Họ tên:Nguyễn Văn Duy
Mã sinh viên:22174600011
Lớp:DHKL16A1HN

Bước 1 : Mã hóa và giải mã bằng AES

```python
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 đã 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 đã mã hóa (AES): b')\xac\x9c\x95B\x85\xcbB\x04\xe8O\xb1\x13\xda\x9d\xcc\x9c\xf9C\x8c\xc7p\xcd\xef\x82{M\xc9\x16\xaa\x8eE\xba\x1fK]=2H\xcd^jMv\x85X\x93V9}\:
Thời gian mã hóa AES: 0.002006053924560547 giây
Văn bản giải mã (AES): Hello, this is a test message for AES encryption!
Thời gian giải mã AES: 0.0 giây
```

Bước 2 : Mã hóa và giải mã bằng RSA

```python
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")
```

✓ 1.8s Python

```
Khóa AES sau khi mã hóa bằng RSA: b'\xbc>g\x91\xf2\xc9\xf2I\xf3\xcb\x1b\xddI\x859\x06\x04T\x07\xe2\x97\x1c7\x98\xe3\xffyu\xc9a\xf3\xf3}R7\x158\xd3\xa5;K\xe7\xb4\>
Thời gian mã hóa RSA: 0.0 giây
Khóa AES sau khi giải mã: b'\xfaI\x00e\x83\xb3q\x16\x12\xb4\xcd\x02\x18\xe7\xc1,'
Thời gian giải mã RSA: 0.0 giây
```

Bước 3 : So sánh thời gian thực thi giữa AES và RSA

AES nhanh hơn RSA rất nhiều trong hầu hết trường hợp thực tế, đặc biệt khi xử lý dữ liệu lớn.

Họ tên:Nguyễn Văn Duy
Mã sinh viên:22174600011
Lớp:DHKL16A1HN

AES mất khoảng 2 mili-giây (ms) để mã hóa dữ liệu văn bản.

RSA trong trường hợp này chỉ dùng để mã hóa khóa AES, nên mất gần như không đáng kể thời gian (0.0 giây, nhưng thực tế có thể là vài micro-giây, chỉ là quá nhỏ để hiện thị rõ ràng).

Tiêu chí	**AES**	**RSA**
Loại thuật toán	Đối xứng	Bất đối xứng
Tốc độ	Rất nhanh (xử lý khối)	Chậm hơn, không phù hợp cho dữ liệu lớn
Dùng cho	Mã hóa dữ liệu chính	Mã hóa khóa (nhỏ, ví dụ như AES key)
Kích thước dữ liệu	Có thể xử lý dữ liệu lớn	Thường chỉ dùng với dữ liệu nhỏ