Криптографија

Задаци за рад по групама

Група II

Задатак ове групе је да направи "калкулатор" великих бројева, односно бројева који су представљени као низови цифара. Такође, задатак ове групе је да реализује програм за испитивање и генерисање простих бројева. Овдје су бројеви представљени као стрингови. **Узимаћемо да је генерално ограничење за сваки стринг да је његова дужина највише 40.**

Задатак 1.

Направити програм за брзо степеновање по задатом модулу. Објашњење овог алгоритма се налази на 24. страници књиге "Mathematical Cryptography" која је дата у литератури на сајту.

pow_m

Улаз: стринг1, стринг2, стринг-м;
Излаз: стринг1$^{\text{стринг2}}$ (mod стринг-м)

Задатак 2.

Направити програм за испитивање да ли унесени стринг цифара представља прост број или не. Користити Милер-Рабинов алгоритам а резултат је са одређеном вјероватноћом тачан.

miller_rabin

Улаз: стринг; $m \in \mathbb{N}$
Излаз: "прост" или "није прост" са могућношћу грешке 10^{-m}

Следећи програм се природно наставља на претходни а његов циљ је да пронађе прост број за унапријед задати број цифара.

prim – num_find

Овај програм треба да нађе прост број за дати број цифара.
За његову реализацију се може користити програм **miller_rabin**.
Улаз: k-жељени број цифара
Излаз: стринг (представља прост број са датом дужином стринга)

Задатак 3.

Написати програм за тражење реда датог елемента у пољу $\mathbb{Z}_p$.

prim – ord_find

Улаз: p, g (стрингови до 40 цифара)
Излаз: ред елемента g у пољу $\mathbb{Z}_p$.

Напомена: Сви појединачни програми се обједињују у оквиру јединственог корисничког интерфејса. Кориснику се нуде различите опције... Сваки програм мора бити user-friendly са прецизним упуствима просјечном кориснику. За пројекат је потребно направити одговарајућу **документацију**. Документација обједињена у једном документу 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.