Криптографија

Задаци за рад по групама

Група IV

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) претворити у бројеве, а касније примјенити RSA 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 p (представља прост број са датом дужином стринга)

rsa_set

Овај програм поставља RSA систем.
Улаз: k-жељени број цифара
Помоћу **prim − num_find**, налази 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 (директно или из неке датотеке), N, e
(**N** је број добијен као производ два проста броја p и q,
а **e** је експонент за енкрипцију)
Излаз: стринг (омогућити да се резултат упише у датотеку)

rsa_dec

Улаз: стринг (директно или из неке датотеке), N, d
(**d** је тајни кључ - експонент за декрипцију)
Излаз: стринг (омогућити да се резултат упише у датотеку)
(Декрипција RSA алгоритмом)

Напомена: Сваки програм мора бити user-friendly са прецизним упуствима просјечном кориснику. За пројекат је потребно направити одговарајућу **документацију**. Документација подразумијева

1. Прецизна упуства потенцијалним корисницима како се користе поједини програми, шта они раде и која су им ограничења.

2. Описати поступак рада групе и назначити сваки појединачни допринос чланова групе.

3. Написати предлог побољшања постојећих програма.

4. 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.