컴퓨터보안 Assignment #1. Cryptography

2018008177 김찬위

1. 컴파일환경

```
from Crypto import Random
from Crypto.Cipher import DES
from Crypto.Cipher import AES
from Crypto.Cipher import ARC4
import hashlib
from Crypto.Cipher import PKCS1_OAEP
from Crypto.PublicKey import RSA
```

- linux: ubuntu 18.04.4 기준 정상작동 확인

- python 3.7.7 로 작성

- crypto, hashlib 등의 모듈을 import 할 수 있어야 함

- 실행파일은 main.py `$ python main.py` 명령어로 실행가능

2. 기본 알고리즘 및 입력 주의사항

- 대칭키 암호화: DES, AES, ARC4

- hash 함수: SHA, SHA256, SHA384, SHA512

- 비대칭키 암호화: RSA

- 모든 한글 입력은 제외!! 오로지 영어로만 입력해주세요!!

- 입력과 출력 형태는 과제 명세서의 실행 예시와 동일

- 지시문에 실행 가능한 type과 유효한 value 범위 명시

- original message의 경우 입력이 있을 때까지 반복

- 그 외 입력에 대해서 경고 메시지와 함께 임의의 타입, 데이터 값으로 알아서 실행

3. 코드 구현

- 'printInfo(enc, dec)' 암호화, 복호화된 데이터 출력

- 'padding(msg, length)' 블록 암호화의 경우 부족한 길이만큼 알고리즘에 맞춰 padding. ' '로 부족한 문자를 채워 넣음

- 'aes(msg)' key값으로 16,24,32 길이의 문자열을 받으며 그 외의 입력의 경우 '1234567812345678'이 키 값. iv 값은 random하게 블록 단위만큼 불러오고 AES.MODE_CBC로 암호화, 복호화

- 'des(msg)' key값으로 8 길이의 문자열을 받으며 그 외의 입력의 경우 '12345678'이 키 값. DES.MODE_ECB로 암호화, 복호화

- 'arc4(msg)' key값으로 어떤 길이도 상관없이 받으며 null이 입력될 경우 '1234'가 키 값.

- 'rsa(msg)' key length 값을 추가로 입력 받으며 1024 미만인 값이나 숫자가 아닌 문자열을 입력하게 되면 1024가 key length값. publickey와 privatekey를 생성해 암호화, 복호화

- 대칭키 암호화의 경우 명시되지 않은 cipher type을 입력하면 DES가 실행

- hash 함수의 경우 입력 받은 데이터를 적절한 함수의 인자로 넣어주고, 명시되지 않은 hash type를 입력하면 SHA가 실행

4. 실행 화면

```
(cg-course) chanwi@chanwi-VirtualBox:~/security/2020_ite4007_2018008177/Assignment1$ python main.py

original message: Hello World!

cipher type(DES/AES/ARC4): AES
key(16/24/32): 1234123412341234
encrypted:
b't\xdc\x8f6\xdc\x9e\xf9\x05\xfdS\xe3\xd6\x84\x99k\xdd'
decrypted:
Hello World!

hash type(SHA/SHA256/SHA384/SHA512): SHA256
7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd200126d9069

RSA
key length(>= 1024): 1024
encrypted:
b'WJF\x9b.a\x9dQ\xe5\xe3wX\xa6\xdc\xdb>\xee\x13\x01\xbd\xdedc\x18\xf8\xcfb\xbb\x14)\xdd$242\xa4<\x9
1\xe7V\x9d/\x7fC\xc1\xab\xf2\x1f:]\xed\xab[jB\xfdx\x92sh\xcb!\x14\x8e\xf8\xd5\xae\x99\xac\xe6G<,onL
\xf6w\x91\x16\x17\xfd\xc2\xf6H\xdf\xbf\xb3\x05\xad^\x0b\xd7\xb5\xf9Pl8\xdd\xdbr\x81\xd8\xado\xb6\xb
5-n\xc8<\xb4q\xd0p\xbek\xbc#\xa9\xc2\xeanNUMW\x84'
decrypted:
Hello World!
```

```
original message: DES / SHA test

cipher type(DES/AES/ARC4): DES
key(8): helloyou
encrypted:
b'\x1aab\x8f\xa7\xb5\x96\xa2\xdf\xd4\xf3}\xab\xcf\x03\xd9'
decrypted:
DES / SHA test

hash type(SHA/SHA256/SHA384/SHA512): SHA
6dd75b6a240f928b42208e045ffa9bb07b409421

RSA
key length(>= 1024): 2000
encrypted:
b'\x04\''\xbf\xc5\xa3:\xeb\xe3\xbb\xe1\x1c\xcd\xac\xa5\x83\x87\xb5\xaa[p\xa1\x87\x87\xf6\xba\xfdAy\x
e5\x91\x9d\x9d\x96\x9b\x98\n\xc9\x92\x19\t\x8e\xcfz\x08\xe6\tmI\xca\xbe3",X\xf8\xec\xbd\xfd\x9b\xe8
IS4yH\xa4`\\u\x93\xb4`\x96\xd1n\xa9&yh\x05\xf4\xec\x98\xf5\x1b\x1a\xf3\x08\xf6q\xd83\xcb\x87w\xa6>\
x01\''\xd0\x92P!\xca\x92m\xe2\x0f:A\x83ac\x93\x00\xdaP\x8a\x15Q\x9c\'c\xf9K\xa0/Ph{\xbeg\xde\x8d\x9d
\xee\xfb2\xebyBy\xde\xc5_\x1e\x04^\xd2\xc3\xd4\xaf+\xd7PuIq.K\xa2\xde\xdf\xb7\xef:\x8b\x90\x0c]\xf6
\xb0\xaf\x83t\xcc6\xe1:\xd2\x99\x9ff<\xb0\xa4N!\xc4\xf2oxG\x10\xe8\'(\xd1\xf3\xf0\xc1G\x8c\x97*\x9a
\xc468T\xc9\xb9qU\xee\x86\xf2\xdf\x8f\xa2\xfc\xdb\xdc\xa5\xc6\x16\x92\xf5@ \x8ds\x8b\x089n\x1b\x1b\
xe8\xa9\xf8,\xff}\x9d :9\x19f'
decrypted:
DES / SHA test
```

```
original message: ARC4 / SHA384 test

cipher type(DES/AES/ARC4): ARC4
key: it's okay to enter any key 123
encrypted:
b'\x9a\x1c\x14=S]\xb2\x9bV\xdek\xac\x05\x99\xaf\x11\\j'
decrypted:
ARC4 / SHA384 test

hash type(SHA/SHA256/SHA384/SHA512): SHA384
aa026b3e77721d1b706bb514137597b843e13c3c1c7de1b327bd1978151ee6e67db3ad145cc1cbe725d551e515b341d3

RSA
key length(>= 1024): 1500
encrypted:
b"\x04Q\x81u\x9dQ\xdeP1\x7f\xbc\xb6\x91\x82\x85\xf5\x80\x03\x9f\xce\xa0\xe5\xfc7\xa0`\xc0-\x90?\x0c
\xe8\xbcu\xf2^V\xb2$Q\xc6\xfd\x80\x11G\x16\xc3\xe9\x9c\x82R\xd4y\xc5\x03\xf2\xf3R|\x85\xd1)\xc3R'\x
0e<\xda\xcf\xf4\xb0\x10\xc9<\x89\xa4\x05Q\x05\x1bbH\x95\xacML\xffJ\x14w\xc8\xd3\xed\xf1\xd42\xb1\x9
5r\xb0\x8d\xe8\x9c$\xa2\xd4\xbd\x1a\xa2\x99'q'\xf1~\n\x04`\xa3b@Gh}\xb5~\x0f\xfa\x18\xb6\xb3\xb6\xe
4\xe2}\xe3\x87\xabU\xb5\xa5XQUAG\xf5M\xa9 \xd05\x83/Q_\xe7\xec\xdcI\xbd\x9c\xc9@\xa3\x84\x16\xdc\xc
5\x7f\xa7\xac\xb4\xa4\xd42\xbfRY\x83\x8b\rB\xc7%\\6\xe0"
decrypted:
ARC4 / SHA384 test
```

```
original message: cipher error / SHA512 test

cipher type(DES/AES/ARC4): hello
[warning] temporary DES executed
key(8): 12341234
encrypted:
b'Gg\xa6>>P\xdc\x0e\x1f\xa8#t:2_\xf4!\xbfd\x9b\xdc\xe1\x1e\xc6\x96\xf0\xd6BC\xfcf\xbc'
decrypted:
cipher error / SHA512 test

hash type(SHA/SHA256/SHA384/SHA512): SHA512
a060017ab3d8f6c5f18ba4c65c9b639643e0a4a84850d0b90fcf5ce9b08e00f25a6b2e89ec630e87bc6ffa214aead9353da
e1dab493c7ca5d9f0fb11b957a64a

RSA
key length(>= 1024): 3000
encrypted:
b'\x9f\\\xbf\x10\xd3?\xe3\x06\x06=%\xbcr.\xc1\xf6=-\x99A\xc27`\x91\xab\x08\xe0\xcd\x81\xfa\xff\x16\
xb0\xeb0\xd7\x84l\xd0[@m\xeb\x1a\xb2W\x1c\x81:_*\xb9^\xc9\xcfW:/pk\x07\x9b\x820\xe2?T\xafbF\x1f>0\x
86\x94\xaa\xad\xe4\xafz\x0f\xc4\xadC\xec\xf8%\xf7)\xc9\xa2|(\xaa\x0c\x14\t\xea \xd8\xcegH\xc9\x00S\
xe8\xa4>\x9e\x86\xda\xa3o\xa0 \xb1Q\xcc\x853\xdd\xc0\xdb\xb8Gm\xe7\xf4\x94\xf5U\xea\xa3t\x9d\xca9\x
e1\xab\x8bv\x85\xe0m\x08l\xb3\xdd\x8b\xe3G\x00\x88\x03{\xba\x11\x02^\xe5A/\xb7\xa9|\xf4S5)\x02\x08\
x05\\\x01\x84^\xec\x84\xe2?\xe1\xb0\x1dx\x99\xda\xb8\x9f\x1c\x1a\x02\xc9\xdfM\xb0n\xfe\xb7\x80\xb1\
x88\xc1\xcch\xc53\xf9":\xdb\x92\x80\'\xa5\x1d\xeb;]\'\x11\xec\xf7\xcd\xdd\x80\t\x17\xa8@E\xfb)<\xfc
\x06\x9b2<\x7f\x16?\x8f\xb1T/c\xf4\x03K\x94\xa8u\xe61\x97\xf7/,\xaco\xc4\x0b\n\xa2~\x8a#s(\x8c[\x88
\xe0?\x94jv\xe23\tH\xeb\x13X\xabK\x9c\xb4\xcbc FJ\xb0\xf3\x13\xeeZ\x8c\\\xc7\xc3{cb\x94\xa9t\x86\xb
4\xbd\x8c<\xfb\xa2\x9b+\x08\xc1\xd9\x87$n\x9fb\x03\x08{\xe0\xack\xe5\xb0\x81\xfe\xb5\xbf\xd9\xae~\x
b4\x0fd\xabS\xa5\xbar~\xc1\xb4S\xe4\r\xee\x88\'8\xcdX:\xfe0\x03\x02\xef\xc4\x8a\x7fa\xe5`\x7fB'
decrypted:
cipher error / SHA512 test
```

```
original message:
original message:
original message: invalid input example

cipher type(DES/AES/ARC4):
[warning] temporary DES executed
key(8): 1
[warning] temporary key is "12345678"
encrypted:
b'n\x15\xb0\xe3\x8e,\x99\xe8\xd2\xf6\xaf\x97\x16\x00\x00j9\t\x8b@c\x0co\x8e'
decrypted:
invalid input example

hash type(SHA/SHA256/SHA384/SHA512): no
[warning] temporary SHA executed
3aaaf130231624741efcf4a27aeb51a39f61c19e

RSA
key length(>= 1024): 0
[warning] temporary key length is 1024
encrypted:
b'\x07=1\xbbk\x08\xe0nB\x1bI\x81\xa1\xd2\x02\xc0\x1d\x91\xfa-\xfe\xd6\x01\x1e\x91\xba-\x87\xbb\xac3
:\xed\xd1\xb5y\xe4\x1f\xcb?]`\x14\xe7\t\xa2\x0f\x8bm\xd5hET\x10L\x99z+fc\x0c\xfc\xaeI\xc5\xee\xa2e\
x14<W#\xd39\xb2\x9d\x9bx\xe4_\xf7\xc6t\xf6\xcci\xc6`\xeb\x964\xaa\xe1\x8e\xbb} \xbf\xf0YJ\x1f\xab\x
a8\xa3\x82\xc0d\xb2\x1e\x87-\xda\xc5\x85]\xf7\x0f\x8f\xa4\xf4\x17h\x90*\x8d1\x1a'
decrypted:
invalid input example
```