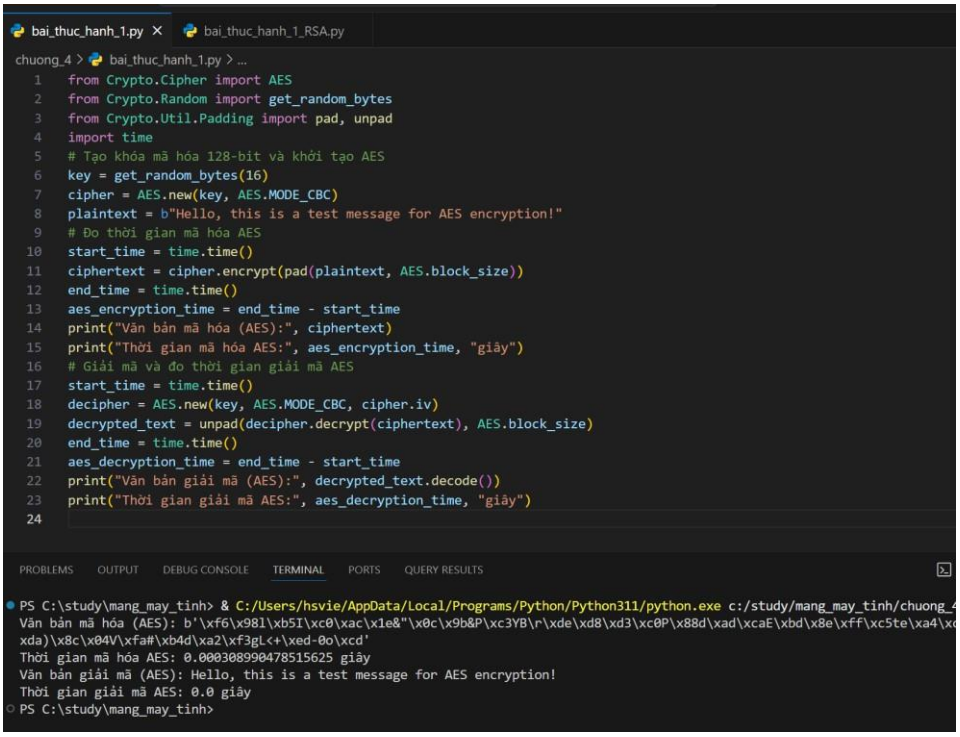
Phạm Thị Thu Trang-22174600030-DHKL16A1HN

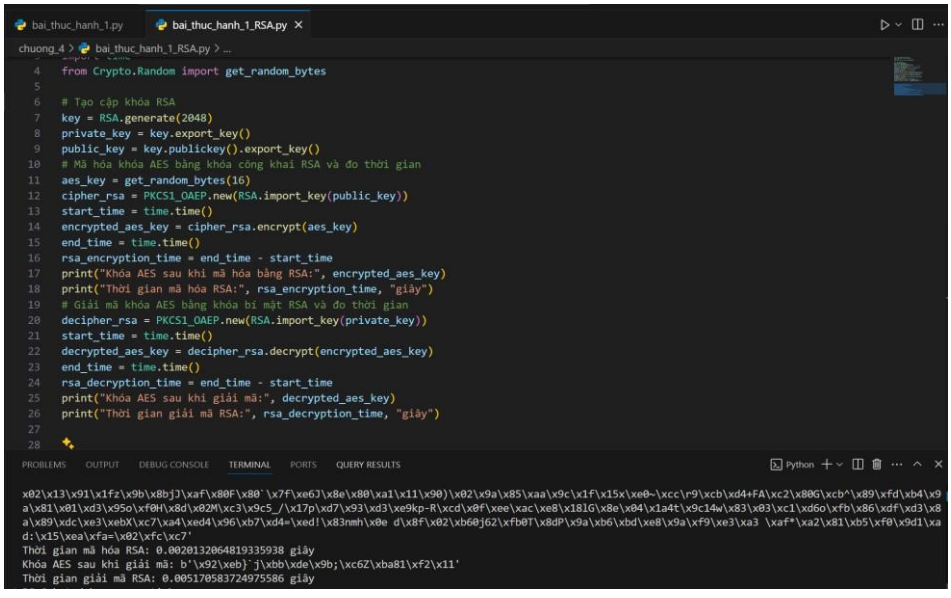
ASE:



```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")
```

```
PS C:\study\mang_may_tinh> & C:/Users/hsvie/AppData/Local/Programs/Python/Python311/python.exe c:/study/mang_may_tinh/chuong_4
Văn bản mã hóa (AES): b'\xf6\x98l\xb5I\xc0\xac\x1e&"\x0c\x9b&P\xc3YB\r\xde\xd8\xd3\xc0P\x88d\xad\xcaE\xbd\x8e\xff\xc5te\xa4\xc
xda)\x8c\x04V\xfa#\xb4d\xa2\xf3gL<+\xed-0o\xcd'
Thời gian mã hóa AES: 0.0003089904785156 25 giây
Văn bản giải mã (AES): Hello, this is a test message for AES encryption!
Thời gian giải mã AES: 0.0 giây
PS C:\study\mang_may_tinh>
```

RSA:

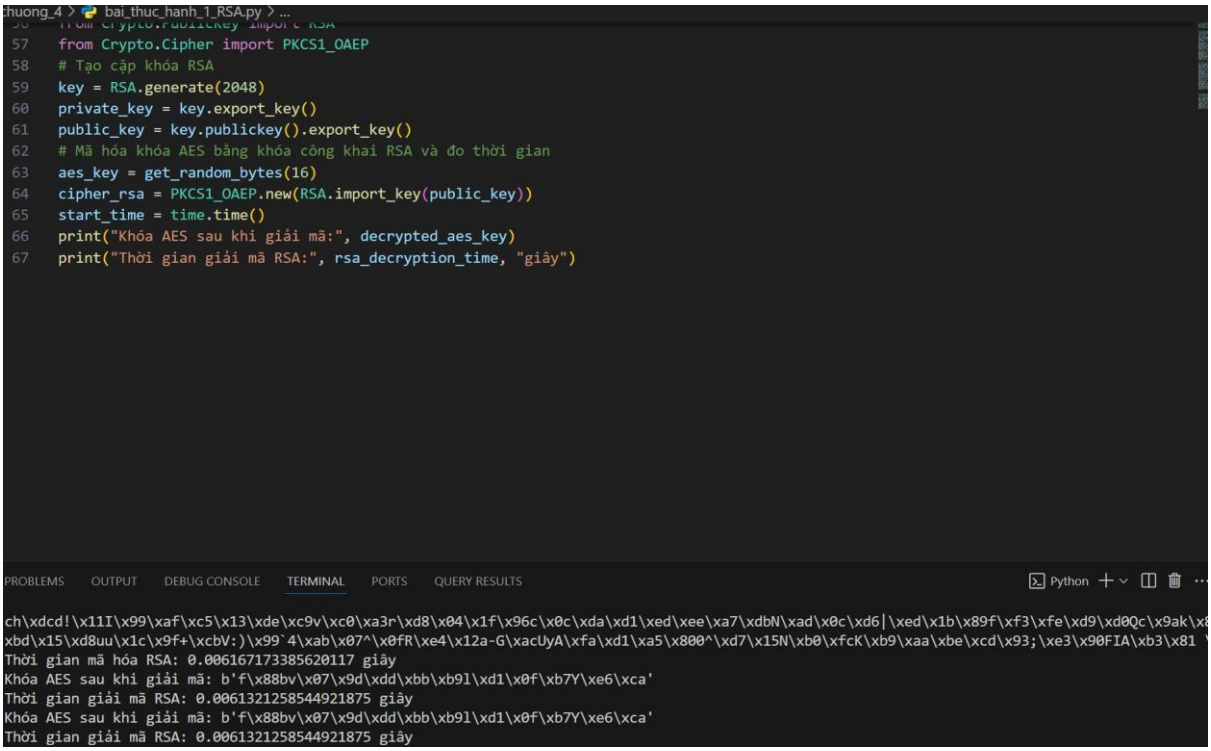


```python
from Crypto.Random import get_random_bytes

# 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")
```

```
x02\x13\x91\x1fz\x9b\x8bjJ\xaf\x80F\x80`\x7f\xe6J\x8e\x80\xa1\x11\x90)\x02\x9a\x85\xaa\x9c\x1f\x15x\xe0~\xcc\r9\xcb\xd4+FA\xc2\x80G\xcb^\x89\xfd\xb4\x9
a\x81\x01\xd3\x95o\xf0H\x8d\x02M\xc3\x9c5_/\x17p\xd7\x93\xd3\xe9kp-R\xcd\x0F\xee\xac\xe8\x181G\x8e\x04\x1a4t\x9c14w\x83\x03\xc1\xd6o\xfb\x86\xdf\xd3\x8
a\x89\xdc\xe3\xebX\xc7\xa4\xed4\x96\xb7\xd4=\xed!\x83nmh\x0e d\x8F\x02\xb60j62\xfb0T\x8dP\x9a\xb6\xbd\xe8\x9a\xf9\xe3\xa3 \xaf*\xa2\x81\xb5\xf0\x9d1\xa
d:\x15\xea\xfa=\x02\xfc\xc7'
Thời gian mã hóa RSA: 0.0020132064819335938 giây
Khóa AES sau khi giải mã: b'\x92\xeb}`j\xbb\xde\x9b;\xc6Z\xba81\xf2\x11'
Thời gian giải mã RSA: 0.0051705837249755 86 giây
```

So sánh :



1. Tại sao mã hóa AES có tốc độ nhanh hơn đáng kể so với RSA?

AES (Advanced Encryption Standard) là thuật toán mã hóa đối xứng, trong khi RSA là thuật toán mã hóa bất đối xứng. Một số lý do AES nhanh hơn đáng kể:

Cấu trúc thuật toán: AES sử dụng các phép toán đơn giản trên khối dữ liệu (substitution, permutation, shift, XOR...) được tối ưu cho phần cứng và phần mềm.

Khóa đối xứng: AES chỉ dùng một khóa, nên quá trình mã hóa và giải mã không cần thực hiện các phép toán số học phức tạp như RSA.

RSA dùng số học lớn: RSA dựa trên các phép toán với số nguyên rất lớn (2048-bit hoặc hơn), ví dụ: lũy thừa modulo của số lớn — chậm hơn rất nhiều so với các phép bitwise của AES.

Tối ưu hóa phần cứng: AES được hỗ trợ phần cứng trên nhiều CPU hiện đại (ví dụ: Intel AES-NI), tăng tốc đáng kể so với RSA vốn khó tối ưu.

2. Trong thực tế, tại sao người ta thường kết hợp cả AES và RSA trong một hệ thống bảo mật?

Đây gọi là hệ thống mã hóa lai (hybrid encryption system). Lý do kết hợp:

RSA để trao đổi khóa AES an toàn: RSA dùng để mã hóa khóa AES, vì nó an toàn khi truyền qua mạng (nhờ tính bất đối xứng).

AES để mã hóa dữ liệu chính: Sau khi trao đổi khóa AES, hệ thống dùng AES để mã hóa dữ liệu thực, vì nhanh và hiệu quả cho dữ liệu lớn.

Lợi ích kép:

Tốc độ cao của AES cho dữ liệu lớn.

Tính bảo mật cao của RSA cho quá trình trao đổi khóa.

Ví dụ thực tế: Giao thức TLS/SSL (dùng trong HTTPS) sử dụng phương pháp kết hợp này.

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 là lựa chọn phù hợp hơn.

Lý do:

Tốc độ cao: AES có thể mã hóa hàng MB/GB dữ liệu với tốc độ cao nhờ thiết kế hiệu quả và hỗ trợ phần cứng.

Chi phí tính toán thấp: AES tiêu tốn ít tài nguyên CPU hơn RSA.

RSA không thích hợp cho dữ liệu lớn: RSA chỉ phù hợp để mã hóa các đoạn dữ liệu nhỏ (ví dụ: khóa AES), vì thời gian mã hóa tăng đáng kể theo kích thước dữ liệu.