**IZVJESTAJ IZ 3. LABORATORISJKE VJEŽBE**

U ovoj vježbi odradili smo primjer simetrične kriptografije. Prvo smo trebali pronaći naš izazov na način smo hashirali naše ime i prezime te nakon toga i dodali nastavak “.encrypted“ te na temelju toga bismo pronašli naš osobni izazov. Zatim smo trebali otkriti što je enkriptirano u samom izazovu. To možemo otkriti na temelju brute force napada ako znamo neke podatke o enkriptiranoj poruci ili ako znamo na koji je način poruka enkriptirana. S obzirom da smo znali da se radi o .png slici mogli smo prilagoditi sam algoritam za pronalaženje ključa za dekriptiranje poruke, tj. mogli smo iskoristiti njegove slabosti. Hackeri u stvarnom životu također na taj način prilagođavaju svoj algoritam na temelji uzorka žrtve.

Fotografije formata .png započinju sa 8.bytenim potpisom 137 80 78 71 13 10

26 10 u decimalnom formatu. Na temelju toga smo prilagodili algoritam za naš brute force napad. I uspješno smo dekriptirali našu poruku.

Kod brute force napada koji smo koristili:

def brute\_force\_attack(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"KEY FOUND: {key}")

with open("BINGO.png", "wb") as file:

file.write(plaintext)

break

except InvalidToken:

dekriptirana poruka:

