Lab 2

Simulirali smo brute force attack na ciphertext kako bi dobili nepoznati plaintext. U našem slučaju u ciphertextu je bio enkriptirana slika png formata. Kako smo to znali mogli smo saznati metapodatke koje sadržava png format i pomoću tih metapodataka znati kako će izgledati dio plaintexta. Kako nismo znali kojim je ključem enkriptiran ciphertext, isprobavali smo redom sve 32-bitne ključeve i provjeravali prepoznajemo li u dekriptiranom ciphertextu metapodatke png formata. Kada nađemo odgovarajući ključ pronaći ćemo moći ćemo dekriptirati sliku.

Nisam uspio dekriptirati sliku.