Криптографија

Задаци за рад по групама

Група III

Задатак ове групе је реализује неке програмски пакет који обухвата неке класичне крипто-системе. Програм је потребно урадити у виду десктоп и веб апликације.

Задатак 1.

Направити програм који ће кориснику омогућити да

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

Задатак 2.

Направити програм **vigener_anal** за криптонализу Виженеровог криптосистема. Програм користи све аспекте напада на Виженеров криптосистем: Индкес коинциденције, Касиски тест... У програму се омогућава и кориснику да у одређеној фази "интервенише" директно и тако помогне у коначној криптоанализи. За овај програм се мора водити рачуна о статистичким особинама језика који се користи.

Напомена: Сваки програм мора бити user-friendly са прецизним упуствима 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.