Create Ransomware with RSA

Encryption with AES

- طبعا زي ما احنا عارفين اني نوع التشفير AES هو Symmetric Key يعني نفس المفتاح بيستخدم فالتشفير وفك التشفير واتعلمنا نعمل كده ازاي فالدروس السابقه

Encryption with RSA

- دا بقي نوع ال RSA اللي بستخدم فيه مفتاحين وواحد public للتشفير وال private للتشفير
- تعالي بقي اقولك ازاي نعمل الكلام ده

Import Librarys and Generate Keys

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

pair_keys = RSA.generate(1024)

private_key = pair_keys.export_key()
public_key = pair_keys.public_key().export_key()

print(private_key)
print(public_key)
```

- اول حاجه استدعيت المكتبات زي مانت شايف عادي
- بعد كده `pair_keys = RSA.generate(1024)` هنا انا بقولو اعملي مفتاح بحجم 1024 بت يعني 128 بايت يعني طول المفتاح 128 حرف
- خلي بالك هو هيعمل مفتاح واحد وهو ال private طب احنا هنجيب ال public ازاي؟ تعالي اقولك بقي
- اول حاجه `private_key = pair_keys.export_key()s` انا بقولو هنا الpair_keys ده اعملي ليه export وحطهولي ف متغير اسمه private_key
- وانا من ال private key هطلع ال public بص كده

`()public_key = pair_keys.public_key().export_key`

- بقولو هنا ياباشا اعملي export للpublic key من ال pair_keys وحطهولي ال public_key

- وبعد كده بقولو اطبعهملي عادي بقي عشان اخدهم كوبي عندي

Encrypt Data

- خلي بالك زي ما اتفقنا اني اللي بيشفر ال public

```
public_key = b'-----BEGIN PUBLIC KEY-----
\nMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQChi+hafkfuuvUQaTyI4EmVThml\nxgstYVBBmHa3phk
OheD+D5OxT29Znc3tkwvwScg85lmsruJnWbeCVVpYDb17m3zy\n/Rokvs33WzQdRE+Pdg10A6nUeT/qFfXD
WXrmRr+kqwY4VscXf56QFCvgE3pD+RhH\n7f/xSXoSKZ6zjRCN3wIDAQAB\n-----END PUBLIC KEY----
-'

imported_public_key = RSA.import_key(public_key)

enc = PKCS1_OAEP.new(imported_public_key)

data = b"this is tantawy"
encrypted_data = enc.encrypt(data)

print(encrypted_data)
```

- اول حاجه الكود بتاع عمل المفاتيح ده ممكن اشيله خلاص عادي براحتك كده كده احنا عملنا مفتاحين وخدناهم كوبي
- اول حاجه هعمل متغير اسمه public_key وهحط فيه الpublic key اللي طلعناه من الكود اللي فات عشان ده اللي هنشفر بيه
- وبعد كده عاوز اقول للبايثون استخدملي المفتاح ده فا انا هعمله import بقي مش export لما جيت اكريت المفتاح عملت export بقولو صدرلي مفتاح انما هنا انا بقولو استورد المفتاح ده
  `imported_public_key = RSA.import_key(public_key)`
  وخزنته ف متغير اسمه `imported_public_key
- بعد كده عاوز اقوله خلاص استخدملي المفتاح ده فالتشفير بقي فا هقوله
  `enc = PKCS1_OAEP.new(imported_public_key)`
  كده خلاص انا بقوله دا المفتاح اللي هشفر بيه
- هعمل بقي متغير اسمه data وهيكون فيه الحاجه اللي هتتشفر انا عن نفسي هشفر الكلمه دي دلوقتي
  `"data = b"this is tantawy`
- عاوز اقوله بقي شفر ياعم الجمله دي
  `encrypted_data = enc.encrypt(data)`
  من خلال فانكشن encrypt بقوله شفر الحاجه اللي جوا المتغير data وخزنهولي ف ال encrypted_data

- وبعد كده بقوله اطبعلي ال encrypted_data ده فا طبعا هيطبعلي الكلمه متشفره كلها علامات وحروف مش مفهومه

Decrypt Data

- هنا بقي هوريك كود فك التشفير والمفروض انه مش محتاج شرح ولاحظ التغيير

```
private_key = '-----BEGIN RSA PRIVATE KEY-----
\nMIICXAIBAAKBgQChi+hafkfuuvUQaTyI4EmVThmlxgstYVBBmHa3phkOheD+D5Ox\nT29Znc3tkwvwScg
85lmsruJnWbeCVVpYDb17m3zy/Rokvs33WzQdRE+Pdg10A6nU\neT/qFfXDWXrmRr+kqwY4VscXf56QFCvg
E3pD+RhH7f/xSXoSKZ6zjRCN3wIDAQAB\nAoGAPRbaK/ZbH1UFvUn+gUhHqzVYj46/xU5qehO8uSAPk6Ve+
tRLJp8CXaJGMFQO\nDLTqCtWVDa8ooKqVsayzOF8hytWEAM1P5Fi4LuYo9cpqUgkrbkMo/9Fl2tYHH+YC\n
kZG5nCe5iuxR9iUoHvwL1MOjEDyyJdkwLJbJmO+Bhih8dkECQQDCy9ZGcE3501h3\n4p+vEn4wB4ggFprEG
60MpEPqX9EwXK1lSGme26emn7hk5VLWAfdI6WckE9Eq6jPw\nSYgjecL/AkEA1E2s8X533VIOCro5N6aR6g
BukuCIZ7lgKzXbO3krVaIcxAEGt4nm\nQV0WwX+/v1DHkoXOkFLttgYdU6iDRCCVIQJADM7ELutxZQytU2y
WHTe1DklgfOOf\nl2dOcHdYc8+K/IgLao5hS22bz0vPHuspECMe9C9MdcXLyeuOMK1VAygdVwJAN7SZ\n6F
Oyx9O783yhfsSqDKhIWymnIPA3F59uAtDsWe/LdHKAfLAmRohSbDtE6MIdW4jY\nhm38CYLZNxZEOyABgQJ
BAJdBGIzeHJnW7oVS7x6LQz+U932e8QcxsmaieOuSWbxW\nNESSiYv21DHJXqAqN1vR79Kazhqp9fH3kBWH
n1qr3j0=\n-----END RSA PRIVATE KEY-----'

imported_private_key = RSA.import_key(private_key)

enc = PKCS1_OAEP.new(imported_private_key)

data =
b"3;\xda\x1a\xe7\xec1YE\xbfep\x17w\xd1\xf5\xe5\xd1\xf2w\xc1(\x90\xef\xef\xe1f\xf0e\
x17\x10\x14\x1fb\xae\xc3(\xceDD'v\xe1\xd0\xfb\xe7\xf4\x1d\xac\x088\xce\x92\x88n\xec
\xe6q\x86\xbeq]\xcb\x88>\xf9\x06-
4\xc7\x1c\xac,\xdf\x0bQ\xb4\xa1\x1bo/\xe8I\xd3%\xea/h\xec?
P\x15;\xc1\x116\x7f\xe2u\xfe\xba\x7fH\xb2\x13\xe5\xa09,\xff\x9a\xe5!\x19\xea\xb1(8\
xad\x98y\x11\xef\xda\xea\xa8Nf"

encrypted_data = enc.decrypt(data)

print(encrypted_data)
```

- هنا بدل ما احطلو ال public زي فوق لأ هحطلو ال private عشان البرايفت اللي بفك بيه
- متغير ال `data` هنا التشفير بتاع الحاجه اللي متشفره فاهمني؟
- وبس بدل ما استخدم فانكشن `encrypt` عشان اشفر لأ انا هقوله `decrypt`