Dokumentacija za Domaći 4 – Kriptografija

# Postavka problema

Dešifrovati presretnutu poruku uz pomoć nabavljenog ključa.

Šifrovana poruka:

**o/O38rGJ4ozlt+aJ6LLQsNC90LAg0L/QvtGA0YPQutCwINC90LAg0ZvQuNGA0LjQu9C40YbQuC4=**

Ključ:

**sifra12345678**

Izvesti izraz po kom se može dobiti originalna poruka koristeći logičke operatore i navesti poslatu poruku u čitljivom formatu.

# Postupak rešeavanja

Pretpostavka je da treba **XOR**-ovati poruku koja je u **Base64** formatu (tako da je treba prebaciti u bajtove), sa ključem koji treba enkodovati preko **UTF-8**, jer on nije šifrovan. Pošto su različitih dimenzija, prvobitna ideja je bila da se napravi ključ koji se ponavlja do dimenzije poruke, nešto kao:

*decrypted\_msg\_bytes = bytearray( [encrypted\_msg[i] ^ key\_bytes[i % len(key\_bytes)] for i in range(len(encrypted\_msg))]*

Nakon dekodiranja dekriptovane poruke dobijeno je „Крипто???????????????????” tako da je zaključak da je deo poruke dobro dešifrovan, dok većina nije. Uklanjanjem karaktera 7 i 8 iz šifre dobijeno je „Крипт????????????????????” itd. Zaključeno je da je samo prvi deo poruke koji je dešifrovan sa šifrom dobro bio dešifrovan, dok pri prvom ponavljanju šifre dolazi do greške što znači da šifra nije:  
sifra12345678sifra12345678… već nešto drugo. Nakon pokušavanja različitih formi šifri dešifrovanja šifrovane poruke bez šifre zaključak je da šifrovana poruka bez XOR-ovanja sa ključem daje ostatak poruke. Zbog toga zaključuje se da treba XOR-ovati šifrovanu poruku sa ključem koji je do kraja popunjen nulama jer tako karakteri ostaju isti pri XOR-ovanju. Nešto ovog tipa:  
*key\_bytes = key\_bytes.ljust(len(encrypted\_msg), b'\x00')*

Posle toga sledi:  
*decrypted\_msg\_bytes = bytearray( [encrypted\_msg[i] ^ key\_bytes[i] for i in range(len(encrypted\_msg))])*

Nakon čega ostaje samo dekodiranje poruke preko UTF-8, uz upis u .txt fajl u slučaju da konzola iz nekog razloga ne podržava UTF-8 ili ćirilicu.

U Python fajlu je odrađeno ovo u kodu.