2020-2 임을규 교수님 컴퓨터보안

Assignment #1. Cryptography

과제 제출: 모든 소스코드 및 보고서를 본인의 git repository에 업로드

제출 기한: 10월 9일 금요일 23:59까지. 제출 기한에서 한 시간 단위로 10%씩 감점, 최소 0점

문의 사항: 장준영 조교, lartist@hanyang.ac.kr (제출 관련 문의 등)

과제 내용

이론수업 자료 '02.CryptographicTools'에서 소개된 내용 중
대칭키 암호화(DES, AES 등) 중 한 가지 이상,
hash 함수(SHA256 등) 중 한 가지 이상,
비대칭키 암호화(RSA 등) 중 한 가지 이상
을 API 사용 또는 직접 구현하여 문자열 및 key가 필요한 경우 key (RSA와 같이 key 길이가 긴 경우 key 길이)를 입력 받고, 암호화 및 복호화가 가능한 경우 복호화하는 과정을 보일 것

100자 이하의 문자열을 암호화 및 복호화 하는 과정에서 문제가 없도록 예외처리 하며,
입력할 때 문자열이나 key의 길이 등에 대한 입력 제한이 있는 경우 보고서에서 명시할 것

실행 예시

```
(base) C:₩Users₩bassist₩Desktop₩CLASS₩CS>python 1.py
original data: Hello World!

cipher type(DES/DES3/AES/ARC4): AES
key(16/24/32): 1234123412341234
encrypted: b"₩xf1₩xa6₩xeb₩xe4₩xd7A₩x96₩ro₩x85'[₩x92]₩xf3X"
decrypted: Hello World!____

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

RSA
key length(x256, >=1024): 1024
encrypted: (b'₩xb5₩x9b₩xf4J:b₩xa2₩x17₩xbc"L@!₩x82₩xdd~GO₩x10xI₩xa7s₩x10₩x17₩xecee₩xed₩x03₩x11₩x86v₩xc4e
₩x17₩xe0X₩xd6₩xec₩x88₩x8b(₩xbb₩xa5₩xceQKO₩xd37₩xf7₩x03₩t₩xc6₩xa6₩xb5-%+₩xc7₩xb8x₩xf3t₩x03₩xff<f₩xb4₩xea
C+qH₩xbO₩xc1₩xf4{-₩xc7₩xff₩x14₩xfdw!₩x9a₩xce₩xa5₩xd2₩x97₩xObk₩xa1:₩xafI₩xOcK₩xd4-₩xbb₩xc1₩x17C₩x8e₩xcf~
₩x9dn₩x8e6C₩x8f₩xbb₩x9a₩xceh₩x84₩x19₩xea₩xe8₩x16₩x13&₩x10₩xO6Y',)
decrypted: Hello World!
```

힌트

Python의 Crypto
https://pycryptodome.readthedocs.io/en/latest/src/api.html

Python의 hashlib
https://python.flowdas.com/library/hashlib.html#

등 본인이 원하는 API 사용 가능

문자열 <-> 바이트 코드 변환에 유의할 것 (인코딩, 디코딩)

블록 암호화의 경우 부족한 길이만큼 padding을 수행하거나 필요한 길이를 정확히 명시할 것

그 외 주의사항

코드 작성은 본인이 직접 할 것. 소스코드 유사도 검사하여, copy한 과제는 0점 처리

프로그래밍 언어 제한 없음

보고서
- 분량 제한 없음
- 실행 화면 캡쳐 필수
- 컴파일 환경 및 본인의 구현 내용에 대한 설명 등 작성