehonyah@oo:~/Desktop/TIL/정보보호$ cat ./encrypt.txt
9 #+ V aA orehonyah@oo:~/Desktop/TIL/정보보호$ cat ./decrypt.txt
HelloSecurity!!
orehonyah@oo:~/Desktop/TIL/정보보호$