Криптографија

Задаци за рад по групама

Група II

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

Задатак 1.

Написати програм за енкрипцију и декрипцију ЕлГамал алгоритмом.
У следећем програму, подразумијевамо да корисник има све јавне податке ЕлГамал енкрипције. Овај програм, дакле, симулира Боба. Корисник (у овом случају Боб) преузима податке са Алисиног вебсајта: прост број p, експонент $g^a \pmod{p}$. Обавезно је да се у оквиру програма провјери да ли је p стварно прост или не. Ако није, да се корисник обавјести о томе. Програм треба да садржи неку "рандом" функцију којом се бира Бобов експонент k_m који се користи у енкрипцији.

---

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

Задатак 2.

Циљ овог програма је енкрипција и декрипција RSA алгоритмом.

rsa_enc

Улаз: број за енкрипцију: x, N, e
(**N** је број добијен као производ два проста броја p і q,
а **e** је експонент за енкрипцију)
Излаз: број x'
(Енкрипција RSA алгоритмом)

У следећем програму, корисник врши декрипцију доспјелог криптограма. Корисник (симулација Алисе која врши декрипцију) мора да обезбиједи тајни експонент d, као и N као улазне податке.

rsa_dec

Улаз: број x', N, d
(**d** је тајни кључ - експонент за декрипцију)
Излаз: број x
(Декрипција RSA алгоритмом)

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.