PRÁCTICA 6: Firma Dual

Seguridad de la Información
Curso 2018-2019

Lenguajes y Ciencias de la Computación.
E.T.S.I. Informática, Universidad de Málaga

RELACIÓN DE EJERCICIOS:

1. (**10 puntos**) Considerando la firma dual establecida por el protocolo SET y especificado en el tema 4 de la asignatura, se pide:

    a. (**3 puntos**) Completar la implementación del protocolo SET en el dual_sig_cli.py, de forma que se realice correctamente la firma dual en el cliente:

    $$\text{Signature}(H(H(OI) \,||\, H(PI)))$$

    b. (**3.5 puntos**) Verificar que la información recibida por parte del vendedor es integra considerando para ello la firma dual establecida originalmente por el cliente y teniendo en cuenta que la concatenación de las partes sigue el siguiente orden preestablecido: OIMD + PIMD.

    c. (**3.5 puntos**) Realizar la misma operación que el punto b), pero verificando en este caso que la información recibida por el vendedor es realmente integra y se corresponde con la información recibida por parte del cliente.

En este ejercicio, se utilizará la clase SOCKET_SIMPLE_TCP del campus virtual, que permite crear un cliente y un servidor TCP básicos y las clases RSA y AES para la gestión de claves, cifrado y firma.