3.laboratorijska vjezba

Na trećoj laboratorijskoj vježbi trebalo je dešifrirati *ciphertext,* a za to nismo imali pristup enkripcijskom ključu. Upoznali smo se sa načinom na koji možemo enkriptirati i dekriptirati poruke korištenjem Fernet sustava. Na sljedećoj adresi http://challenges.local nalazila su se imena koja su predstavljala naša *hash* imena i prezimena. Najlakši način za rješavanje bio je da hashiramo svoje ime i prezime pa potom usporedimo s ponuđenima. Za enkripciju smo koristili ključeve ograničene entropije - 22 bita(koristili Brute-force napad - kroz ključeve smo prolazili po redu). Znali smo da se radi o PNG slici, provjerili smo da li prva 32 bita plaintexta počinju sa heksadekadskim vrijednostima 89 50 4E 47 0D 0A 1A 0A. Ako je uspješno, plaintext će se spremiti u datoteku PNG formata odnosno sadržaj te datoteke bit će izvorna slika.

```
import base64
from cryptography.fernet import Fernet
from os import path
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()

def test_png(header):
    if header.startswith(b"\211PNG\r\n\032\n"):
        return True
    return False

def brute_force(ciphertext):
    ctr = 0
    while True:
        key_bytes = ctr.to_bytes(32, "big")
        key = base64.urlsafe_b64encode(key_bytes)

        try:
            plaintext = Fernet(key).decrypt(ciphertext)
            header=plaintext[:32]

            if test_png(header):
```

```
                print(f"BINGO: {key}")
                with open("BINGO.png", "wb") as file:
                    file.write(plaintext)
                break
        except Exception:
                pass
        ctr += 1
        if not ctr & 1000:
            print(f"[*] Keys tested: {ctr:,}", end="\r")

filename = hash("prezime_ime") + ".encrypted"
if __name__ == "__main__":
    filename = hash("mamic_anamarija") + ".encrypted"

    #Spremiti naš plaintext u obliku datoteke
    if not path.exists(filename):
        with open(filename, "wb") as file:
            file.write(b"")

    with open(filename, "rb") as file:
        ciphertext=file.read()

brute_force(ciphertext)
```