Криптографија

`Други колоквијум`, 18.05.2013.

Максималан број бодова на испиту је 100. Укупно вријеме рада је **90** минута. **Нечитко исписани одговори и некомплетна рјешења се неће бодовати**. Срећно!

Задатак 1. (15 поена)

а Показати да је број 3 примитивни коријен модуло 29, а потом ријешити једначину

$$3^x \equiv 2 \pmod{29}$$

користећи се Шанксовим алгоритмом. Прецизно исписати сваки корак и дати детаљна објашњења.

б Доказати да двије листе успостављене у Шанксовом алгоритму увијек морају имати непразан пресјек.

Задатак 2. (25 поена)

Нека је дата функција f која пресликава коначан скуп S у њега самог. Нека је $x_0 \in S$ произвољан елемент датог скупа. Нека је $y_0 = x_0$. Формирамо два низа:

$$x_{i+1} = f(x_i) \quad y_{i+1} = f(f(y_i)), \quad i = 0, 1, \ldots$$

Доказати

а $y_i = x_{2i}, \;\; i = 0, 1, \ldots$

б Постоји неко $r \in \mathbb{N}$ тако да $y_r = x_r$.

в На који начин се претходни резултат може искористити у тражењу рјешења једначине

$$g^x \equiv a \pmod{p},$$

гдје је g примитивни коријен модуло прост број p, док је $a \in \mathbb{Z}_p$? Описати детаљно и образложити.

Задатак 3. (20 поена)

а Описати начин рјешавања конгруенције

$$x^e \equiv c \pmod{p}$$

гдје је p прост број, c природан број модуло p, а e природан број такав да је **нзд**$(e, p-1) = 1$. Детаљно описати поступак и образложити.

б На основу поступка описаног горе ријешити конгруенцију

$$x^{77} \equiv 2 \pmod{246}.$$

(Упуство: Кинеска теорема о остацима)

Задатак 4. (15 поена)

Показати да, ако би Ева у РСА криптосистему знала вриједност $p + q$, онда би била у стању вршити декрипцију.

Задатак 5. (25 поена)

Претпоставимо да имамо алгоритам који у групи G, за елементе $u, v \in G$, рјешава дискретни логаритам

$$u^x = v,$$

гдје је ред елемента u једнак q^e, за прост број q, природан број e и функцију $f : \mathbb{N} \leftrightarrow \mathbb{N}$, у $\mathcal{O}(f(q^e))$ корака. Нека је $g \in G$ елемент реда N и претпоставимо да N можемо факторисати на просте факторе

$$N = q_1^{e_1} q_2^{e_2} \cdots q_t^{e_t}.$$

Доказати да се дискретни логаритам $g^x = h$ може ријешити у

$$\mathcal{O}\left(\sum_{i=1}^{t} f({q_i}^{e_i}) + \log(N)\right)$$

корака.