Криптографија

Задаци за рад по групама

Алгоритми за факторизацију

Задатак ове групе је да користећи неку постојећу библиотеку корисних програма, везаних за аритметику великих бројева, односно бројева који су представљени као низови цифара реализује групу неких познатих криптографских алгоритама. Овдје су бројеви представљени као стрингови. **Узимаћемо да је генерално ограничење за сваки стринг да је његова дужина највише 40.**

Задатак 1.

Написати програм за реализацију Полардовог $p-1$ алгоритма за факторизацију. Улазни податак је број N који је производ два проста броја. Кориснику дати могућност да посебно генерише два проста броја, потом их помножи како би тај резултат користио за Полардов $p-1$ алгоритам.

Pollard p – 1

Улаз: Број N
(претходно добијен као производ два велика проста броја)
Излаз: Факторизација N, односно p и q.

Задатак 2.

Написати програм за факторизацију путем разлике кавдрата, односно метода "квадратног сита". Улазни податак је број N који је производ два проста броја. Кориснику дати могућност да посебно генерише два проста броја, потом их помножи како би тај резултат користио за факторизациу назначеним алгоритмом

---

quadratic_sieve

Улаз: Број N
(претходно добијен као производ два велика проста броја)
Излаз: Факторизација N, односно p и q.

Напомена: Сви програми се обједињују у оквиру јединственог корисничког интерфејса. Сваки програм мора бити user-friendly са прецизним упуствима просјечном кориснику. За пројекат је потребно направити одговарајућу **документацију**. Документација подразумијева

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

Документацију доставити у склопу пројекта у електронској форми.

Програм је неопходно доставити у самосталној извршној верзији (standalone executable - без инсталирања посебних окружења, библиотека...) или као веб апликацију.