대칭키 암호 프로그래밍 실습

PYCRYPTO

- 설치

```
$ sudo apt install python3-pip
$ sudo pip3 install pycrypto
```

- 지원 대칭 암호
  - AES
  - ARC2
  - Blowfish
  - CAST
  - DES
  - DES3
  - IDEA
  - RC5

기본 사용법

- import

  from Crypto.Cipher import [암호알고리즘]

- 암복호기 constructor

  new ([key], [mode], [iv])

- 암복호

  encrypt ("평문")

  decrypt ("암호문")

AES 기본

```
$ python3  AES.py
```

- 키 길이는 16, 24, 32 bytes 중 하나
- Initial vector 는 블록 사이트 (=16 bytes)
- 메시지 길이는 블록 사이즈 (16 byte) 의 배수
  - 부족분은 padding 으로 채워야

과제1

- AES.py 코드를 수정 하시오
  - 메시지를 입력 받아, 즉시 암호화하여 출력하고
    - Str -> bitearrary : str.encode('ascii') or 'utf-8'
    - 메시지가 짧으면 암호문도 짧아야 함
    - Padding 사용 안함
    - 여기에 적합한 모드 사용해야
  - 복호화된 결과를 출력하는 것을
  - 무한 반복하는 프로그램
  - 1.py로 저장
  - 실행화면 캡처: 1.jpg

AES 파일 암호화

파일 암호화 : aes-file-encrypt.py

- Iv 를 생성하여 암호화된 파일에 같이 저장
- 원본파일 size를 암호화된 파일에 같이 저장
- 입력 파일을 읽어서 암호화 후 저장
  - Padding 필요
  - 파일 구조

IV(16)	Org filesize(8)	Encrypted txt

파일 복호화 : aes-file-decrypt.py

- 파일을 읽어서 iv 를 읽음
- 파일을 읽어서 원본파일 size를 읽음
- 파일을 읽어서 복호화 후 복호화 파일에 저장
- 원본 파일 size에 맞춰 truncate

과제2

문제 파일 복호화

- Enc1.txt 파일 복호화하여 화면에 출력하기
- Key : ABCDEF0123456789
- Iv : Netsec@Soongsil.
- Mode : CBC
- 파일 구조

Org filesize(4)	Encrypted txt

소스 파일 : 2.py

실행 결과 : 2.jpg

CTR 모드

```
from Crypto.Util import Counter
ctr=Counter.new(128)  # bits, block size
Aes = AES.new (key, AES.MODE_CTR, counter=ctr)
```

- 과제 3 : Enc2.txt 복호화하여 화면 출력
  - Key : ABCDEF0123456789
  - Mode : CTR

- 소스 파일 : 3.py
- 실행 결과 : 3.jpg

과제 제출

- 6개 파일 => 02.zip