

# Криптографија

Задачи за рад по групама

## Калкулатор модуларне аритметике

Задатак ове групе је реализује пакет корисних програма за Теорију бројева, првенствено за модуларну аритметику.

### Задатак 1.

Направити програм који ће кориснику омогућити

- Сабирање, одузимање и множење по задатом модулу.
- Рачунање највећег заједничког дјелиоца  $\text{нзд}(a, b)$  путем Еуклидовога алгоритма са приказом корака у поступку.
- Рачунање најмањег заједничког садржаоца  $\text{нзс}(a, b)$ .
- Представљање  $\text{нзд}(a, b)$  као линеарне комбинације датих бројева, остављајући могућност да корисник може, уколико жели, да добије ток Бланкшип методе у пригодном облику.
- Направити програм за тражење инверзног елемента  $a^{-1}$  за дати елемент  $a$  по модулу  $m$  уколико такав постоји.
- Рјешавање конгруенција  $ax \equiv b \pmod{m}$ .
- Рјешавање система конгруенција помоћу Кинеске теореме о остацима.
- Рачунање израза облика  $a^k \pmod{m}$  на ефикасан начин. (Објашњење овог алгоритма се налази на 24. страници књиге "Mathematical Cryptography" која је дата у литератури на сајту.)

- Израчунавање вриједности Ојлерове функције  $\phi(n)$  за задато  $n$ .  
Потребно је имати на уму да ово можемо успјешно рачунати за све бројеве  $n$  које је могуће успјешно и ефикасно факторисати, тако да је и овдје потребно увести одређена ограничења у сислу величине броја  $n$ .

**Овај програм је потребно развити и као веб апликацију. Сви додаци, проширења и допуне постојећег задатка ће бити посебно вредновани.**

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

**Задатке реализовати тако да постоји јединствени интерфејс, а корисник бира различите опције.**

За пројекат је потребно направити одговарајућу документацију. Документација подразумијева

1. PYTHON код за сваки од задатака.
2. Прецизна упутства 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.**