Laboratorijske vježbe 3

Na trećim laboratorijskim vježbama tema je bila **Symmetric key cryptography**.

Cilj vježbe bio je dobiti *plaintext* od odgovarajućeg *ciphertexta* bez prethodnog poznavanja ključa.
Trebalo je otkriti koji je naš enkriptirani dokument, pronaći ključ te pomoću njega dekriptirati spomenuti dokument.

Na linku http://challenges.local/ nalazile su se enkriptirane datoteke (imena i prezimena studenata). Svaki student je uz pomoć koda koji smo pisali s profesorom pronašao svoje ime i prezime. Koristili smo **Brute-force napad** za otkrivanje ključa kojom je bila enkriptirana datoteka.

Kroz više iteracija pomoću trenutnog ključa pokušali smo dekripcijskim algoritmom dekriptirati *ciphertext* te njemu pridružiti varijablu *plaintext* i pozvati funkciju *test_png* kojoj smo slali prva 32 bita *plaintexta* gdje smo provjeravali odgovaraju li oni headeru datoteke png formata. Ako se poklapaju, funkcija bi vratila istinu, saznali bismo ključ i dobili originalni sadržaj (sliku u png formatu s personaliziranom porukom).