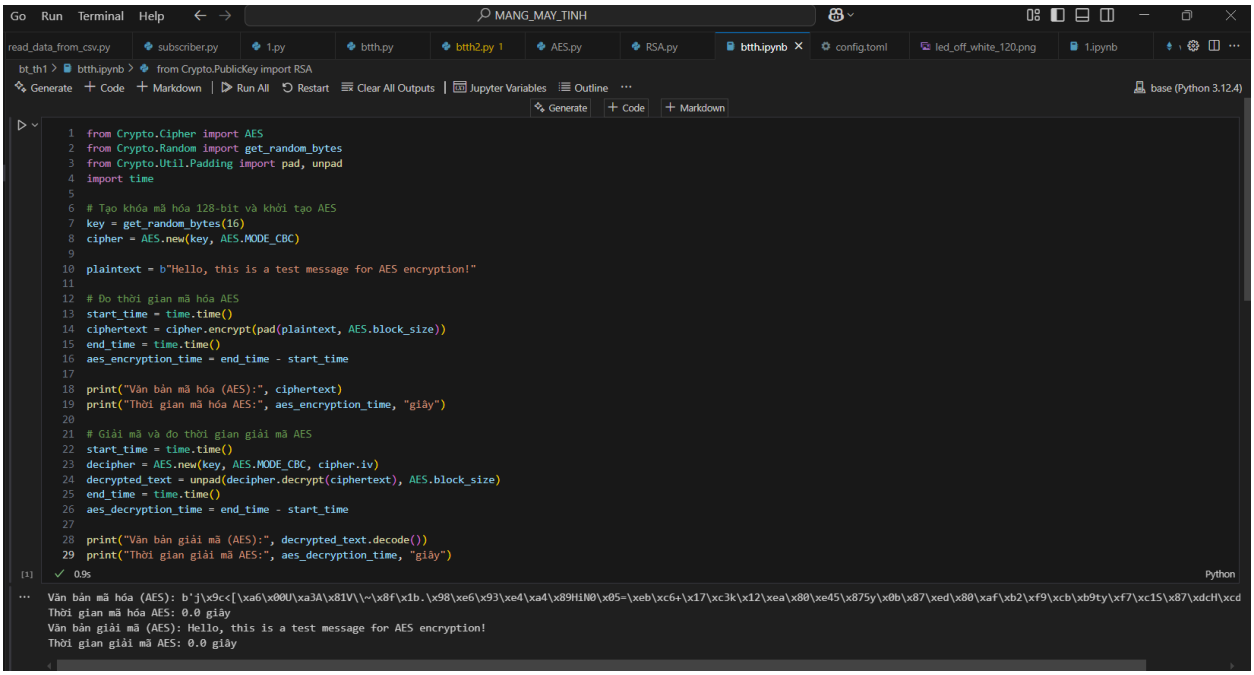
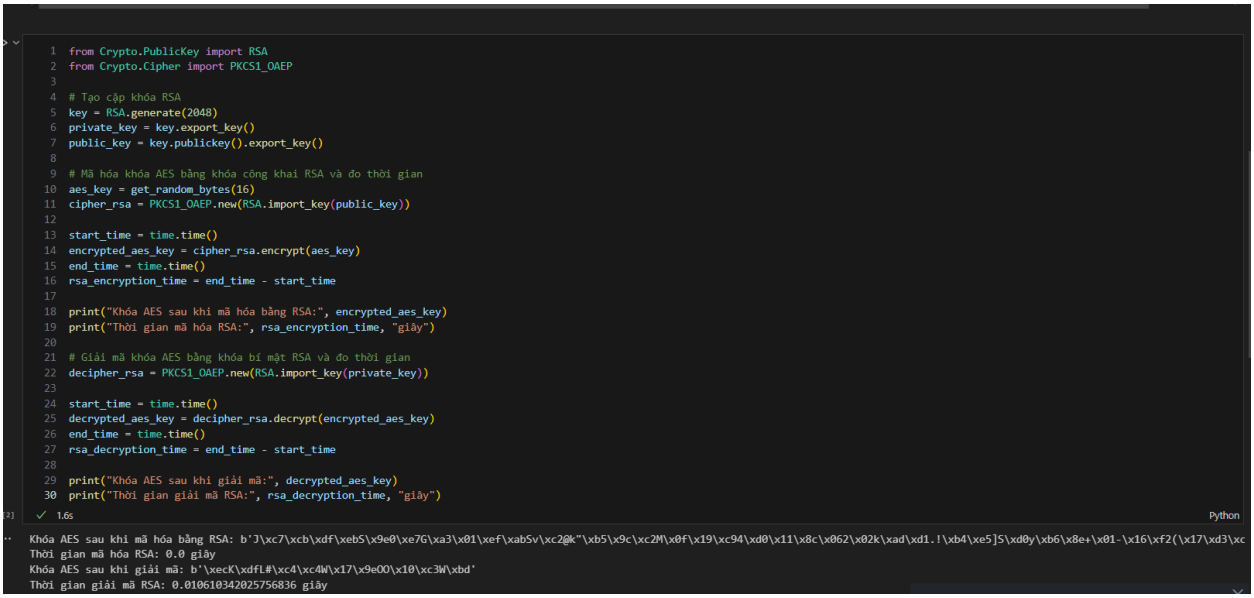
NGUYỄN THỊ NA_ DHKL16A1HN TH1 MSV :22174600084



```python
from Crypto.Cipher import AES
from Crypto.Random import get_random_bytes
from Crypto.Util.Padding import pad, unpad
import time

# Tạo khóa mã hóa 128-bit và khởi tạo AES
key = get_random_bytes(16)
cipher = AES.new(key, AES.MODE_CBC)

plaintext = b"Hello, this is a test message for AES encryption!"

# Đo thời gian mã hóa AES
start_time = time.time()
ciphertext = cipher.encrypt(pad(plaintext, AES.block_size))
end_time = time.time()
aes_encryption_time = end_time - start_time

print("Văn bản mã hóa (AES):", ciphertext)
print("Thời gian mã hóa AES:", aes_encryption_time, "giây")

# Giải mã và đo thời gian giải mã AES
start_time = time.time()
decipher = AES.new(key, AES.MODE_CBC, cipher.iv)
decrypted_text = unpad(decipher.decrypt(ciphertext), AES.block_size)
end_time = time.time()
aes_decryption_time = end_time - start_time

print("Văn bản giải mã (AES):", decrypted_text.decode())
print("Thời gian giải mã AES:", aes_decryption_time, "giây")
```

```
Văn bản mã hóa (AES): b'j\x9c<[\xa6\x00U\xa3A\x81V\\~\x8f\x1b.\x98\xe6\x93\xe4\xa4\x89HiN0\x05=\xeb\xc6+\x17\xc3k\x12\xea\x80\xe45\x875y\x0b\x87\xed\x80\xaf\xb2\xf9\xcb\xb9ty\xf7\xc1S\x87\xdcH\xcd
Thời gian mã hóa AES: 0.0 giây
Văn bản giải mã (AES): Hello, this is a test message for AES encryption!
Thời gian giải mã AES: 0.0 giây
```



```python
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP

# Tạo cặp khóa RSA
key = RSA.generate(2048)
private_key = key.export_key()
public_key = key.publickey().export_key()

# Mã hóa khóa AES bằng khóa công khai RSA và đo thời gian
aes_key = get_random_bytes(16)
cipher_rsa = PKCS1_OAEP.new(RSA.import_key(public_key))

start_time = time.time()
encrypted_aes_key = cipher_rsa.encrypt(aes_key)
end_time = time.time()
rsa_encryption_time = end_time - start_time

print("Khóa AES sau khi mã hóa bằng RSA:", encrypted_aes_key)
print("Thời gian mã hóa RSA:", rsa_encryption_time, "giây")

# Giải mã khóa AES bằng khóa bí mật RSA và đo thời gian
decipher_rsa = PKCS1_OAEP.new(RSA.import_key(private_key))

start_time = time.time()
decrypted_aes_key = decipher_rsa.decrypt(encrypted_aes_key)
end_time = time.time()
rsa_decryption_time = end_time - start_time

print("Khóa AES sau khi giải mã:", decrypted_aes_key)
print("Thời gian giải mã RSA:", rsa_decryption_time, "giây")
```

```
Khóa AES sau khi mã hóa bằng RSA: b'J\xc7\xcb\xdf\xeb5\x9e0\xe7G\xa3\x01\xef\xab5v\xc2@k"\xb5\x9c\xc2M\x0f\x19\xc94\xd0\x11\x8c\x062\x02k\xad\xd1.!\xb4\xe5]5\xd0y\xb6\x8e+\x01-\x16\xf2(\x17\xd3\xc
Thời gian mã hóa RSA: 0.0 giây
Khóa AES sau khi giải mã: b'\xecK\xdfL#\xc4\xc4W\x17\x9eOO\x10\xc3W\xbd'
Thời gian giải mã RSA: 0.010610342025756836 giây
```

```python
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
# Tạo cặp khóa RSA
key = RSA.generate(2048)
private_key = key.export_key()
public_key = key.publickey().export_key()

# Mã hóa khóa AES bằng khóa công khai RSA và đo thời gian
aes_key = get_random_bytes(16)
cipher_rsa = PKCS1_OAEP.new(RSA.import_key(public_key))

start_time = time.time()

print("Khóa AES sau khi giải mã:", decrypted_aes_key)
print("Thời gian giải mã RSA:", rsa_decryption_time, "giây")
```

[3] ✓ 0.1s

```
Khóa AES sau khi giải mã: b'\xecK\xdfL#\xc4\xc4W\x17\x9eOO\x10\xc3W\xbd'
Thời gian giải mã RSA: 0.010610342025756836 giây
```

CÂU HỎI

1. Tại sao mã hóa AES có tốc độ nhanh hơn đáng kể so với RSA?
   AES nhanh hơn RSA vì AES dùng thuật toán đối xứng, chỉ thực hiện các phép toán đơn giản trên khối dữ liệu nhỏ, còn RSA là thuật toán bất đối xứng, phải tính toán số học lớn nên chậm hơn nhiều.
2. Trong thực tế, tại sao người ta thường kết hợp cả AES và RSA trong một hệ thống bảo mật?

   Kết hợp AES và RSA vì RSA dùng để trao đổi khóa AES an toàn qua mạng, còn AES dùng để mã hóa dữ liệu lớn nhanh chóng và hiệu quả.

3. Dựa trên kết quả đo thời gian, loại mã hóa nào phù hợp hơn cho việc mã hóa dữ liệu dung lượng lớn?
   AES phù hợp hơn cho mã hóa dữ liệu dung lượng lớn vì tốc độ nhanh, còn RSA chỉ nên dùng để mã hóa dữ liệu nhỏ như khóa.