Drugi izvještaj

Pokrenuli smo virtualno okruženje u Pythonu, da ne smetamo globalnom okruženju. Za enkripciju smo koristili biblioteku cryptography.

Pokrećemo okruženje s python -m venp srp

```
cd lkevric
cd srp
cd Scripts
activate
```

Instaliramo biblioteku cryptography, prisutnu samo u ovom virtualnom okruženju

```
pip install cryptography
```

Generiramo enkripcijski ključ, spremamo ga u varijablu key. Plaintext je podatak kojeg želimo enkriptirati, u binarnom formatu.

```
fromcryptography.fernetimport Fernet
key = Fernet.generate_key()
f = Fernet(key)
plaintext = b"Hello world"
ciphertext = f.encrypt(plaintext)
```

Crypto challenge

Izazov skidamo sa internog servera, pišemo skriptu u Visual Studio Code-u.

Naredbom brute_force.py nam se ispiše ime našeg filea. Znamo da je rješenje slika, pa početak svakog dekriptiranog plaintexta provjeravamo je li se radi o png headeru.

```
from cryptography.hazmat.primitives import hashes

def hash(input):
```

```
    if not isinstance(input, bytes):
        input = input.encode()

    digest = hashes.Hash(hashes.SHA256())
    digest.update(input)
    hash = digest.finalize()

    return hash.hex()

filename = hash('prezime_ime') + ".encrypted"

def test_png(header):
    if header.startswith(b"\211PNG\r\n\032\n"):
        return True
def brute_force():
    filename="ime_filea.encrypted"
    with open(filename, "rb") as file:
       ciphertext=file.read()

    ctr=0
    while True:
        key_bytes = ctr.to.bytes(32, "big")
        key = base64.urlsafe.b64encode(key_bytes)

        if not (ctr+1)%1000:
             print(f"[*] Keys tested: {ctr+1:,}", end ="\r")
        try:
           plaintext = Fernet(key).decrypt(ciphertext)
           header = plaintext[:32]

           if test_png(header):
               print(f"[+] KEY FOUND: {key}")

                with open("BINGO.png", "wb") as file:
                    file.write(plaintext)
                break
           except Exception:

           ctr+=1

if __name__ == " main ":

hash_value=hash("kevric_laura")

print(hash_value)
```

Konačno rješenje:

Congratulations Kevric Laura!

You made it!