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

Cifrado simétrico

Librerias Python:

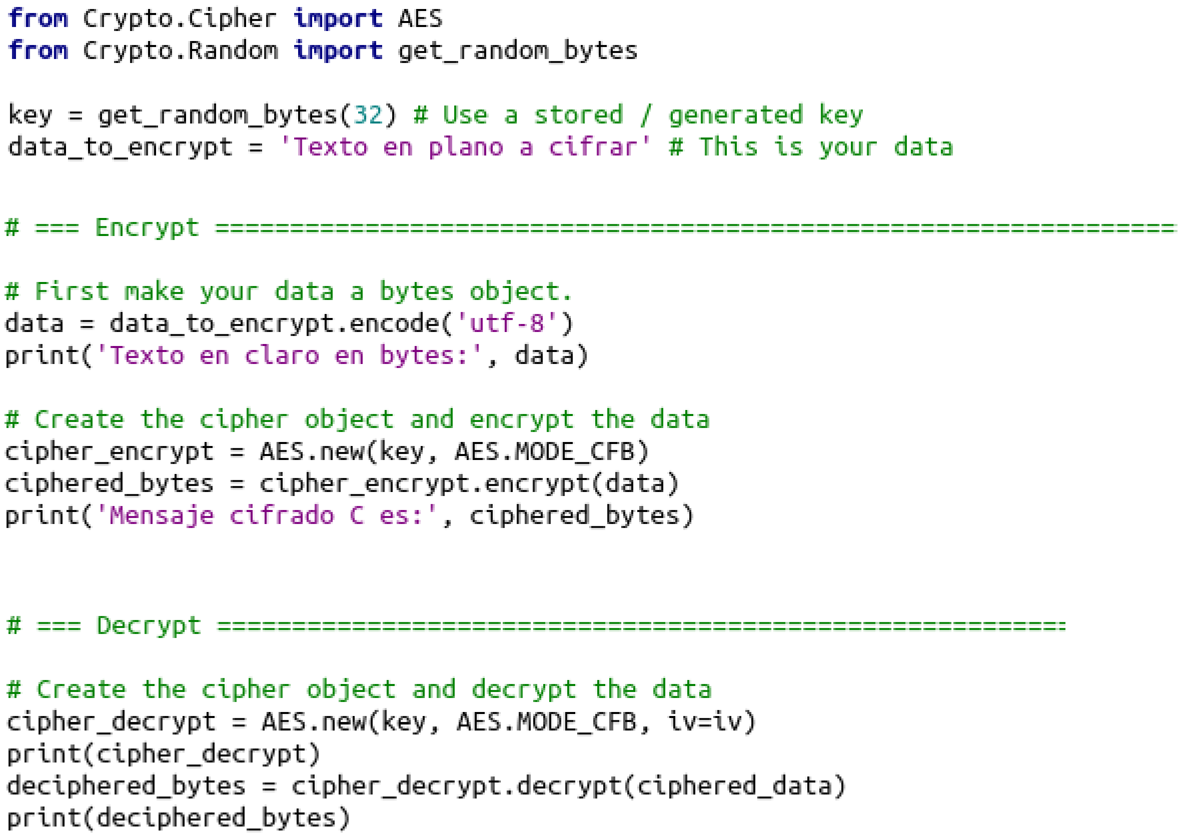
- pyca/cryptography
  https://cryptography.io/en/latest/

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

  conda install -c conda-forge pycryptodome

Cifrado simétrico

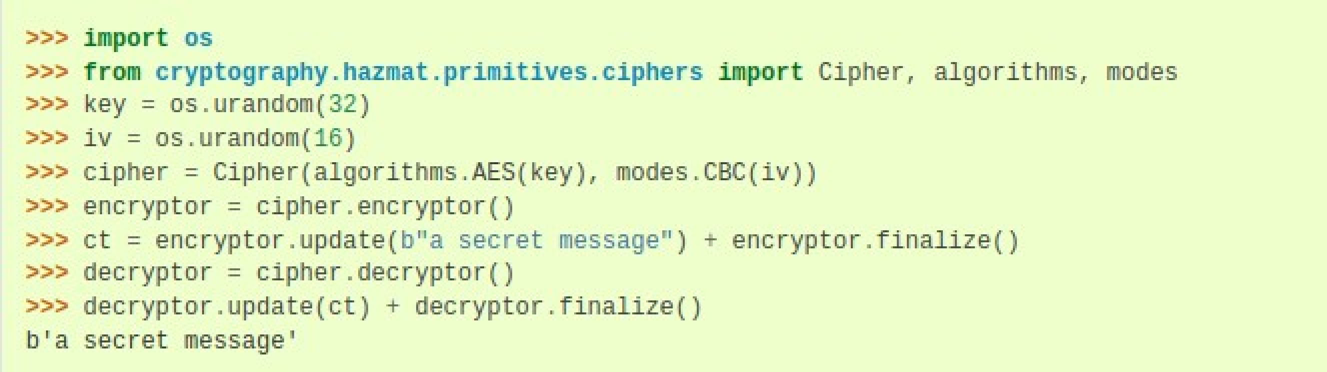
Ejemplo en Python con PyCryptodome:



```
from Crypto.Cipher import AES
from Crypto.Random import get_random_bytes

key = get_random_bytes(32) # Use a stored / generated key
data_to_encrypt = 'Texto en plano a cifrar' # This is your data

# === Encrypt ================================================================

# First make your data a bytes object.
data = data_to_encrypt.encode('utf-8')
print('Texto en claro en bytes:', data)

# Create the cipher object and encrypt the data
cipher_encrypt = AES.new(key, AES.MODE_CFB)
ciphered_bytes = cipher_encrypt.encrypt(data)
print('Mensaje cifrado C es:', ciphered_bytes)


# === Decrypt ========================================================

# Create the cipher object and decrypt the data
cipher_decrypt = AES.new(key, AES.MODE_CFB, iv=iv)
print(cipher_decrypt)
deciphered_bytes = cipher_decrypt.decrypt(ciphered_data)
print(deciphered_bytes)
```

Cifrado simétrico

Ejemplo en Python con pyca/cryptography:



```
>>> import os
>>> from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes
>>> key = os.urandom(32)
>>> iv = os.urandom(16)
>>> cipher = Cipher(algorithms.AES(key), modes.CBC(iv))
>>> encryptor = cipher.encryptor()
>>> ct = encryptor.update(b"a secret message") + encryptor.finalize()
>>> decryptor = cipher.decryptor()
>>> decryptor.update(ct) + decryptor.finalize()
b'a secret message'
```

Desiderata – Sesión Cifrado

- Definir Interfaz de nuestro programa
- Input/Output
- Elegir que cifrado simétrico queremos utilizar

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

COSEC

uc3m | Universidad Carlos III de Madrid