

# Криптографија

Задаци за рад по групама

## RSA крипто-систем

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)

**Израз:** 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)

**Израз:** стринг (омогућити да се резултат упише у датотеку)  
(Декрипција RSA алгоритмом)

---

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

1. **PYTHON код за сваки од задатака.**
2. Прецизна упутства 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.**