Laboratorijska vježba 3- Symmetric key cryptography (a crypto challenge)

U ovoj vježbi smo napravili crpyto challenge, odnosno, dešifrirali smo odgovarajući ciphertext
bez poznavanja ključa.

Kako bi to napravili, prvo smo trebali preuzeti osobni izazov sa servera, odnosno pronaći odgovarajuću vlastitu datoteku. Izazov je bio pohranjen u file-u čije smo ime generirali sljedećim kodom :

```
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('granic_andjela') + ".encrypted"
```

Za sliku smo znali da je u PNG formatu pa smo zaključili da ciphertext počinje sa ”\211PNG\r\n\032\n” jer je to prvih 8 byteova karakterističnih za PNG format.
Znali smo tako plaintext i ciphertext, pa smo odlučili otkriti ključ brute-force napadom.

Kako bi provjerili je li file kojeg ćemo dobiti dekripcijom PNG formata, postavili smo counter
ctr=0 kako bi počeli provjeravati od ključa 0 i tako provjerili svaki. Dekripciju smo izvršili uz
pomoć funkcije iz Fernet librarya :

```
plaintext = Fernet(key).decrypt(ciphertext)
```

Cijeli kod:

```
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)

        # Now initialize the Fernet system with the given key
        # and try to decrypt your challenge.
        # Think, how do you know that the key tested is the correct key
        # (i.e., how do you break out of this infinite loop)?
        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("granic_andjela") + ".encrypted"

    # Create a file with the filename if it does not already exists
    if not path.exists(filename):
        with open(filename, "wb") as file:
            file.write(b"")

    # Open your challenge file

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

    # print(ciphertext)
    brute_force(ciphertext)
```

Dekriptirana datoteka: