Vjezbe 3

Otvorili smo Visual Studio i pokrenili Docker kako bi mogli raditi na virtualnom disku.

Zadatak je bio prvo odrediti koji *cyphertext* je ciji sto smo odredili usporedbom *hash*-a vlastitog imena i naziva *cyphertext* datoteke.

Zatim je trebalo brute force napadom pogoditi kljuc od 22 bita entropije (2^22 ~ 4 mil. razlicitih kljuceva) za sto smo napravili program koji pocevsi od 0000000…0000 povecava vrijednost kljuca za 1 i redom pokusava desifrirati *cyphertext* sa svakim.

Jos jedan problem je bio u tome kako automatizirati recognition tocnog kljuca tj. dobijanje tocnog *plaintext*-a. To smo rijesili provjeravajuci prvih nekoliko byte-ova iz dobivenog *plaintext*-a sa tzv. *signature byte*-ovima trazenog formata (u slucaju .png formata to su **137 80 78 71 13 10 26 10**).

Pokrenuli smo program i cekali dok nismo pronasli tocan key i dobili tocan *plaintext*.

Nisam screenshot-ao ili prepisao kod sa vjezbi ali zelim reci kako iako se kod uredno izveo ja nisam uspio pronaci tocan key tako da sam negdje falio ili u kodu ili kod ubacivanja cyphertexta u program.