Криптографија

Задаци за рад по групама

Група IV

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.

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)

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.

Овај програм поставља ЕлГамал систем . Помоћу **prim − num_find**, избаца прост број p од k цифара, бира случајан елемент $g \in \mathbb{Z}_p$ а помоћу

prim − ord_find налази ред n елемента g у $\mathbb{Z}_p$. Такође, бира на случајан начин тајни експонент ЕлГамал енкрипције $a \in \{0, 1, \ldots, n-1\}$. Овдје треба водити рачуна да ред n не смије бити премали.

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
Излаз: стринг (број p), стринг (број g реда n),
тајни експонент a из $\{0, 1, \ldots, n-1\}$, као и $g^a \pmod{p}$.

У следећем програму, подразумијевамо 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, $p, g^a \pmod{p}, k_m, m$
Прва два податка Боб добија од Алисе, а друга два сам бира.
Излаз: (стринг1, стринг2) ЕлГамал енкрипција.

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, p, a, g (**a** је Алисин тајни кључ) **Излаз:** стринг (Декрипција ЕлГамал алгоритмом)

Напомена: Сви програми се обједињују у оквиру јединственог корисничког интерфејса. Кориснику мора бити понуђено да ли жели да степенује неке бројеве по модулу, да успостави RSA, ЕлГамал... 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.