**Student ID: 2016025105**

**Name: 강재훈**

1. **대칭키 암호화 중 AES**

텍스트이(가) 표시된 사진

자동 생성된 설명

main 함수에서 input으로 받은 origin data를 AES 방법으로 encrypt하고 decrypt 하는 함수 입니다. block size는 16byte로 하고 그에 맞게 iv도 16byte의 랜덤한 값을 갖게 해줍니다. origin data는 \_pad함수를 통해 부족한 byte를 채워줍니다. 이후 AES API를 이용해 encrypt 해줍니다. 주의해야 할 점은 python은 기본적으로 unicode를 사용하므로 utf-8로 인코딩 해주는 과정이 필요합니다. cipher\_text의 앞 16byte는 encrypt할때 사용된 iv가 저장되도록 만들었습니다. 이후 decrypt 과정에서 iv를 다시 가져오고 cipher\_text의 iv부분을 뺀 나머지를 decrypt 해주고 앞서 padding해준 부분을 \_unpad함수로 잘라 내준 후 출력합니다.

1. **hash 함수 중 SHA256**

텍스트이(가) 표시된 사진

자동 생성된 설명

main 함수에서 input으로 받은 origin에 SHA256 hash 함수를 사용합니다. hexdigest는 인코딩된 결과값을 가져옵니다.

1. **비대칭키 암호화 중 RSA**

텍스트이(가) 표시된 사진

자동 생성된 설명

main 함수에서 input으로 받은 origin에 RSA 방법으로 encrypt하고 decrypt하는 함수입니다. key의 length는 1024보다 크거나 같고 256의 배수가 되도록 만들었습니다. 이후 random한 키를 만들고 public key로 encrypt하고 private key로 decrypt 했습니다. 역시 AES때와 마찬가지로 python은 unicode를 사용하므로 utf-8로 인코딩 해주었고 exportKey함수의 default 값은 RFC1421/RFC1423을 따르는 PEM이므로 DER으로 설정해주어야 합니다.

1. **실행 화면 캡쳐**

**영어 문자열에 대해**

텍스트이(가) 표시된 사진

자동 생성된 설명

**한글 문자열에 대해**

텍스트이(가) 표시된 사진

자동 생성된 설명

1. **컴파일 환경 및 주의사항**

**macOS Catalina version 10.15.6**



**hashlib은 python 표준 라이브러리**

**origin data는 실행시 input으로 넣어주어야 함**