Криптографија

Задаци за рад по групама

Група III

Задатак ове групе је да направи програм за ЕлГамал енкрипцију/декрипцију, наслањујући се на резултате Групе II. Овдје су бројеви представљени као стрингови. **Узимаћемо да је генерално ограничење за сваки стринг да је његова дужина највише 40.**

Задатак 1.

Написати програм за енкрипцију и декрипцију ЕлГамал алгоритмом. Улаз је текстуални фајл. Фајл је потребно помоћу неке **encoding scheme** (нпр. ASCII, UTF8...) претворити у бројевни еквивалент, а касније примјенити ЕлГамал алгоритам.

Овај програм поставља ЕлГамал систем. Помоћу програма Групе II, $\mathbf{prim-num\_find}$, избаца прост број p од k цифара, бира случајан елемент $g \in \mathbb{Z}_p$ а помоћу $\mathbf{prim-ord\_find}$ 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. Корисник (у овом случају Боб) преузима податке са Алисиног вебсајта: прост број p, експонент $g^a \pmod{p}$. Потом корисник бира текстуални фајл који треба енкриптовати. Програм треба да садржи неку "рандом" функцију којом се бира Бобов експонент k_m који се користи у енкрипцији.

elgam_enc

Улаз: стринг, $p, g^a \pmod{p}$
Излаз: стринг енкриптован помоћу ЕлГамал енкрипције.

Напомена: Корисник у програму бира текстуални фајл за енкипцију. Тај фајл се, у зависности од одабраног p, дијели на низ стрингова који се потом енкриптују помоћу претходног програма. Потом се то уписује у посебан фајл који се касније може користити за декрипцију.

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 :
(стринг1, стринг2) - пар из ЕлГамал енкрипције
(**a** је Алисин тајни кључ)
Излаз: стринг настао декрипцијом помоћу ЕлГамал-а

Напомена: Корисник у програму бира текстуални фајл за декрипцију. Тај фајл је по описаној процедури већ дат као низ уређених парова који се потом предају програму за декрипцију. Декриптован садржај се уписује у посебан фајл.

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.