Криптографија

Задаци за рад по групама

Група IV

Задатак ове групе је да направи програм за RSA 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.

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

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

---

rsa_set

Овај програм поставља RSA систем.
Улаз: k-жељени број цифара
Помоћу **prim − num_find**, избаца два проста броја p, q,
а затим рачуна $N = pq$, $\phi(N)$, експонент за енкрипцију e,
експонент за декрипцију d, $ed \equiv 1 \pmod{\phi(N)}$.
Излаз: стринг (број p), стринг (број q), стринг (број $N = pq$),
стринг (број e), стринг (број d), стринг (број $\phi(N)$)

---

rsa_enc

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

Напомена: Корисник у програму бира текстуални фајл за енкипцију. Тај фајл се, у зависности од одабраног N, 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, 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: стринг, N, d
(**d** је тајни кључ - експонент за декрипцију)
Излаз: стринг
(Декрипција RSA алгоритмом)

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

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 ко-

риснику. 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.