

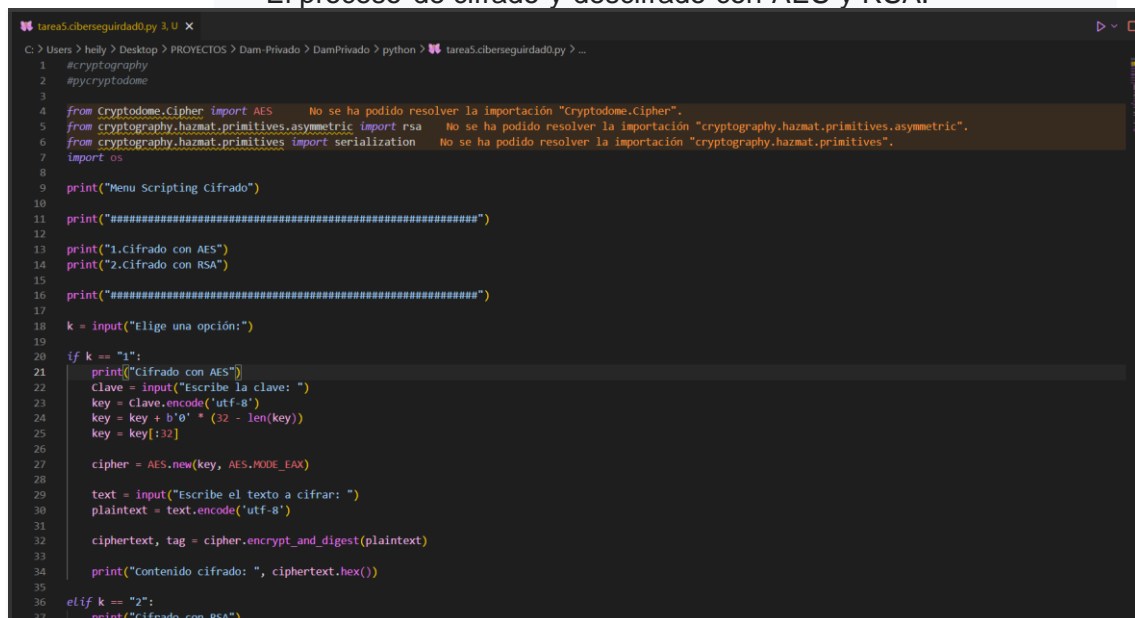
Descripción de la Tarea

Con base en el código proporcionado, se solicita a los alumnos realizar las siguientes modificaciones y desarrollos:

- **Cifrado simétrico:**
 - Implementar cifrado y descifrado utilizando el algoritmo AES con una clave generada aleatoriamente.
 - Utilizar un modo de operación seguro como CBC o GCM.
 - Guardar la clave de cifrado en un archivo separado de los datos cifrados.
- **Cifrado asimétrico:**
 - Generar un par de claves pública y privada utilizando RSA.
 - Utilizar la clave pública para cifrar un mensaje y la clave privada para descifrarlo.
 - Almacenar las claves generadas en archivos separados.

Entregable

- Capturas de pantalla del código y de la ejecución del programa mostrando:
 - La generación de claves.
 - El proceso de cifrado y descifrado con AES y RSA.



```
1 #cryptodome
2 #pycryptodome
3
4 from Cryptodome.Cipher import AES No se ha podido resolver la importación "Cryptodome.Cipher".
5 from cryptography.hazmat.primitives.asymmetric import rsa No se ha podido resolver la importación "cryptography.hazmat.primitives.asymmetric".
6 from cryptography.hazmat.primitives import serialization No se ha podido resolver la importación "cryptography.hazmat.primitives".
7 import os
8
9 print("Menu Scripting Cifrado")
10
11 print("=====")
12
13 print("1.Cifrado con AES")
14 print("2.Cifrado con RSA")
15
16 print("=====")
17
18 k = input("Elige una opción:")
19
20 if k == "1":
21     print("Cifrado con AES")
22     Clave = input("Escribe la clave: ")
23     key = Clave.encode('utf-8')
24     key = key + b'\0' * (32 - len(key))
25     key = key[:32]
26
27     cipher = AES.new(key, AES.MODE_EAX)
28
29     text = input("Escribe el texto a cifrar: ")
30     plaintext = text.encode('utf-8')
31
32     ciphertext, tag = cipher.encrypt_and_digest(plaintext)
33
34     print("Contenido cifrado: ", ciphertext.hex())
35
36 elif k == "2":
37     print("Cifrado con RSA")
```

```
tarea5.ciberseguridad0.py 3, U X
C: > Users > heily > Desktop > PROYECTOS > Dam-Privado > DamPrivado > python > tarea5.ciberseguridad0.py > ...
27 cipher = AES.new(key, AES.MODE_ECB)
28
29 text = input("Escribe el texto a cifrar: ")
30 plaintext = text.encode('utf-8')
31
32 ciphertext, tag = cipher.encrypt_and_digest(plaintext)
33
34 print("Contenido cifrado: ", ciphertext.hex())
35
36 elif k == "2":
37     print("Cifrado con RSA")
38
39     private_key = rsa.generate_private_key(
40         public_exponent=65537,
41         key_size=2048
42     )
43     public_key = private_key.public_key()
44
45     private_pem = private_key.private_bytes(
46         encoding=serialization.Encoding.PEM,
47         format=serialization.PrivateFormat.TraditionalOpenSSL,
48         encryption_algorithm=serialization.NoEncryption()
49     )
50
51     public_pem = public_key.public_bytes(
52         encoding=serialization.Encoding.PEM,
53         format=serialization.PublicFormat.SubjectPublicKeyInfo,
54     )
55
56     print("Clave privada: ", private_pem.decode())
57     print("Clave publica: ", public_pem.decode())
```

```
▼ TERMINAL
PS C:\Users\heily> cd C:\Users\heily\Desktop\PROYECTOS\Dam-Privado\DamPrivado\python
PS C:\Users\heily\Desktop\PROYECTOS\Dam-Privado\DamPrivado\python> python tarea5.ciberseguridad0.py
Menu Scripting Cifrado
#####
1.Cifrado con AES
2.Cifrado con RSA
#####
Elige una opción:1
Cifrado con AES
Escribe la clave: MiClaveSecreta2024!
Escribe el texto a cifrar: Hola Profe
Contenido cifrado: 1d3c185571016e41b065
PS C:\Users\heily\Desktop\PROYECTOS\Dam-Privado\DamPrivado\python> python tarea5.ciberseguridad0.py
Menu Scripting Cifrado
#####
1.Cifrado con AES
2.Cifrado con RSA
#####
Elige una opción:2
Cifrado con RSA
Clave privada: -----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAw/P5FIM+PSydyKEq8qRT45Jxm2pSUWZzG+FecR5rrA9q/wzz
TQXi2LVUVPRp7XTOGRYgpUSI/d03nFnfrnV6Xz6YHZ3oLGdG7GvR/LZ46VeQtaLUM
rMeNq7/qmmmmEsc7V4N6DaGxs/MgFofT0pk/QTuKwKd6F0o2lB+ShH94en2EYyaZ
6TKc0esbM08nmFDue1D0mJTqJhChG/oJtBry8gnJ1B6nJpd06p17opm2R3EJGqW
QC1Fr01HSQkdSj+QzUAwEeAiQFwxFKiC4EMScC6So/nhIMCRmtHdyAA9utjLzo9f
3IX/9d0vu67fubSdVPGzZZzrQR6Oz6uxge/mEwIDAQABaoIBAAQJQn8690kfJ1mX
ryKTFgpDD/Yi4ZaJoVDr14bhLkFz/JjWoEITL+s7D4Gissel11NUTlbeLmowW9xs
dJBVDSG+9iECfy/TNzWJQySGGdG5/zi9Vmh+HfFejhH53coxwxLTRkHFlu9VX1eX
xmCsBC4miYmsOfJMGrTenP9eNDrwEWeggoTrRVvt1+0Vc2ZjShakgcilJk30c+PST
YK6347MH687dprDaadlUr+rVVYSBh2UL4V86v4fnsVE7ZqbqXpQh26daQ+BHn2cE
omE4Rs/OPF2LDPTv8LZxnewyaoXwddkjkGBlY3A/IKYazzwQMB7DFZ79VhHe7zK8
Q9p5/4ECgYEA9pYb2QbSI0xy/OJ/B7+cR+Krh+2IwgKw0Fq+IpeZC5VKHoUA7FmXX
D4zx7NwPnbfAc1Qazr6gEkW5XgoxTrNtDsBotmMnyQMdRR7He4btLrV6wIUZYzom
gsZ5nb7tPmYtamFNQOb5vkoYBXUT1KA+1Prc1m36xZdGq7VAObxfepECgYEAy28G
Ix2l1DgRcnCP0gdHL4ef2GLWztH/dnJvZmFIu/RGF0pDwOgzcTHDXfZs8gZK6iL0
PCQx0p3eLvgoJXxv9iGwZeaXOgrqPssZHHasdzQn9HbmNYTTBTtCZqj7aVa0xsIN
G83IctmtjXxwN5dC2sywc+wfuoXekLi32e+LgGwCgYBoMU1bCtLKzPdPydF8uTqS
xEHw0rCz7g+kdk9bKkyh8Zl1vVo6QJX67Wg+FpoFJLug/6zEJzAkCy1CxZQueQpf
```

▼ TERMINAL

```
MIIEowIBAAKCAQEAW/P5FIM+PSydyKEq8qRT45Jxm2pSUwZzG+FecR5rrA9q/wzz
TQXi2LVUVP RP7XTOGRYgpUSI/d03nFnfnV6Xz6YHZ3oLGdG7GvR/LZ46VeQtALUM
rMeNq7/qmmmmwEsc7V4N6DaGxs/MgFofT0pk/QTuKwKd6F0o2lB+SHH94en2EYyaz
6TkC0esbNM0BnmFDUe1D0mJTqJhChG/oJtBrY8gnJ1B6nJpd06p17opm2R3EJGqW
QC1FrO1HSQkdSj+QzUAWeEaiqFwxfkic4EMsCc6So/nhIMCRmtHdyAA9utjLzo9f
3Ix/9d0vu67fubSdVPGzZZzrQR6Oz6uxge/mEwIDAQAABaoIBAAXJQn8690kfJ1mX
ryKTFgpDD/Yi4ZajoVDr14bhLkfz/JjwoEITL+s7D4Gissel11NUTlbelmowW9xs
dJBVDsg+9iECfy/TNzWJQySGgDg5/z19Vln+HFfeJH53coxwLTrkHF1u9VX1eX
xmCsBC4miYmsOfJMGrTenP9eNDrwEwegg0TrRVvt1+0Vc2ZjShakGciJk30c+pST
YK6347MH687dpRDaad1Ur+rVvYSbh2UL4V86v4fnsve7ZqbqXpQh26daQ+BHn2cE
omE4Rs/OPF21DPTv8LZxnewyaOXWddkjkBgBIY3A/IKYazzwQMB7DFZ79YhHe7zK8
Q9p5/4ECgYEA9pyb2QbsKXy/OJ/B7+cR+Krh+2IwgKw0Fq+IpeZC5VKHoUA7FmXX
D4Zx7MlpNbfAc1Qazr6gEkW5XgoxTrNtDsBotmMnyQMdRR7He4btLrV6wIUZYzoM
gsZ5nb7tPmYtamFNQOb5vkoYBXUT1KA+1Prc1m36xZdGq7VA0bxfepECgYEAy28G
Ix211DgRcnCP0gdHL4ef2GLWztH/dnJvZmFIu/RGf0pDwOgzcTHDXfZs8gZK6iL0
PCQx0p3elVgoJXxv9iGGWZeaXQgrqPssZHHasdzQw9HbmNYTTBTcZqJ7aVaoxsIN
G83IctmtjXxwN5dC2syWc+wfu0xekli32e+LgGCMGYBoMU1bctLKzPdPydF8uTqS
xEHworCz7g+kdk9bKkyh8Z11vVo6QJX67Wg+FpoFJLug/6zEJzAkCylCXzQueQpf
7VVRm9E7WqGHj1XjEEQwNGbF6nerwd9/crX4vbAaatPBAZMokxs54n25F2Yvo10
GSiVSRFPzF5sN44H11zQwQKBgQC0WTTjpMECpsIw5kFaPUGKjX3T46vzppAHfePs
q4pDtodZCYmPV0tjmq48ut5SoemAMIS9XIke4v26Ph25PcUncw14TuJ2Qw2RvTrZ
wXUEKJXBHDdYctJyVDQlHM8K6tsqVPdtk1iJECMEimZ3utR9dXb5xUqgsXEKApN
luPhaQKBghKwfozy1gz7kboqIYks7DIB82zRXKvYybh9TBavf+1Ij/3jz4hytNg
qB5tCQc1sDX52lSKprKzMfPtBmUmpvdLUZkrchws0IS9vxlC6NZmM7wSljwxLF2+
fver34SnjxwW/30JLE5X/sbLlKRWZ7ihpqhOJU72u0kt9oSfHe1
-----END RSA PRIVATE KEY-----
```

Clave publica: -----BEGIN PUBLIC KEY-----

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAW/P5FIM+PSydyKEq8qRT
45Jxm2pSUwZzG+FecR5rrA9q/wzzTQXi2LVUVP RP7XTOGRYgpUSI/d03nFnfnV6X
z6YHZ3oLGdG7GvR/LZ46VeQtALUMrMeNq7/qmmmmwEsc7V4N6DaGxs/MgFofT0pk/
QTuKwKd6F0o2lB+SHH94en2EYyaz6TkC0esbNM0BnmFDUe1D0mJTqJhChG/oJtBr
y8gnJ1B6nJpd06p17opm2R3EJGqWQC1FrO1HSQkdSj+QzUAWeEaiqFwxfkic4EMs
Cc6So/nhIMCRmtHdyAA9utjLzo9f3Ix/9d0vu67fubSdVPGzZZzrQR6Oz6uxge/m
EwIDAQAAB
-----END PUBLIC KEY-----
```

PS C:\Users\heily\Desktop\PROYECTOS\Dam-Privado\DamPrivado\python>