Desarrollo de un programa criptográfico

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

María del Carmen Cámara
José María de Fuentes
Daniel Garzón
Lorena González
Ana Isabel González-Tablas
Pablo Martín
Antonio Nappa

uc3m | Universidad Carlos III de Madrid

COSEC

Creación de hashes

- Tenemos que responder a las siguientes preguntas
  - ¿Qué hash queremos utilizar?
  - ¿Cómo/ dónde se almacena el hash?
  - ¿De qué datos calculamos el hash?
  - ¿Que hace que un hash sea bueno?

- Ejemplo en Python

```
digest = hashes.Hash(hashes.SHA256())
digest.update(b"   DATOS")
digest.finalize()
```


Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Creación de HMAC

- Tenemos que responder a las siguientes preguntas
  - ¿Qué hash queremos utilizar?
  - ¿Qué clave vamos a utilizar? ¿Quién crea la clave?¿La introduce el usuario?¿Cómo/dónde se almacena?
  - ¿Cómo/ dónde se almacena el hash?
  - ¿De qué datos calculamos el hash?

- Ejemplo en Python

```
h = hmac.HMAC(key, hashes.SHA256())
h.update(b"   DATOS   ")
h.finalize()
```


Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Librerias Python

Librerias Python:

- pyca/cryptography
  https://cryptography.io/en/latest/

- PyCrypto
  https://pycryptodome.readthedocs.io/en/latest/index.html

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Ejemplo con pyccryptodome:

Ejemplo con pyca/cryptography:

```python
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
"""
Created on Tue Oct 19 11:17:22 2021

@author: mayca
"""


reset -f

#=== PYCRIPTODOME ============================================================

#==== SHA2-256 =========
# https://pycryptodome.readthedocs.io/en/latest/src/hash/sha256.html
from Crypto.Hash import SHA256

h = SHA256.new(data=b'First')
h.update(b'Hello')
print h.hexdigest()



#==== SHA3-256 ===========
# https://pycryptodome.readthedocs.io/en/latest/src/hash/sha3_256.html
from Crypto.Hash import SHA3_256

h_obj = SHA3_256.new()
h_obj.update(b'Some data')
print h_obj.hexdigest()



#=== PYCA CRIPTOGRAPHY ========================================================
from cryptography.hazmat.primitives import hashes
digest = hashes.Hash(hashes.SHA256())
digest.update(b"abc")
digest.update(b"123")
digest.finalize()


digest_sha3 = hashes.Hash(hashes.SHA3_256())
digest_sha3.update(b"abc")
digest_sha3.update(b"123")
digest_sha3.finalize()
```

Desiderata – Sesión Hash

- Tipos de hash
- Que es una colisiones
- Porqué es útil un hash?
- Familiarizar con calculo de hashes con la libreria elegida.

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

COSEC

uc3m | Universidad Carlos III de Madrid