**컴퓨터보안 Assignment1 Report**

2018008613 안상욱

1. **대칭 키 암호화 (AES)**

대칭 키 암호화 중 AES를 선택해서 구현해보았습니다. AES는 블록 단위가 64bit, 즉 16byte 단위이므로 입력 받은 plaintext의 길이가 16의 배수여야 합니다. 따라서 이를 만족시키기 위해 padding을 해 준 뒤 복호화 후 padding해주었던 글자를 지워주는 작업을 해 주었습니다. 따라서 100자 이하인 plaintext의 길이 제약조건은 없습니다.

Key 값은 128, 192, 256 bit 중 하나여야 하므로, 16, 24, 32 byte 중 하나의 길이를 가져야 합니다. 따라서 key 값을 입력 받을 때 16, 24, 32글자가 아니라면 해당 길이를 만족할 때까지 입력 받도록 프로그램을 구현했습니다.

그 후 Crypto 모듈의 AES를 사용하여 암호화 및 복호화를 구현했습니다.

1. **Hash 함수 (SHA256)**

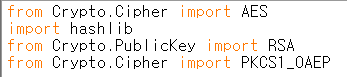
Hashlib를 사용하여 입력 받은 plaintext를 해시함수를 통해 해시값을 구한 뒤 이를 출력해주는 프로그램을 구현했습니다.

1. **비대칭 키 암호화 (RSA)**

1024글자 이상의 KEY 길이를 입력 받는데 2048자를 사용하도록 권장하고 있습니다. 1024글자보다 작은 길이를 입력 받았을 때는 1024 이상의 KEY 길이를 입력 받을 때 까지 계속 KEY 길이를 입력 받도록 구현했습니다.

입력 받은 plaintext와 key 길이를 이용해 Crypto 모듈의 RSA를 이용하여 암호화 및 복호화를 구현했습니다.

1. **코드**

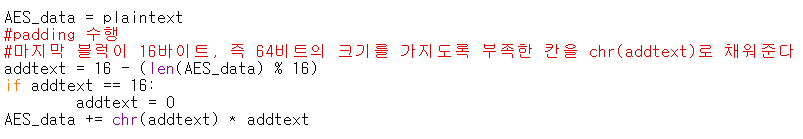


다음 모듈들을 import합니다.

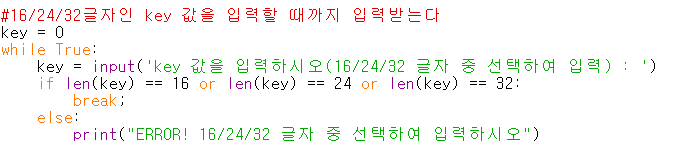


Plaintext를 입력 받습니다.

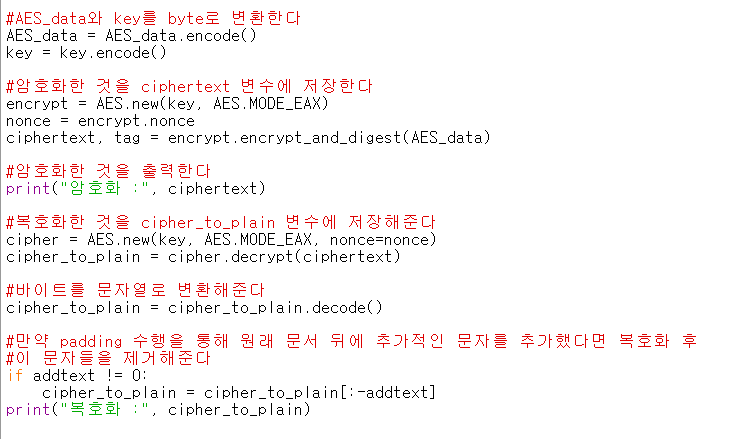
1. **대칭 키 암호화 (AES)**



Padding을 통해 plaintext의 길이를 16의 배수로 맞춰주고, 추가된 길이를 addtext에 저장해줍니다.

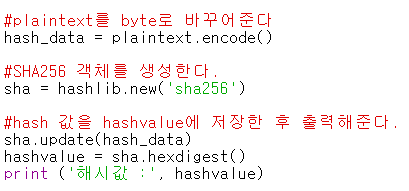


16/24/32글자인 key 값을 입력할 때까지 입력 받습니다.



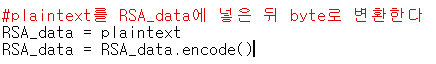
암호화 및 복호화 작업을 수행 후 암호화, 복호화 결과를 출력해줍니다. 복호화 시 padding을 통해 추가해준 문자들을 제거해준 후 출력합니다.

1. **Hash 함수 (SHA256)**

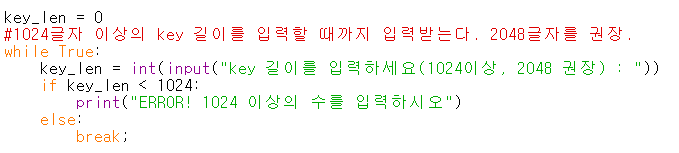


Plaintext를 byte로 바꾸어 준 뒤 hashlib를 사용해서 hash값을 도출해낸 후 출력해줍니다

1. **비대칭 키 암호화 (RSA)**



Plaintext를 byte로 변환해줍니다.



1024 이상의 key 길이를 입력할 때까지 입력 받습니다.



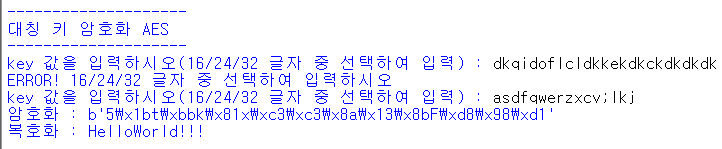
Crypto의 RSA를 이용해 암호화 및 복호화 한 뒤 결과를 출력해줍니다.

1. **코드 실행**



Plaintext를 입력 받습니다.

1. **대칭 키 암호화 (AES)**

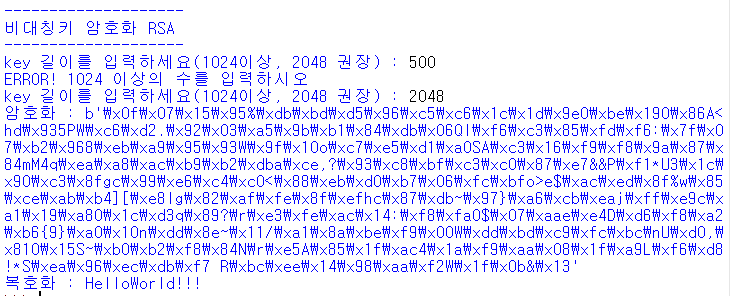
Key 값을 입력 받을 때 16/24/32 글자가 아니라면 다시 입력 받도록 합니다. 올바른 key 값을 입력했다면 key 값을 가지고 암호화 및 복호화 결과가 출력됩니다.

1. **Hash 함수 (SHA256)**



초기 입력 받은 plaintext에 대한 hash 값을 출력해줍니다.

1. **비대칭 키 암호화 (RSA)**



Key 길이를 입력 받는데 1024보다 작은 숫자를 입력하면 1024 이상의 수를 입력 할 때까지 다시 입력 받습니다. 그 후 암호화 및 복호화 결과를 출력합니다.