

제목: 공개키 암호화 과정 이해하기

이름: 홍길동

학번: 2345678

암호화 관련 프로그램 설치

```
!pip install pycryptodome
```

Requirement already satisfied: pycryptodome in /usr/local/lib/python3.10/dist-packages (3.20.0)

1. 홍길동 키생성

```
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
```

```
# 한 쌍의 키 생성
key_pair = RSA.generate(2048)
```

```
# 개인키 생성
private_key = key_pair.export_key()
print('홍길동 개인키 :', private_key)
```

```
# 공개키 생성
public_key = key_pair.publickey().export_key()
print('홍길동 공개키 :', public_key)
```

```
홍길동 개인키 : b'-----BEGIN RSA PRIVATE KEY-----WnMII EogI BAAKCAQE A4KcwEISsYdPTH2SL0wmmbcE+gz3a96Wj iH1ht6eI8U0X4YkWnUBEfrcnJRkp5Yo1Fr sZZIPLc33+s73+wxYyrWn8QSFdNznW5:
홍길동 공개키 : b'-----BEGIN PUBLIC KEY-----WnMII B1jANBgkqhkiG9w0BAQEFAAOC AQ8AMI BCGKCAQE A4KcwEISsYdPTH2SL0wmmWnbcE+gz3a96Wj iH1ht6eI8U0X4YkWnUBEfrcnJRkp5Yo1Fr sZZIPLc33+s73+wxYyrWn8QSFdNznW5:
-----END PUBLIC KEY-----'
```

2. 홍길동이 임꺽정에게 공개키 전달

```
print(public_key)
```

```
xDxFvif8N3iNMajdjH2PxQKWtKoyokXTgCTdjVo00npWnyKCdxvB4t08w6ToXrpa3xvfXHWfE1fZUZRGhZQuXybCoUmyI48cBNuJXHncdFEf0WnbwIDAQABWn-----END PUBLIC KEY-----'
```

3. 임꺽정이 홍길동의 공개키 확보

임꺽정은 홍길동으로부터 전달받은 공개키 저장

주의사항: 공개키는 생성할 때마다 달라짐. 따라서 공개키를 새로 생성할 때마다 새로 생성된 공개키를 저장해야 함

```
public_key = b'-----BEGIN PUBLIC KEY-----WnMII B1jANBgkqhkiG9w0BAQEFAAOC AQ8AMI BCGKCAQE A4KcwEISsYdPTH2SL0wmmWnbcE+gz3a96Wj iH1ht6eI8U0X4YkWnUBEfrcnJRkp5Yc
```

```
public_key
```

```
b'-----BEGIN PUBLIC KEY-----
WnMII B1jANBgkqhkiG9w0BAQEFAAOC AQ8AMI BCGKCAQE A4KcwEISsYdPTH2SL0wmmWnbcE+gz3a96Wj iH1ht6eI8U0X4YkWnUBEfrcnJRkp5Yo1Fr sZZIPLc33+s73+wxYyrWn8QSFdNznW5:
-----END PUBLIC KEY-----'
```

4. 임꺽정이 메시지 생성

전송할 메시지 생성

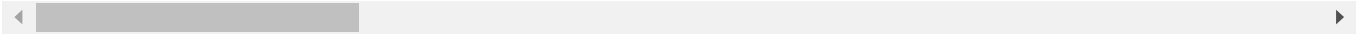
```
message = '임꺽정 임시 ID: XYZ345, 임꺽정이 좋아하는 동물 : 강아지 '
```

5. 임꺽정이 홍길동의 공개키로 메시지 암호화

```
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
```

```
cipher_text = PKCS1_OAEP.new(RSA.import_key(public_key)).encrypt(message.encode('utf-8'))
cipher_text
```

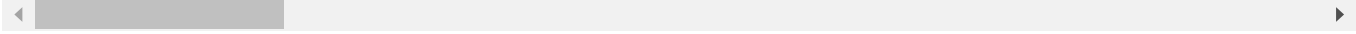
```
b' lWx feWxdeWxc7Wxd3Wx1cWxa8WtWxe8*Wx86Wxf2Wxe2Wxc0[Wx feWxbaeWxbeWx7f i |Wxf fWx89xWx16Wxe2WxaaWxcc%Wxa1WxdWxbdbWx12tWxaa3Wxf3Wxa6Wx96pWxc7Wxd5)
Wx05Wxf1Wxf fWx15Wxf4hWx82Wxc2Wxb20Hwxc7WxecWxa0Wx94Wxf7Wx99RWxbcbWxf eWx03gaWxeaWx8bWxc fWxf aWx01Wxe9Wxf7Wxd27Wxc8Wxfb^WxceWxe50Wx84WxdfWxc fYWxbbdz
```



6. 임꺽정이 암호문을 홍길동에게 전달

```
print(cipher_text)
```

```
b' lWx feWxdeWxc7Wxd3Wx1cWxa8WtWxe8*Wx86Wxf2Wxe2Wxc0[Wx feWxbaeWxbeWx7f i |Wxf fWx89xWx16Wxe2WxaaWxcc%Wxa1WxdWxbdbWx12tWxaa3Wxf3Wxa6Wx96pWxc7Wxd5)
Wx05Wxf1Wxf fWx15Wxf4hWx82Wxc2Wxb20Hwxc7WxecWxa0Wx94Wxf7Wx99RWxbcbWxf eWx03gaWxeaWx8bWxc fWxf aWx01Wxe9Wxf7Wxd27Wxc8Wxfb^WxceWxe50Wx84WxdfWxc fYWxbbdz
```



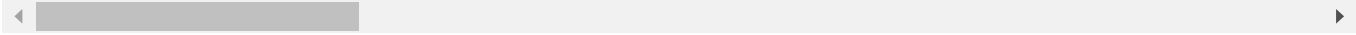
7. 홍길동은 전달받은 암호문을 불러옴

```
# 암호화된 메시지 불러오기
# 주의사항: 새로 생성된 공개키로 암호문을 만들었으면, 새로 암호문을 저장해야 오류가 발생하지 않음
```

```
cipher_text = b' lWx feWxdeWxc7Wxd3Wx1cWxa8WtWxe8*Wx86Wxf2Wxe2Wxc0[Wx feWxbaeWxbeWx7f i |Wxf fWx89xWx16Wxe2WxaaWxcc%Wxa1WxdWxbdbWx12tWxaa3Wxf3Wxa6Wx96pWxc7Wxd5)
Wx05Wxf1Wxf fWx15Wxf4hWx82Wxc2Wxb20Hwxc7WxecWxa0Wx94Wxf7Wx99RWxbcbWxf eWx03gaWxeaWx8bWxc fWxf aWx01Wxe9Wxf7Wxd27Wxc8Wxfb^WxceWxe50Wx84WxdfWxc fYWxbbdz
```

```
cipher_text
```

```
b' lWx feWxdeWxc7Wxd3Wx1cWxa8WtWxe8*Wx86Wxf2Wxe2Wxc0[Wx feWxbaeWxbeWx7f i |Wxf fWx89xWx16Wxe2WxaaWxcc%Wxa1WxdWxbdbWx12tWxaa3Wxf3Wxa6Wx96pWxc7Wxd5)
Wx05Wxf1Wxf fWx15Wxf4hWx82Wxc2Wxb20Hwxc7WxecWxa0Wx94Wxf7Wx99RWxbcbWxf eWx03gaWxeaWx8bWxc fWxf aWx01Wxe9Wxf7Wxd27Wxc8Wxfb^WxceWxe50Wx84WxdfWxc fYWxbbdz
```



8. 홍길동은 자신의 개인키로 암호문을 복호화

```
# 개인키로 암호문을 복호화하기
message = PKCS1_OAEP.new(RSA.import_key(private_key)).decrypt(cipher_text).decode('utf-8')
message
```

```
'임꺽정 임시 ID: XYZ345, 임꺽정이 좋아하는 동물 : 강아지 '
```