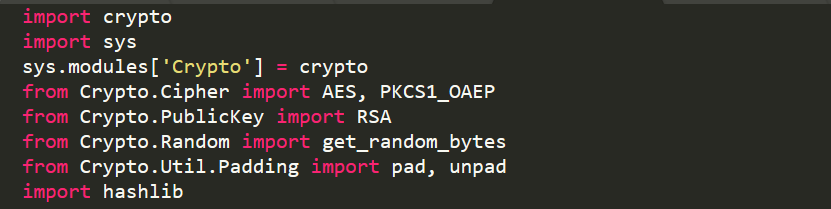
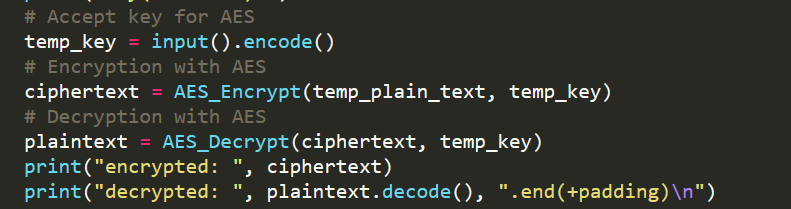
Assignment1 보고서

2017029770 서윤희

1. 제가 사용한 암호화 알고리즘은 각각 AES, SHA256, RSA이고, 과제 설명 document에서 알려주신 python crypto, hashlib api를 사용하였습니다.

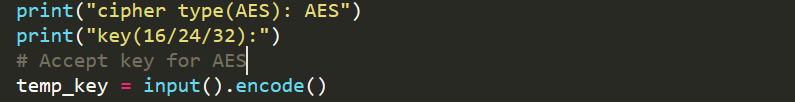


* 1. AES 알고리즘의 경우 Block SIze단위를 256바이트를 기본으로 설정하였습니다. Operation mode는 ECB 모드를 사용하였습니다. Padding 포맷(Style)은 따로 정해두지 않아서 crypto의 함수정의에 의해 ‘pkcs7’ default를 따르게 됩니다. Pad, unpad를 활용하여 decrypted text에는 패딩을 없애주었습니다. encrypt함수는 Key, plaintext 파라미터를 받고 처리하여 ciphertext를 decrypt 함수에 넘겨주게 됩니다.

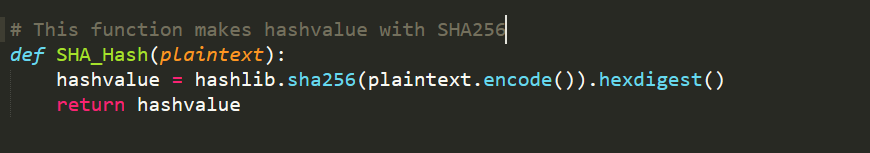
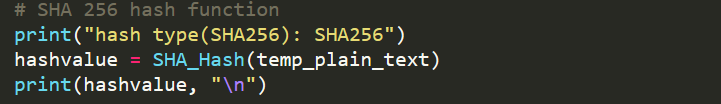




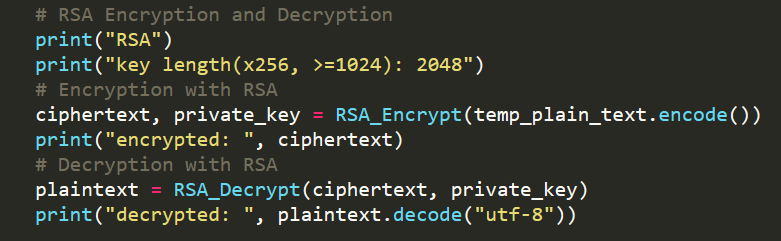
Key를 받는 부분은 16,24,32 바이트 길이의 key 값을 입력할 수 있습니다

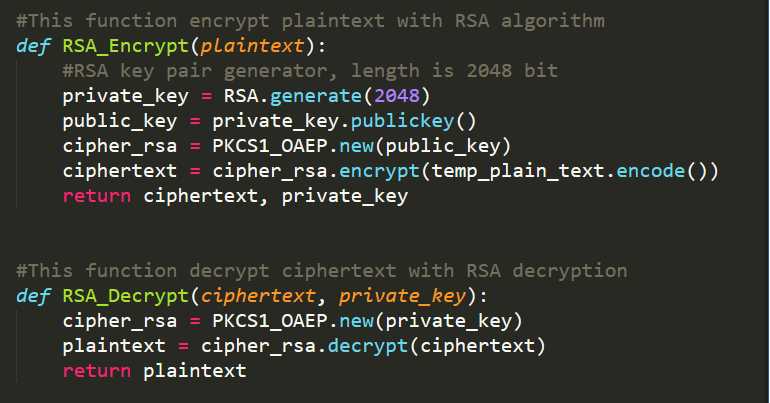


* 1. Hash 함수의 경우 hashlib에서 지원하는 SHA256 해쉬 function을 사용하였습니다.



* 1. RSA 알고리즘의 경우 key size를 2048 bit으로 설정하여 214바이트까지 encrypt 가능합니다. 실제로는 secret code를 넣거나 key 포맷을 정의해서 export key 한 후, 다시 불러와 key를 활용할 수 있는데, 바로 encrypt, decrypt하여 결과값을 보여주기 위해 key를 export, import하는 과정은 생략하였습니다. encrypt함수에 plaintext를 파라미터로 넘겨주고 만들어진 key, ciphertext값을 return한 후, decrypt 함수에 넘겨주어 실행합니다.





2 . 실행환경은 Windows10 64bit powershell, python 3.6.5 에서 실행하였습니다.

실행화면

