

Криптографија

Задаци за рад по групама

Група III

Задатак 1.

Направити програм који ће кориснику омогућити да

- Врши енкрипцију односно декрипцију помоћу Виженеровог алгорита.
- Врши енкрипцију и декрипцију помоћу LFSR алгорита.
- Врши енкрипцију и декрипцију помоћу ARCFOUR алгорита.

Задатак 2.

Направити програм `vigenere_anal` за криптоанализу Виженеровог криптосистема. Програм користи све аспекте напада на Виженеров криптосистем: Индекс коинциденције, Касиски тест... У програму се омогућава и кориснику да у одређеној фази "интервенише" директно и тако помогне у коначној криптоанализи.

Задатак 3.

Направити програм за напад на LFSR, користећи линеарност система, односно рјешавањем система линеарних једначина.

Напомена: Сваки програм мора бити user-friendly са прецизним упућствима просјечном кориснику.

Задатке реализовати тако да постоји јединствени интерфејс, а корисник бира различите опције. За пројекат је потребно направити одговарајућу документацију. Документација подразумијева

1. Прецизна упуства потенцијалним корисницима како се користе поједини програми, шта они раде и која су им ограничења.
2. Описати поступак рада групе и назначити сваки појединачни допринос чланова групе.
3. Написати предлог побољшања постојећих програма.
4. Указати на могуће недостатке у прецизности формулације постављених задатака.

Документацију доставити у склопу пројекта у електронској форми.