Create Ransomware with DES

مبدأيا كدا عشان اقدر اشفر او استعمل مودويل التشفير فالبايثون لازم اسطب مكتبة pycryptodome

```
pip install pycryptodome
```

Encryption with AES (CTR)

- بص ياباشا احنا عرفنا اني انواع التشفير AES و DES و RSA
- احنا بقي هنستخدم ال AES بوضع اسمه CTR (Counter Mode)
- مبدأيا عشان ابدأ اعمل عملية التشفير هقولك علي تلت مودويلات جوا ال pycryptodome لازم تستخدمهم و هفهمك ليه

```
from Crypto.Cipher import AES
from Crypto import Random
from Crypto.Util import Counter
```

- اول حاجه `from Crypto.Cipher import AES` انا هنا بقوله هاتلي المودويل AES وده اللي هيعملي المفتاح
- تاني حاجه `from Crypto import Random` هنا انا بقوله لما تعملي key اعملهولي random الحروف والارقام يعني ميكونش الkey ب sqeuence او بتسلسل عشان دي هتكون سهل ال fuzzing
- تالت حاجه `from Crypto.Util import Counter` هنا انا بقوله هاتلي مودويل ال counter وهو اساس ال CTR

- اول حاجه عشان اعمل key اصلا تعالي اقولك تعمل ايه

```
from Crypto.Cipher import AES
from Crypto import Random
from Crypto.Util import Counter

def genKey():
    return(Random.new().read(16))
key = genKey()
```

- انا عملت فانكشن هنا اسمها `genKey` جوا الفانكشن دي بترجعلي المفتاح

- قولتله `return(Random.new().read(16))` قولتلو هنا Random يعني المفتاح يبقي عشوائي و `read(16)` يعني طول المفتاح 16 بت يعني 8 بايت
- بس كده وحطيت المفتاح اللي الفانكشن هترجعهولي ف متغير اسمه key

عملية التشفير

```
from Crypto.Cipher import AES
from Crypto import Random
from Crypto.Util import Counter

def encryption(key, word):
    counter = Counter.new(128)
    c = AES.new(key, AES.MODE_CTR, counter=counter)
    print(c.encrypt(word.encode('ascii')))

def genKey():
    return(Random.new().read(16))

key = genKey()

encryption(key, 'this is mohamed')
```

- واحده واحده عملنا هنا فانكشن اسمها `encryption` وليها اتنين بارامیتر اول واحد هو `key` وده هيبقي المفتاح اللي احنا عملنا من شويه وتاني واحد `word` ودي الكلمه اللي هنشفرها
- بعد كدا `counter = Counter.new(128)` أنت كده بتنشئ عداد بطول 128 بت (يعني 16 بايت)، والعداد ده بيتغير مع كل عملية تشفير، بحيث ما يبقاش فيه بلوك متكرر بنفس النتيجة المشفرة حتى لو دخلت نفس النص الأصلي أكتر من مرة
- بعد كدا `c = AES.new(key, AES.MODE_CTR, counter=counter)` ال AES هيا بتخلطلي كل ده وبتطلعلي مفتاح رايق متغلف اعتبر ده بيغلف المفتاح هو بيعوز مني المفتاح والمود وهو هنا ف حالتنا دي CTR وبعد كدا بتديلو الcounter بس كده يبقي انت كده معاك مفتاح رايق ومتظبط
- هنا `print(c.encrypt(word.encode('ascii')))` انت بتقوله شفرلي بقي الكلمه وف نفس الوقت خليها ascii encoding برضو عشان اتجنب اي اخطاء
- اخر حاجه `encryption(key, 'this is mohamed')` خلاص هنا اديتلو الkey واديتلو الword اللي هيا دي اللي هتتشفر
- تعالي بقي اوريك الoutput

`'b'\x05V%\xb2\x14\xcf\xa1 gV\xdc\x97Q/B`

- انت عارف ده ايه؟ دي كلمة this is mohamed بس متشفره وبكدا تكون نجحت عملية التشفير وخلي بالك لازم تاخد ال key زي ماطلعلك مينفعش تغير فيه حاجه

طريقة فك التشفير

- الطريقه هي هي بتاعت التشفير هنغير حاجات بسيطه بس

- طبعا دلوقتي انا كا واحد عاوز افك التشفير اكيد هيكون معايا الحاجه اللي متشفره اللي هيا دي `'b'\x05V%\xb2\x14\xcf\xa1 gV\xdc\x97Q/B`

```
from Crypto.Cipher import AES
from Crypto import Random
from Crypto.Util import Counter

def encryption(key, word):
    counter = Counter.new(128)
    c = AES.new(key, AES.MODE_CTR, counter=counter)
    print(c.decrypt(word))

def genKey():
    return(Random.new().read(16))

key = genKey()

encryption(key, b'\x05V%\xb2\x14\xcf\xa1 gV\xdc\x97Q/B')
```

- بس كده احنا هنا غيرنا كلمة encryption خليناها decryption وحطينا مكان الجمله الحاجه اللي متشفره لم اعمل run هيطلعلي الكلمه اللي عاوزين نفك تشفيرها وهي `this is mohamed`