Ivan Legac Rudan

Izvještaj s drugih laboratorijskih vježbi

Na drugim laboratorijskim vježbama smo uz pomoć biblioteka Ferneta i poznavanjem jezika Python dekriptirali sliku. Prvo smo morali uz pomoć ključa pronaći naše kriptirano ime i preko toga odgovarajuci folder u kojem je kriptirana slika. Potom smo uz pomoc pythona napisali program koji koristi brute force za razbijanje šifre. Problem je bio kako reći programu koji je ključ odgovarajući tj kada je datoteka čitljiva a to smo učinili tako što smo rekli da negde u headeru traži ključnu riječ „png“ koja bi se trebala nalaziti u svakom fileu .png formata kada se prebaci u .txt format.

Za pronalazak ključa u mom specifičnom slučaju je trebalo oko milijun testiranih dok je maksimalni broj mogućih ključeva 4 milijuna (2 na 22.) jer smo u uputama odredili da je ključ kriptiran sa 256 bitova ali su samo zadnja 22 bita neke znamenke koje ne moraju bit nula.