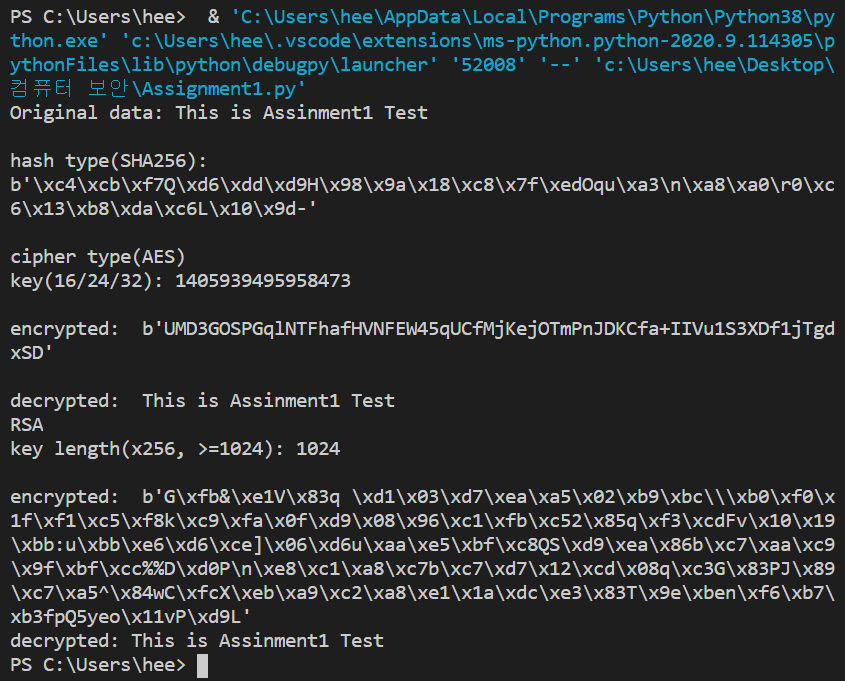
**컴퓨터 보안 Assignment1 보고서**

**2016043790 정희정**

1. **개발 및 테스트 환경**
2. **언어: python3.8.0**
3. **Operating System: Windows10**
4. **IDE: Microsoft visual studio code**
5. **라이브러리: Crypto, Hashlib**
6. **실행 결과**



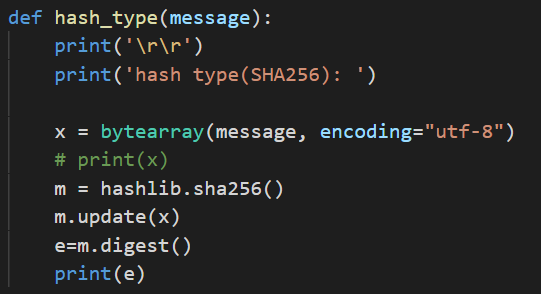
\*\*해당 스크린샷은 pip에 pycrypto가 설치되어 있다는 가정 하에 실행한 결과 화면입니다.

프로그램은 순서대로 Hash type 암호화(sha256), 대칭키 암호화(AES), 비대칭키 암호화(RSA)를 수행합니다. Hash type 의 경우에만 decoding 된 본래 문자열을 반환하지 않으며, 나머지 경우에는 encrypted 문자열을 byte 형식으로, decrypted 문자열을 string 형식으로 출력합니다.

1. **구현 내용**
2. **공통**

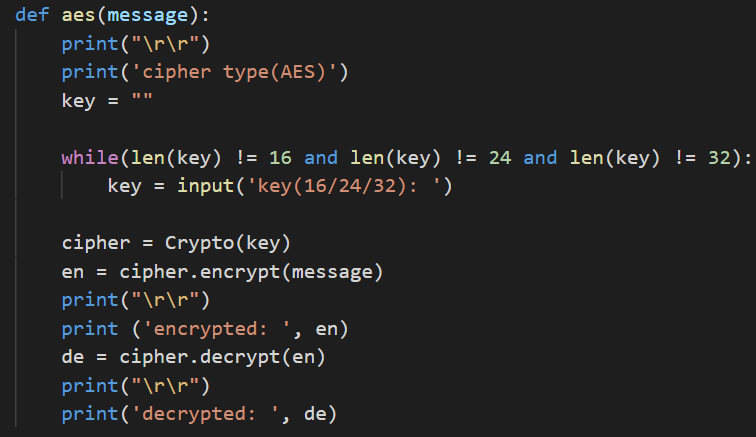
* 암호화 할 input data 는 알파벳 문자와 숫자, 특수 문자가 포함 된 string 형태입니다.
* Pycrypto 라이브러리가 이미 설치되어 있다는 가정 하에 구현하였습니다.

1. **Hash type(SHA256)**

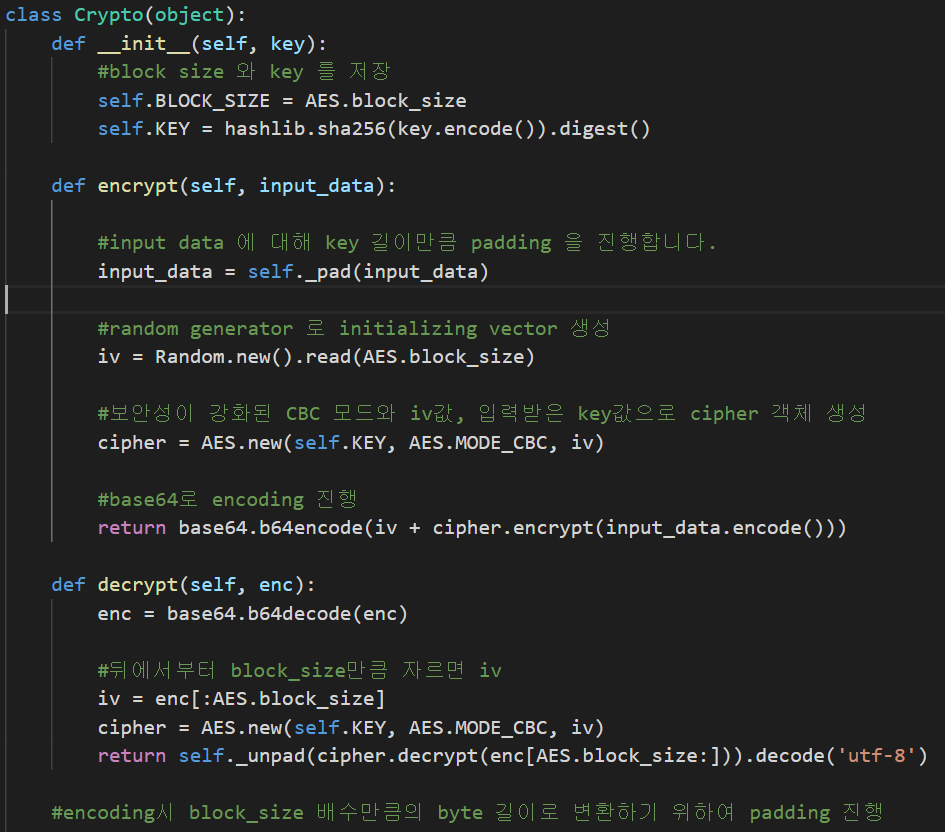


Raw text 를 byte array 로 변환한 뒤 hashlib 을 이용하여 다이제스트를 반환합니다.

1. **대칭키(AES)**

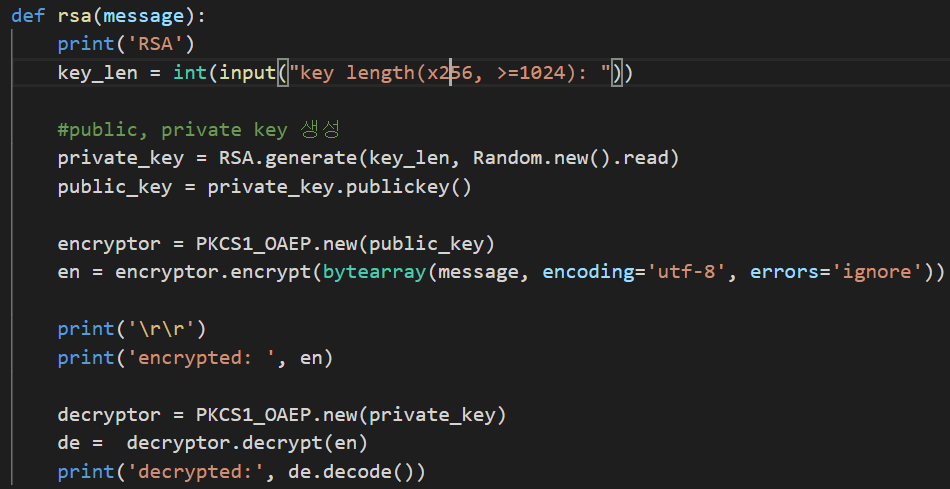


Key 값을 입력 받습니다. Key 는 알파벳, 숫자, 특수 문자로 입력이 제한되며, 16, 24, 32의 길이가 아닐 경우 다시 입력 받습니다.



\*주석을 참고해 주세요

1. **비대칭키(RSA)**



생성할 key 의 length를 입력합니다. 이 때 입력 받는 key의 길이는 256의 배수이며 최소 길이는 1024입니다. key\_len 길이의 random byte 를 private key 로 생성합니다.

PKCS1\_OAEP 프로토콜로 encryptor 와 decryptor 를 생성하여 각각 인코딩, 디코딩합니다.