NGUYỄN QUANG HUY - DHKL16A1HN

MSV: 22174600113

Bài thực hành 1:

```
start_time = time.time()
ciphertext = cipher.encrypt(pad(plaintext.encode(), 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")
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'\xbfh|\xe9\x9a\x99%b\x05\xd7B\x18_j\xa1r\xca\xc6!\xc0\x87\xf6\xc7[\xa5\xd3b\x92
Thời gian mã hóa AES: 0.0014858245849609375 giây
Văn bản giải mã (AES): Hello, this is a test message for AES encryption!
Thời gian giải mã AES: 0.0003459453582763672 giây
Văn bản giải mã (AES): Hello, this is a test message for AES encryption!
```

```
# Corrected typo from PKCS1_0AEP to PKCS1_OAEP
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
# Corrected typo from PKCS1_0AEP to PKCS1_OAEP
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'U|\x08\x06(\x9d6\x0f\xaa\x12W\xcd\xfe\x9d@\x84L\xb2&92\xacy^\xb5\xcd
Thời gian mã hóa RSA: 0.0015218257904052734 giây
Khóa AES sau khi giải mã: b'\xae\x95n\x81\xa4\xa7\xaa\xc1\x01R\xba\x8d\xbe\x85ES'
Thời gian giải mã RSA: 0.0022797584533691406 giây
```

```python
from Crypto. PublicKey import RSA
# Corrected typo from PKCS1_0AEP to PKCS1_OAEP
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()
start_time = time.time()
# Mã hóa khóa AES bằng khóa công khai RSA và đo thời gian aes_key= get_random_bytes(16)
aes_key = get_random_bytes(16) # Added missing aes_key definition
cipher_rsa = PKCS1_OAEP.new(RSA. import_key(public_key))
print("Khóa AES sau khi giải mã:", decrypted_aes_key)
print("Thời gian giải mã RSA:", rsa_decryption_time, "giây")
```

```
Khóa AES sau khi giải mã: b'\xae\x95n\x81\xa4\xa7\xaa\xc1\x01R\xba\x8d\xbe\x85ES'
Thời gian giải mã RSA: 0.0022797584533691406 giây
```

1. Tại sao mã hóa AES có tốc độnhanh hơnđángkể so với RSA?

• AES (Advanced Encryption Standard) là một thuật toán mã hóa đối

xứng, sử dụng cùng một khóa cho cả mã hóa và giải mã. Các thuật toán đối

xứng như AES hoạt động theo các khối dữ liệu và được thiết kế để thực hiện

nhanh, hiệu quả trên cả phần cứng lẫn phần mềm.

• RSA là thuật toán mã hóa bất đối xứng, sử dụng cặp khóa công khai

và bí mật, và dựa vào các phép toán số học phức tạp như lũy thừa mô-đun

trên các số nguyên rất lớn. Do đó, RSA tiêu tốn nhiều tài nguyên tính toán hơn.

Kết luận: Mã hóa AES nhanh hơn RSA do sự đơn giản và hiệu quả trong

thiết kế thuật toán, trong khi RSA chậm hơn vì bản chất toán học phức tạp.

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

thống bảo mật?

• RSA được dùng để bảo mật việc truyền khóa, còn AES được dùng để

mãhóadữliệu.

• Cách kết hợp thường thấy là:

o Khóa AES (tạo ngẫu nhiên) được mã hóa bằng RSA.

o Dữliệu thực tế được mãhóabằngAES (vì nhanh và hiệu quả).

• Phươngpháp này đượcgọi là mãhóalai (hybrid encryption):

o Kết hợptính bảo mật cao của RSA choquản lý khóa.

o Kết hợptốc độxử lýnhanh của AES chodữliệu lớn.

Kết luận: Kết hợp AES và RSA tận dụng điểm mạnh của cả hai: bảo mật khóa tốt (RSA) và tốc độ mã hóa dữ liệu nhanh (AES).

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

• Từkết quảtrong đoạn code:

o AES mãhóavàgiải mãmấtdưới0.01 giây.

o RSAmấtthời gian dài hơn rõ rệt cho cùng thao tác.

• AES có thể xử lý hàng MB hay GB dữ liệu rất nhanh, còn RSA chỉ thích hợp đểmãhóanhữngđoạndữliệu nhỏ(nhưkhóaphiên).

Kết luận: AES là lựa chọn phù hợp hơn để mã hóa dữ liệu dung lượng lớn, trong khi RSA chỉ nên dùng để mã hóa khóa hoặc dữ liệu nhỏ