# Криптографија

Задаци за рад по групама

## Група II

Задатак ове групе је да направи програм за ЕлГамал енкрипцију и декрипцију.

### Задатак 1.

Написати програм за енкрипцију и декрипцију ЕлГамал алгоритмом.
У следећем програму, подразумијевамо да корисник има неки начин да генерише све јавне податке ЕлГамал енкрипције, прост број $p$, експонент $g^a \pmod{p}$. Програм треба да садржи неку "рандом" функцију којом се бира Бобов експонент $k_m$ који се користи у енкрипцији. За провјеру да ли је неки број прост, искористити Милер-Рабинов алгоритам.

---

**elgam_enc**

---

**Улаз:** број за енкрипцију: $m$, $p, g^a \pmod{p}$
**Излаз:** број енкриптован помоћу ЕлГамал енкрипције.

---

У следећем програму, Алиса врши декрипцију доспјелог криптограма који је претходно енкриптован помоћу јавних података које је она истакла.

---

**elgam_dec**

---

**Улаз:** $p, a, g$ :
(број1, број2) - пар из ЕлГамал енкрипције
(**a** је Алисин тајни кључ)
**Излаз:** број настао декрипцијом помоћу ЕлГамал-а

---

**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.