201603867 CBC

AES 의 encrypt, decrypt 를 통해 암호화, 복호화를 함.

AES 를 import 하기 위해서는 해당 모듈을 다운 받아야하는데, pip 을 통해 python 을 위한 pycrypto 를 다운받기 위해서는 c++컴파일을 위해서 build tool 을 다운받아야 한다. 하지만 최근에 pycryptodome 를 통해 pycrpyto 를 대체하는 방법이 있어서 본 과제에서는 이를 다운받았다.

AES(key, mode, iv)를 통해 객체를 생성, 생성된 객체를 encrypt, decrypt 함수를 통해 암호화 복호화를 진행한다.

iv 값을 넣는 이유는, 블록체인에서 암호화 시에, 단순히 구역을 나눠서 암호화를 하는 대신, 이전 블록의 암호화 결과에서 값을 입력받아 같이 암호화를 하기 때문에 전체적으로 예상을 할 수 없는값으로 만듬과 동시에 복호화를 하는데 어렵게 하기 위해 이런 식으로 설계를 했다. 이때 맨 첫번째 값을 암호화 하기 위해 임의로 넣는 값이다.

이렇게 encrypt 를 하면, 평문을 blocksize 로 나눠서 block 을 만든 후 순차적으로 암호화를 진행한다. 암호화가 다 끝나면 해당 암호문을 이어서 하나의 문장으로 만들고 이를 반환한다. 이때 한 블락을 맞추기 위해 입력된 값을 pad 를 통해 크기를 맞춘다. Pad 는 block size 를 주기로 길이가 일정하도록 맞추는 함수이다.

Decrypt 는 반대로 암호문을 복호화한 후 unpad 를 통해 원래 문장을 다시 찾아오는 방식으로 했다.

여기서 코드가 encrypt 와 decrypt 를 나눴는데, string 을 c 코드로 넣을 수 없다는 오류가 발생, iv 와 key 값을 utf-8 로 인코딩해서 AES 객체를 만듬. Cipher.encrypttldp pad(message)를 byte 로 만들기 위해 ascii 코드로 인코딩. 했다.

반대로 decrypt 에서는 message 자체가 binary 형식이기 때문에 파일을 읽을 때 binary 모드로 읽고 binary 모드로 쓴다.