Read the Cryptography with Python blog at tutorialspoint.com (link is in the reading list). Select one of the methods described/ examples given and create a python program that can take a short piece of text and encrypt it.

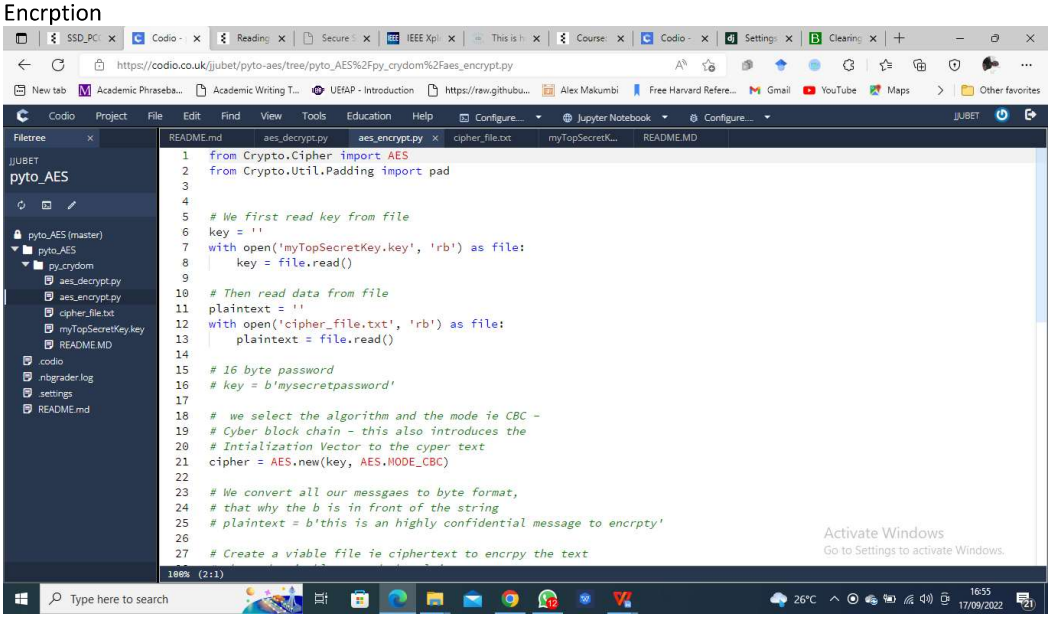
Create a python program in Codio (you can use the Jupyter Notebooks space provided in the Codio resources section) that can take a text file and output an encrypted version as a file in your folder on the Codio system. Demonstrate your program operation in this week's seminar session.

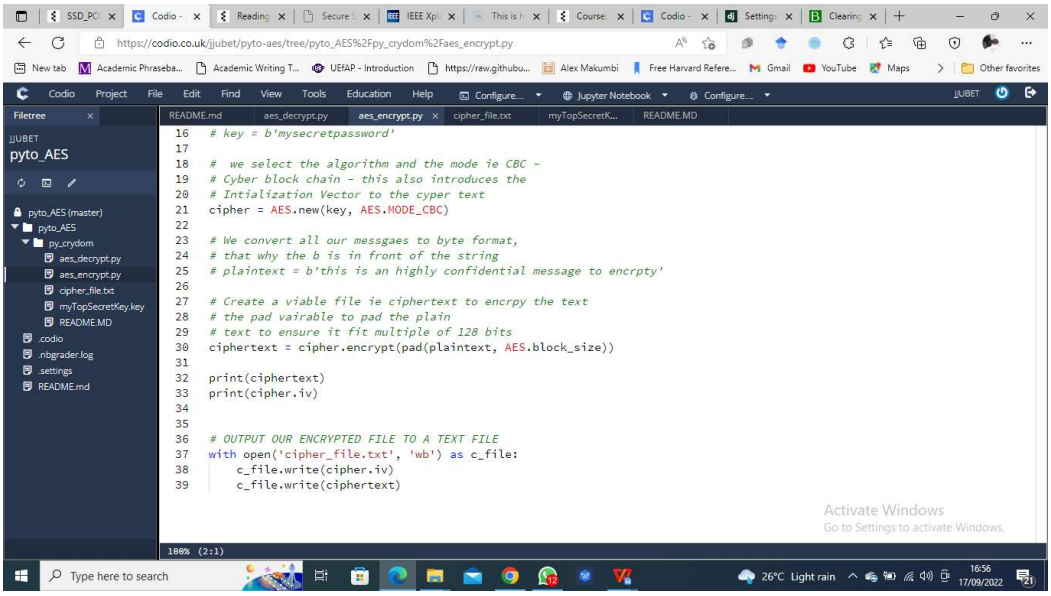
Answer the following questions in your e-portfolio:

Why did you select the algorithm you chose?
Would it meet the GDPR regulations? Justify your answer.

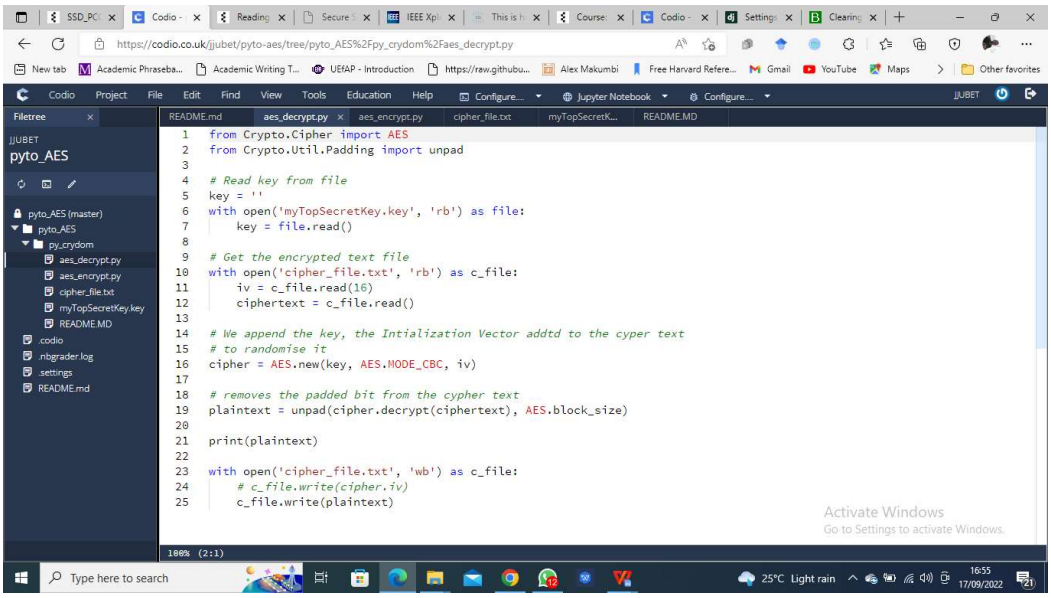
SEE SCREEN SHOTS

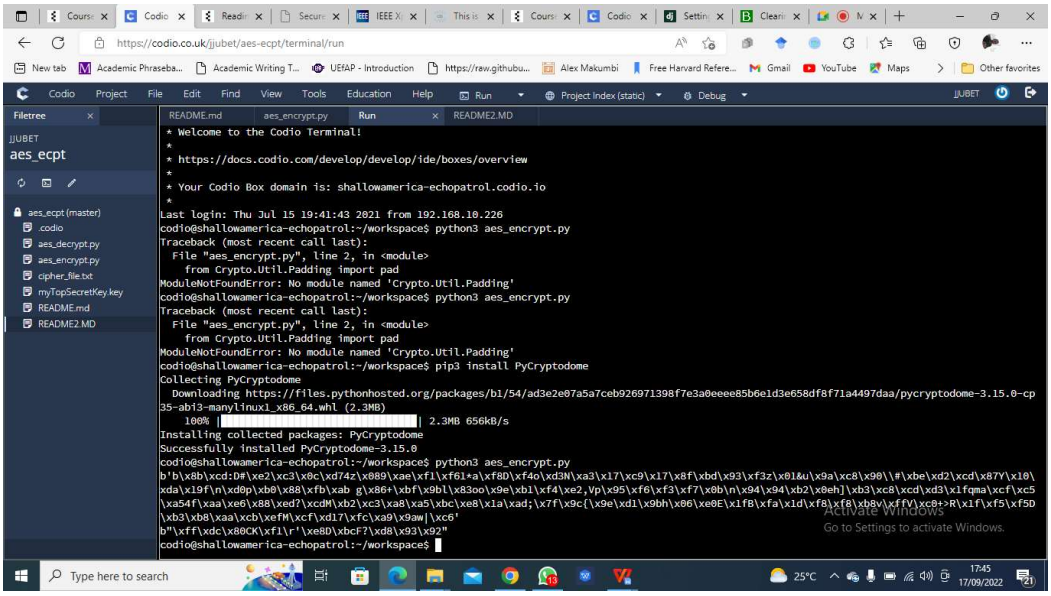
Encrption

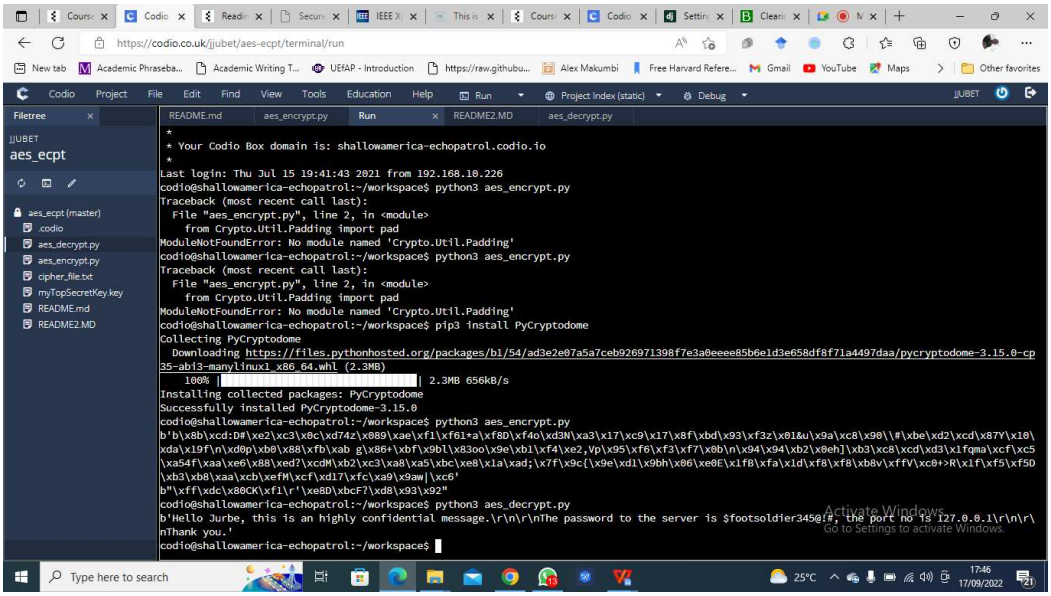



https://codio.co.uk/jjubet/pyto-aes/tree/pyto_AES%2Fpy_crydom%2Faes_encrypt.py
Codio Project File Edit Find View Tools Education Help
Filetree
JJUBET
pyto_AES
pyto_AES (master)
pyto_AES
py_crydom
aes_decrypt.py
aes_encrypt.py
cipher_file.txt
myTopSecretKey.key
README.MD
.codio
.nbgrader.log
.settings
README.md
README.md aes_decrypt.py aes_encrypt.py cipher_file.txt myTopSecretK... README.MD
16 # key = b'mysecretpassword'
17
18 # we select the algorithm and the mode ie CBC -
19 # Cyber block chain - this also introduces the
20 # Intialization Vector to the cyper text
21 cipher = AES.new(key, AES.MODE_CBC)
22
23 # We convert all our messgaes to byte format,
24 # that why the b is in front of the string
25 # plaintext = b'this is an highly confidential message to encrpty'
26
27 # Create a viable file ie ciphertext to encrpy the text
28 # the pad vairable to pad the plain
29 # text to ensure it fit multiple of 128 bits
30 ciphertext = cipher.encrypt(pad(plaintext, AES.block_size))
31
32 print(ciphertext)
33 print(cipher.iv)
34
35
36 # OUTPUT OUR ENCRYPTED FILE TO A TEXT FILE
37 with open('cipher_file.txt', 'wb') as c_file:
38 c_file.write(cipher.iv)
39 c_file.write(ciphertext)
Activate Windows
Go to Settings to activate Windows.
100% (2:1)
Type here to search
26°C Light rain
16:56
17/09/2022

Decryption


https://codio.co.uk/jjubet/pyto-aes/tree/pyto_AES%2Fpy_crydom%2Faes_decrypt.py
Codio Project File Edit Find View Tools Education Help
Filetree
JJUBET
pyto_AES
pyto_AES (master)
pyto_AES
py_crydom
aes_decrypt.py
aes_encrypt.py
cipher_file.txt
myTopSecretKey.key
README.MD
.codio
.nbgrader.log
.settings
README.md
README.md aes_decrypt.py aes_encrypt.py cipher_file.txt myTopSecretK... README.MD
1 from Crypto.Cipher import AES
2 from Crypto.Util.Padding import unpad
3
4 # Read key from file
5 key = ''
6 with open('myTopSecretKey.key', 'rb') as file:
7 key = file.read()
8
9 # Get the encrypted text file
10 with open('cipher_file.txt', 'rb') as c_file:
11 iv = c_file.read(16)
12 ciphertext = c_file.read()
13
14 # We append the key, the Intialization Vector addtd to the cyper text
15 # to randomise it
16 cipher = AES.new(key, AES.MODE_CBC, iv)
17
18 # removes the padded bit from the cypher text
19 plaintext = unpad(cipher.decrypt(ciphertext), AES.block_size)
20
21 print(plaintext)
22
23 with open('cipher_file.txt', 'wb') as c_file:
24 # c_file.write(cipher.iv)
25 c_file.write(plaintext)
Activate Windows
Go to Settings to activate Windows.
100% (2:1)
Type here to search
25°C Light rain
16:55
17/09/2022





Why did you select the algorithm you chose?

AES Encryption is known as a secure encryption algorithm.

Would it meet the GDPR regulations? Justify your answer.