컴퓨터 보안 HW1

컴퓨터소프트웨어학부

2016024839 박정민

컴파일 환경은 visual studio code python 3.8.2입니다.

코드작성에 필요한 pycrypto모듈을 다운받았음에도 불구하고 Crypto가 import되지 않아

```
1    import crypto
2    import sys
3    sys.modules['Crypto'] = crypto
```

이렇게 세 줄을 추가하였습니다.

대칭키 알고리즘으로는 DES를 구현하였습니다. 8byte단위로 맞춰주기 위해 padding함수를 구현하였고, key 길이 역시 8byte로 제한을 두었습니다.

Hash 함수는 SHA256 API를 사용하였습니다.

마지막으로 비대칭키 알고리즘으로는 RSA를 구현하였습니다. 가장 작은 15개 소수의 리스트를 만들어 두 개를 랜덤으로 선택해 private_key와 public_key를 구하고 암호화하였습니다.

```
Original data : Hello World
key(8 byte) for DES : 98413151
DES Encrypted : b'\xee\x03\x00\x17\x9ec5\x9a\x1f\xe3\xf9\xfcZb\x0f\x01'
DES Decrypted : Hello World
Hash type : SHA256
Hash Encrypted : b'\xa5\x91\xa6\xd4\x0b\xf4 @J\x01\x173\xcf\xb7\xb1\x90\xd6,e\xbf\x0b\xcd\xa3+
W\xb2w\xd9\xad\x9f\x14n'
p : 41
q : 11
public key : 3
private key : 267
RSA Encrypted : [271, 217, 69, 69, 199, 296, 43, 199, 9, 69, 133]
RSA Encrypted : 271217696919929643199969133
RSA Decrypted : Hello World
```