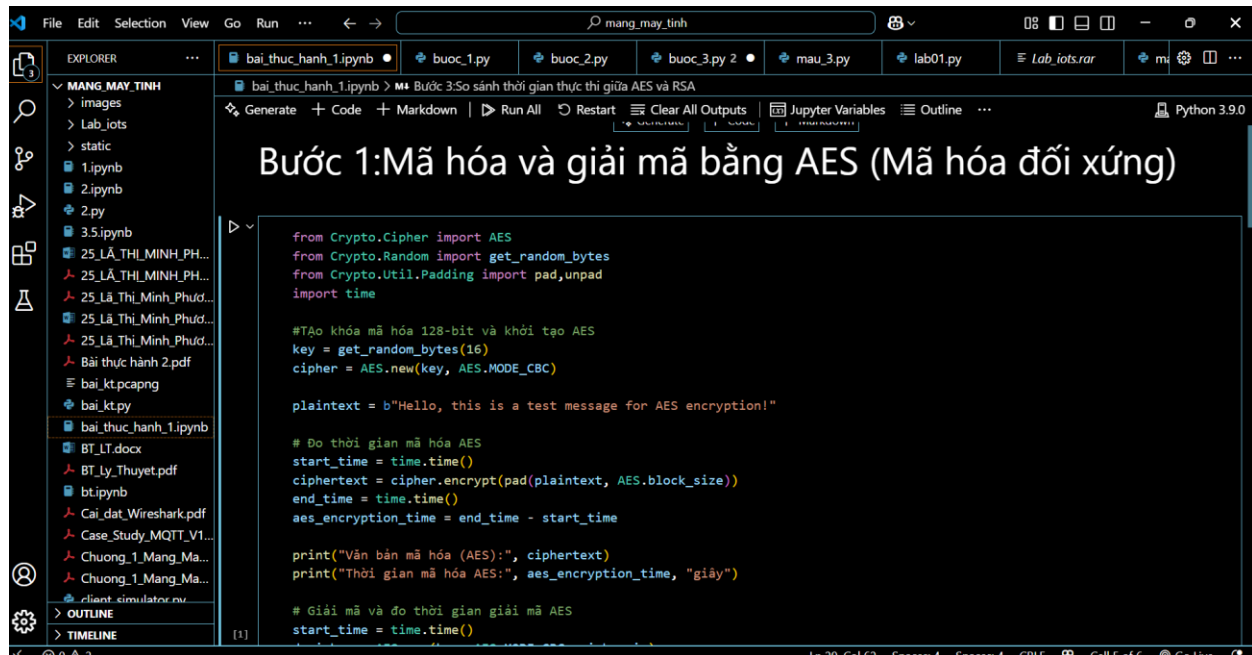


Bài TH1



The screenshot shows a Jupyter Notebook interface with the title "Bước 1: Mã hóa và giải mã bằng AES (Mã hóa đối xứng)". The code in the cell is as follows:

```
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!"

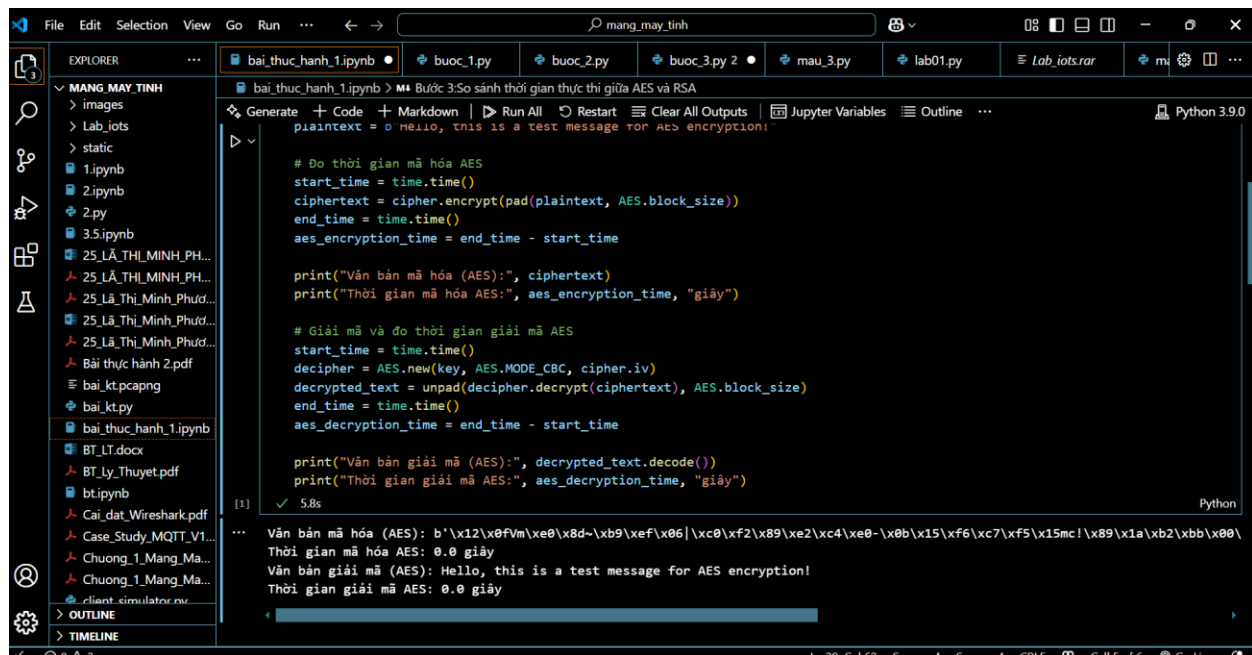
# Đo thời gian mã hóa AES
start_time = time.time()
ciphertext = cipher.encrypt(pad(plaintext, AES.block_size))
end_time = time.time()
aes_encryption_time = end_time - start_time

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()
```

The output of the code is:

```
Văn bản mã hóa (AES): b'\x12\xf0m\x08\x8d~\xb9\xef\x06|\xc0\xf2\x89\xe2\xc4\xe0-\x0b\x15\xf6\xc7\xf5\x15mc|\x89\x1a\xb2\xbb\x00'
Thời gian mã hóa AES: 0.0 giây
```



The screenshot shows the continuation of the Jupyter Notebook, focusing on the decryption part of the code. The code in the cell is as follows:

```
# 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")
```

The output of the code is:

```
Văn bản giải mã (AES): Hello, this is a test message for AES encryption!
Thời gian giải mã AES: 0.0 giây
```

File Edit Selection View Go Run ... mang_may_tinh

EXPLORER ...

▼ MANG MAY TINH

- > images
- > Lab_iots
- > static
- 1.ipynb
- 2.ipynb
- 2.py
- 3.5.ipynb
- 25_LA_THI MINH PH...
- 25_LA_THI MINH PH...
- 25_La_Thi_Minh_Phuc...
- 25_La_Thi_Minh_Phuc...
- 25_La_Thi_Minh_Phuc...
- Bài thực hành 2.pdf
- bai_ktcpang
- bai_kt.py
- bai_thuc_hanh_1.ipynb
- BT_LT.docx
- BT_Ly_Thuyet.pdf
- bt.ipynb
- Cai_dat_Wireshark.pdf
- Case_Study_MQTT_V1...
- Chuong_1_Mang_Ma...
- Chuong_1_Mang_Ma...
- client_simulator.py
- OUTLINE
- TIMELINE

bai_thuc_hanh_1.ipynb > Bước 3: So sánh thời gian thực thi giữa AES và RSA

Generate + Code + Markdown | Run All Restart Clear All Outputs Jupyter Variables Outline ... Python 3.9.0

Bước 2 :Mã hóa và giải mã bằng AES (Mã hóa đối xứng)

```
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
from Crypto.Random import get_random_bytes
from Crypto.Util.Padding import pad, unpad
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")
```

[2] # Giải mã khóa AES bằng khóa bí mật RSA và đo thời gian

Ln 29, Col 62 Spaces: 4 Spaces: 4 CRLF Cell 5 of 6 Go Live

File Edit Selection View Go Run ... mang_may_tinh

EXPLORER ...

▼ MANG MAY TINH

- > images
- > Lab_iots
- > static
- 1.ipynb
- 2.ipynb
- 2.py
- 3.5.ipynb
- 25_LA_THI MINH PH...
- 25_LA_THI MINH PH...
- 25_La_Thi_Minh_Phuc...
- 25_La_Thi_Minh_Phuc...
- 25_La_Thi_Minh_Phuc...
- Bài thực hành 2.pdf
- bai_ktcpang
- bai_kt.py
- bai_thuc_hanh_1.ipynb
- BT_LT.docx
- BT_Ly_Thuyet.pdf
- bt.ipynb
- Cai_dat_Wireshark.pdf
- Case_Study_MQTT_V1...
- Chuong_1_Mang_Ma...
- Chuong_1_Mang_Ma...
- client_simulator.py
- OUTLINE
- TIMELINE

bai_thuc_hanh_1.ipynb > Bước 3: So sánh thời gian thực thi giữa AES và RSA

Generate + Code + Markdown | Run All Restart Clear All Outputs Jupyter Variables Outline ... Python 3.9.0

```
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")
```

[2] ✓ 1.6s Python

... Khóa AES sau khi mã hóa bằng RSA: b'\x03i!E\xe7\xa1\xb5\x96&\xce\x9daY\xda\x8e\x0X\x95\x9c\xd7E\xe1\xce[;\x94\x05]\x01\x01\x0ePe
Thời gian mã hóa RSA: 0.0017178058624267578 giây
Khóa AES sau khi giải mã: b'\xfdf',\x00-\x14\xfc\xdf\x16\x08\x9fo\xe4\x0f"
Thời gian giải mã RSA: 0.014525413513183594 giây

Ln 29, Col 62 Spaces: 4 Spaces: 4 CRLF Cell 5 of 6 Go Live

File Edit Selection View Go Run ...

mang_may_tinh

Lab_iots.rar

EXPLORER

MANG_MAY_TINH

images

Lab_iots

static

1.ipynb

2.ipynb

2.py

3.5.ipynb

25_LA_THI_MINH_PH...

25_LA_THI_MINH_PH...

25_La_Thi_Minh_Phuc...

25_La_Thi_Minh_Phuc...

Bai_thuc_hanh_2.pdf

bai_kt.pcapng

bai_kt.py

bai_thuc_hanh_1.ipynb

BT_LT.docx

BT_Ly_Thuyet.pdf

bt.ipynb

Cai_dat_Wireshark.pdf

Case_Study_MQTT_V1...

Chuong_1_Mang_Ma...

Chuong_1_Mang_Ma...

client_simulator.py

OUTLINE

TIMELINE

bai_thuc_hanh_1.ipynb

buoc_1.py

buoc_2.py

buoc_3.py 2

mau_3.py

lab01.py

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

Generate

Code

Markdown

Run All

Restart

Clear All Outputs

Jupyter Variables

Outline

Python 3.9.0

```
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")
```

[2] ✓ 1.6s

Python

...

Khóa AES sau khi mã hóa bằng RSA: b'\x03i!E\xe7\xa1\xb5\x96&\xce\x9daY\xda\x8e\x0X\x95\x9c\x7E\xe1\xce[\x94\x05]\x01\x01\xcePe'
Thời gian mã hóa RSA: 0.0017178058624267578 giây
Khóa AES sau khi giải mã: b'\xfd',\xaa0-\x14\xfc\xdf\x16\x08\x9fo\xe4\x0f"
Thời gian giải mã RSA: 0.014525413513183594 giây

Ln 29, Col 62 Spaces: 4 Spaces: 4 CRLF

Cell 5 of 6

Go Live