

Криптографија

Задаци за рад по групама

Група V

Циљ овог скупа програма је енкрипција и декрипција ЕлГамал алгоритмом. Најприје, потребно је обезбједити помоћни програм којим се успоставља ЕлГамал систем, проналазе велики прости бројеви, а затим рачунају остали параметри.

Улаз за ЕлГамал енкрипцију је стринг, дакле обичан низ карактера. Њих треба најприје помоћу неке **encoding scheme** (нпр. ASCII) претворити у бројеве, а касније примјенити ЕлГамал алгоритам.

Задатак 1.

Написати програм за енкрипцију и декрипцију ЕлГамал алгоритмом. Улаз је стринг, дакле обичан низ карактера. Њих треба најприје помоћу неке **encoding scheme** (нпр. ASCII или UTF8) претворити у бројеве, а касније примјенити ЕлГамал алгоритам.

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

Изназ: стринг p (представља прост број са датом дужином стринга)

Следећи програм симулира Алису у ЕлГамал сценарију. Тачније - помаже јој да успостави свој ЕлГамал. Све што зна Алиса, треба да буде

излазни податак овог програма.

elgam_set

Улаз: k -жељени број цифара за прост број p

Изназ: стринг (број p), стринг (генератор g у \mathbb{Z}_p),
тајни експонент a из $\{0, 1, \dots, p-1\}$, као и $g^a \pmod{p}$.

У следећем програму, подразумејемо да корисник има све јавне податке ЕлГамал енкрипције. Овај програм, дакле, симулира Боба. Улазне величине су прост број p , експонент $g^a \pmod{p}$.

elgam_enc

Улаз: стринг (директно или из датотеке),
 $p, g^a \pmod{p}, k_m, m$, гдје је генератор g у \mathbb{Z}_p .

Прва два податка Боб добија од Алисе, а друга два сам бира.

Изназ: (стринг1, стринг2) ЕлГамал енкрипција
(омогућити да се рез. упише у неку датотеку).

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

elgam_dec

Улаз: (стринг1, стринг2) ЕлГамал енкрипција

(директно или из датотеке), p, a, g , (**a** је Алисин тајни кључ)

Изназ: стринг (омогућити да се рез. упише у неку датотеку).
(Декрипција ЕлГамал алгоритмом)

Напомена: Сви програми се обједињују у оквиру јединственог

корисничког интерфејса. Сваки програм мора бити user-friendly са прецизним упуштвима 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.

Програм је неопходно доставити у самосталној извршној верзији (standalone executable - без инсталирања посебних окружења, библиотека...) или као веб апликацију.