Criptografía (Parte 4)

Cristina Díaz García

November 2018

Índice

1. Ejercicio 1

1.1. Apartado a

```
Apartado a
    DIGEST: 'b'\x14\x97\xa9v\x9e\xcb\xbf\x16\xbf\x00@Vp\xdbZ=6\xd5\x0b<\x1b\xbe\xf4\xce;\xba0\x0e/\xc2L\x16\x18*E\x9b~\xd1\xff5X\x91P>8@\xbf\x82P\xc61\
x93\xf69\xb1y\x81\x02F>\x87\xe8\xce\xd6''
    HEXDIGEST: '1497a9769ecbbf16bf00405670db5a3d36d50b3c1bbef4ce3bba4f0e2fc24c16182a459b7ed1ff355891503e3840bf8250c63193f639b1798102463e87e8ced6'
```

1.2. Apartado b

```
Apartado b
    DIGEST: 'b"H\xc6n\xf8\xc8,^O`\xcd\x03=\xb5P\xbd6\x1a\x17''\x87\xc5x:\xb9F\x07\xea\xf3X\xb4\xafm\x91\xa6\xe2Q\x82\x8a\x9d\xca%A|\x17\x98v\xe0<\xc8\xb
bJ\xb3&\x81f\xbb<\xab ~E\xa2L("'
    HEXDIGEST: '48c66ef8c82c5e4f60cd033db550bd361a172787c5783ab94607eaf358b4af6d91a6e251828a9dca25417c179876e03cc8bb4ab3268166bb3cab207e45a24c28'

El mensaje 'b'Cristina\nD\xc3\xadaz Garc\xc3\xada\n'' es auténtico
```

1.3. Apartado c

```
Apartado c
    DIGEST: 'b'\xa0\x13\x13B\x1cS\xa3\xdf\t\xeb\xae\x94\x191\xf85\x8ay\xac\xd4a_\xa9\xf0\x9c\xfb$\xa5\x01\xe6\xe4\x00''
    HEXDIGEST: 'a01313421c53a3df09ebae941931f8358a79acd4615fa9f09cfb24a501e6e400'
```

2. Ejercicio 2

SHA-2 family es compatible con *HMAC*, ***SHA-3 family*** no es compatible porque no tiene el parametro *block_size*, ***BLAKE2*** no es compatible porque no se puede establecer el *digest_size* cuando se usa *HMAC*.