Trabalho 2

Arthur Barreiros de Oliveira Mota - 190102829
Erick Rodrigues Fraga - 190086815

Questão 1.

A questão 1 se encontra no arquivo “aes.py”, onde se encontram as funções de cifração e decifração AES, e suas funções auxiliares. Para a cifração a função “encrypt(key, data)” e recebe duas strings de bytes, sendo elas: key, uma seed para a criação para as chaves AES, e data, a mensagem a ser cifrada. Para a decifração é usada a função “decrypt(key, data)” e recebe duas strings de bytes, sendo elas: key, uma seed que foi usada para a criação das chaves AES, e data, a mensagem cifrada a ser decifrada.

Questão 2.

A questão 2 se encontra nos arquivos “rsa.py” e “oeap.py”. Onde se encontram as funções para a cifração e a decifração RSA e OEAP. As funções principais são as seguintes: “rsa_encrypt(key, message)” e “rsa_decrypt(key, message)” em “rsa.py” e “oaep_encode(msg: bytes, k: int, label = b"")” e “oaep_decode(em: bytes, k: int, label = b"")” no arquivo “oeap.py”.

Questão 3.

Se encontra no arquivo “sign.py”. A função “sign(msg: bytes, keys)” assina a hash e as linhas 17 e 18 formatam a mensagem para BASE64 .

Questão 4.

Se encontra no arquivo “sign.py” na função “verify(msg: bytes, sig: bytes, keys)”, onde é feito cada parte que foi requisitada está indicada por comentários no código.

Finalização

Os casos de uso indicados pelo professor estão no arquivo “test.py”, onde os casos de uso são executados na ordem em que foram dados.