

NGUYỄN THỊ NA_DHKL16A1HN TH1 MSV :22174600084

```
Go Run Terminal Help ← → MANG_MAY_TINH
read_data_from_csv.py subscriber.py 1.py btth.py btth2.py 1 AES.py RSA.py btthipynb x config.toml led_off_white_120.png 1.ipynb
bt_th1 > btthipynb > from Crypto.PublicKey import RSA
Generate + Code + Markdown Run All Restart Clear All Outputs Jupyter Variables Outline ... base (Python 3.12.4)

1 from Crypto.Cipher import AES
2 from Crypto.Random import get_random_bytes
3 from Crypto.Util.Padding import pad, unpad
4 import time
5
6 # Tạo khóa mã hóa 128-bit và khởi tạo AES
7 key = get_random_bytes(16)
8 cipher = AES.new(key, AES.MODE_CBC)
9
10 plaintext = b"Hello, this is a test message for AES encryption!"
11
12 # Đo thời gian mã hóa AES
13 start_time = time.time()
14 ciphertext = cipher.encrypt(pad(plaintext, AES.block_size))
15 end_time = time.time()
16 aes_encryption_time = end_time - start_time
17
18 print("Văn bản mã hóa (AES):", ciphertext)
19 print("Thời gian mã hóa AES:", aes_encryption_time, "giây")
20
21 # Giải mã và đo thời gian giải mã AES
22 start_time = time.time()
23 decipher = AES.new(key, AES.MODE_CBC, cipher.iv)
24 decrypted_text = unpad(decipher.decrypt(ciphertext), AES.block_size)
25 end_time = time.time()
26 aes_decryption_time = end_time - start_time
27
28 print("Văn bản giải mã (AES):", decrypted_text.decode())
29 print("Thời gian giải mã AES:", aes_decryption_time, "giây")
[1] ✓ 0.9s Python

... Văn bản mã hóa (AES): b'j\x9c[\xa6\x00\xa3A\x81V\-\x8f\x1b.\x98\xe6\x93\xe4\x89HIN0\x05-\xeb\xc6+\x17\xc3k\x12\xea\x80\xe45\x875y\x0b\x87\xed\x80\xaf\xb2\xfa9\xcb\xb9ty\xf7\xc15\x87\xdcf\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
```

```
1 from Crypto.PublicKey import RSA
2 from Crypto.Cipher import PKCS1_OAEP
3
4 # Tạo cặp khóa RSA
5 key = RSA.generate(2048)
6 private_key = key.export_key()
7 public_key = key.publickey().export_key()
8
9 # Mã hóa khóa AES bằng khóa công khai RSA và đo thời gian
10 aes_key = get_random_bytes(16)
11 cipher_rsa = PKCS1_OAEP.new(RSA.import_key(public_key))
12
13 start_time = time.time()
14 encrypted_aes_key = cipher_rsa.encrypt(aes_key)
15 end_time = time.time()
16 rsa_encryption_time = end_time - start_time
17
18 print("Khóa AES sau khi mã hóa bằng RSA:", encrypted_aes_key)
19 print("Thời gian mã hóa RSA:", rsa_encryption_time, "giây")
20
21 # Giải mã khóa AES bằng khóa bí mật RSA và đo thời gian
22 decipher_rsa = PKCS1_OAEP.new(RSA.import_key(private_key))
23
24 start_time = time.time()
25 decrypted_aes_key = decipher_rsa.decrypt(encrypted_aes_key)
26 end_time = time.time()
27 rsa_decryption_time = end_time - start_time
28
29 print("Khóa AES sau khi giải mã:", decrypted_aes_key)
30 print("Thời gian giải mã RSA:", rsa_decryption_time, "giây")
[1] ✓ 1.6s Python

... Khóa AES sau khi mã hóa bằng RSA: b'J\xc7\xcb\xdf\xeb5\x9e0\xe7G\xa3\x81\xef\xab5v\xc2gk"\xb5\x9c\xc2M\x0f\x19\xc94\xd0\x11\x8c\x862\x02k\xad\xd1.!\xb4\xe5J\xdb8y\xb6\x8e+\xb1-\x16\xf2(\xcd7\xd3\xc
Thời gian mã hóa RSA: 0.0 giây
Khóa AES sau khi giải mã: b'\xecK\xdfL#\xc4\xc4\x17\x9e00\x10\xc3W\xbd'
Thời gian giải mã RSA: 0.010610342025756836 giây
```

```
1 from Crypto.PublicKey import RSA
2 from Crypto.Cipher import PKCS1_OAEP
3 # Tạo cặp khóa RSA
4 key = RSA.generate(2048)
5 private_key = key.export_key()
6 public_key = key.publickey().export_key()
7
8 # Mã hóa khóa AES bằng khóa công khai RSA và đo thời gian
9 aes_key = get_random_bytes(16)
10 cipher_rsa = PKCS1_OAEP.new(RSA.import_key(public_key))
11
12 start_time = time.time()
13
14 print("Khóa AES sau khi giải mã:", decrypted_aes_key)
15 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\x9e00\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.