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-----₩nMIIEogIBAAKCAQEA4KcwEISsYdPTH2SL0wmmbcbE+gz3a96WjiHIht6eI8U0X4YkW₩nUBEfrcnJRkp5Yo1FrsZZIPLc33+s
홍길동 공개키 : b'-----BEGIN PUBLIC KEY-----₩nMIIBIjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIBCgKCAQEA4KcwEISsYdPTH2SL0wmm₩nbcbE+gz3a96WjiHIht6eI8U0X4YkUBEfr
```

2.홍길동이 임꺽정에게 공개키 전달

```
print(public_key)
```

```
xDxFvf8N3iNMajdjHZPxQKWtKoyokXTgCTdjVo00npWnyKCdxvB4t08w6ToXrpa3xvfXHWfE1fZUZRGhZQuXybCoUmyI48cBNuJXHncdFEf0Wnbw1DAQAB₩n-----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-----₩nMIIBIjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIBCgKCAQEA4KcwEISsYdPTH2SL0wmm₩nbcbE+gz3a96WjiHIht6eI8U0X4YkUBEfrcnJRkp5Yo

public_key
```

```
b'-----BEGIN PUBLIC KEY-----
₩nMIIBIjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIBCgKCAQEA4KcwEISsYdPTH2SL0wmm₩nbcbE+gz3a96WjiHIht6eI8U0X4YkUBEfrcnJRkp5Yo1FrsZZIPLc33+s73+wxYyr₩n8QSfDNznW5
----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'I₩xfe₩xde₩xc7₩xd3₩x1c₩xa8₩tW₩xe8*₩x86₩xf2₩xe2₩xc0[₩xfe₩xbae₩xbe₩x7fi|₩xff₩x89x₩x16₩xe2₩xaa₩xcc%₩xa1₩x9d₩xbdb₩x12t₩xaa3₩xf3₩xa6₩x96p₩x0c₩xc7₩xd5
₩x05₩xf1₩xff₩x15₩xf4h₩x82₩xc2₩xb20H₩xc7₩xec₩xa0₩x94₩xf7₩x99R₩xbc₩xfe₩x03ga₩xea₩x8b₩xcf₩xfa₩x01₩xe9₩xf7₩xd27₩xc8₩xfb^₩xce₩xe50₩x84₩xdf₩xcfY₩xbbdz
```

6.임꺽정이 암호문을 홍길동에게 전달

```
print(cipher_text)
```

```
b'I₩xfe₩xde₩xc7₩xd3₩x1c₩xa8₩tW₩xe8*₩x86₩xf2₩xe2₩xc0[₩xfe₩xbae₩xbe₩x7fi|₩xff₩x89x₩x16₩xe2₩xaa₩xcc%₩xa1₩x9d₩xbdb₩x12t₩xaa3₩xf3₩xa6₩x96p₩x0c₩xc7₩xd5
```

7.홍길동은 전달받은 암호문을 불러옴

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

cipher_text = b'I₩xfe₩xde₩xc7₩xd3₩x1c₩xa8₩tW₩xe8*₩x86₩xf2₩xe2₩xc0[₩xfe₩xbae₩xbe₩x7fi|₩xff₩x89x₩x16₩xe2₩xaa₩xcc%₩xa1₩x9d₩xbdb₩x12t₩xaa3₩xf3₩xa6₩x96p₩x0c₩

cipher_text
```

```
b'I₩xfe₩xde₩xc7₩xd3₩x1c₩xa8₩tW₩xe8*₩x86₩xf2₩xe2₩xc0[₩xfe₩xbae₩xbe₩x7fi|₩xff₩x89x₩x16₩xe2₩xaa₩xcc%₩xa1₩x9d₩xbdb₩x12t₩xaa3₩xf3₩xa6₩x96p₩x0c₩xc7₩xd5
₩x05₩xf1₩xff₩x15₩xf4h₩x82₩xc2₩xb20H₩xc7₩xec₩xa0₩x94₩xf7₩x99R₩xbc₩xfe₩x03ga₩xea₩x8b₩xcf₩xfa₩x01₩xe9₩xf7₩xd27₩xc8₩xfb^₩xce₩xe50₩x84₩xdf₩xcfY₩xbbdz
```

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 '
```