

# Криптографија

Задаци за рад по групама

## Група V

Задатак ове групе је да направи програм за рјешавање проблема дискретног логаритма (ДЛОГ). 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 тражење простог броја са задатим бројем цифара.

---

**prim – num\_find**

---

Овај програм треба да нађе прост број за дати број цифара.

**Улаз:**  $k$ -жељени број цифара

**Излаз:** стринг (представља прост број са датом дужином стринга)

---

### Задатак 2.

Написати програм за реализацију Шанксовог (Baby step-giant step) алгоритма. Унос корисника се мора верификовати у смислу провјере да је, на примјер, унешени број  $p$  заиста прост. У ту сврху је потребно искористити Милер-Рабинов алгоритам

---

**shanks**

---

**Улаз:**  $p, g, h$

**Излаз:**  $x \in \mathbb{Z}_p$  тако да  
 $g^x \equiv h \pmod{p}$ .

---

**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. Псеудо-код за сваки од потребних програма.
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.