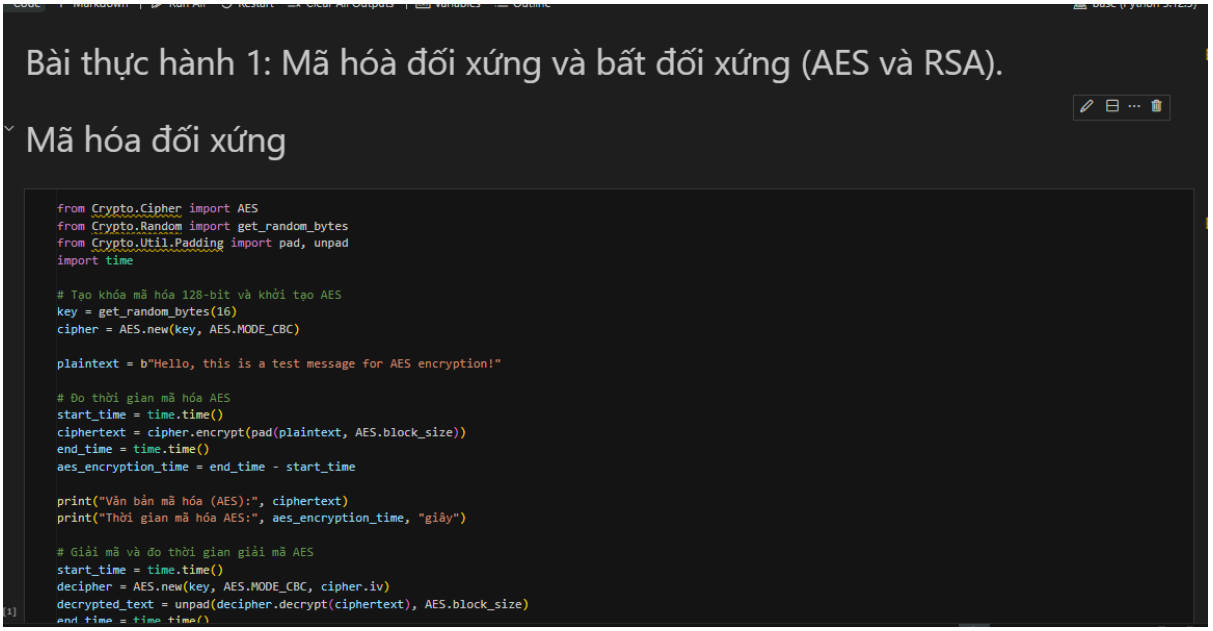
Nguyễn Thị Thanh Hoa
MSV:22174600052
Lớp:DHKL16A1HN

Bài thực hành 1: Mã hóa đối xứng và bất đối xứng (AES và RSA).



```python
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")
```

0.1s Python

```
Văn bản mã hóa (AES): b'I(\x06\xaaFGc(\xe9\xb3\x12\xa0\xfcc\xc3\xf6\x08\xbd\xe3\x01\xd0]\x12\x1e\xeau\x04\xc4>\xc3B\xb2\xec\xb7\xf8\xcb\xff\x0f\x11\x8c\x12\x17\x84\xbe'
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
```

Mã hóa bất đối xứng

```python
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
from Crypto.Random import get_random_bytes
import time

# 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
```

[2]

```
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")
```

1.9s Python

```
Khóa AES sau khi mã hóa bằng RSA: b';\xd4\xfa\x8dCTt\xfd~0\x9c\xf37C\xe7$r\x0b\xf6}9\xdc\xcf\xbc\xf7e\x8b\x8a1D1\x8a>\xc0\x14\xd6\xaf\xff\'\x80\xdf/)\xe8\x1f\xebH\xda}
Thời gian mã hóa RSA: 0.0009968280792236328 giây
Khóa AES sau khi giải mã: b'\xe7\x95\xe1\xea\xc6\ns\xe8\x08\x05\xec\x92\xe6\xe0\x94\xb1'
Thời gian giải mã RSA: 0.00897669792175293 giây
```

So sánh thời gian thực thi giữa AES và RSA

```
print("----- So sánh thời gian mã hóa -----")
print(f"Thời gian mã hóa AES: {aes_encryption_time:.6f} giây")
print(f"Thời gian mã hóa RSA: {rsa_encryption_time:.6f} giây")

print("\n----- So sánh thời gian giải mã -----")
print(f"Thời gian giải mã AES: {aes_decryption_time:.6f} giây")
print(f"Thời gian giải mã RSA: {rsa_decryption_time:.6f} giây")

if aes_encryption_time < rsa_encryption_time:
    print("\nMã hóa AES nhanh hơn mã hóa RSA")
else:
    print("\nMã hóa RSA nhanh hơn mã hóa AES")

if aes_decryption_time < rsa_decryption_time:
    print("Giải mã AES nhanh hơn giải mã RSA")
else:
    print("Giải mã RSA nhanh hơn giải mã AES")
```

0.0s Python

```
----- So sánh thời gian mã hóa -----
Thời gian mã hóa AES: 0.000000 giây
Thời gian mã hóa RSA: 0.001993 giây

----- So sánh thời gian giải mã -----
Thời gian giải mã AES: 0.000000 giây
Thời gian giải mã RSA: 0.007978 giây

Mã hóa AES nhanh hơn mã hóa RSA
Giải mã AES nhanh hơn giải mã RSA
```

Câu hỏi thảo luận:

1. Tại sao mã hóa AES có tốc độ nhanh hơn đáng kể so với RSA?
   - AES nhanh hơn RSA nhiều lần vì bản chất thuật toán đơn giản hơn và được hỗ trợ bởi phần cứng.
2. Trong thực tế, tại sao người ta thường kết hợp cả AES và RSA trong một hệ thống bảo mật?

Vì:

- AES nhanh và hiệu quả, nhưng cần chia sẻ khóa bí mật một cách an toàn.
- RSA an toàn để trao đổi khóa, nhưng không phù hợp để mã hóa dữ liệu lớn do tốc độ chậm.

3. Dựa trên kết quả đo thời gian, loại mã hóa nào phù hợp hơn cho việc mã hóa dữ liệu dung lượng lớn?

Kết quả thực nghiệm:

- AES mã hóa: ~0.000000 giây
- RSA mã hóa: ~0.001993 giây

- AES giải mã:~0.000000 giây
- RSA giải mã: ~0.007978 giây

- Phân tích:
  -Mã hóa dung lượng lớn yêu cầu xử lý hàng nghìn khối dữ liệu — nếu dùng RSA thì sẽ cực kỳ chậm.
  - AES được thiết kế để mã hóa dữ liệu lớn hiệu quả, đặc biệt trong môi trường thời gian thực (streaming, lưu trữ, truyền thông tin...).

- Kết luận: AES là lựa chọn phù hợp nhất cho mã hóa dữ liệu dung lượng lớn do tốc độ vượt trội và hiệu suất cao.