Криптографија

`Први колоквијум`, 04.04.2010.

Максималан број бодова на испиту је 100. Укупно вријеме рада је **120** минута. **Нечитко исписани одговори и некомплетна рјешења се неће бодовати**. Срећно!

Задатак 1. (10 поена)

а. Наћи d= **нзд(423,198)** користећи Еуклидов алгоритам. Приказати сваки корак у поступку.

б. Наћи цијеле бројеве u и v такве да је

$$423u + 198v = d.$$

в. Да ли из претходног можете нешто рећи о **нзд**(u,v)?

Задатак 2. (5 поена)

а. Наћи инверзни елемент елемента $a = 5$ у мултипликативној групи $\mathbb{Z}_{12}^*$.

б. Ако је ϕ Ојлерова функција, објаснити математичко значење израза $\phi(n)$, а затим наћи $\phi(150)$.

Задатак 3. (10 поена)

Нека је ϕ Ојлерова функција, а $\{r_1, \ldots, r_{\phi(m)}\}$ редуковани систем остатака модуло m и **нзд(a,m)=1**. Доказати да је $\{ar_1, \ldots, ar_{\phi(m)}\}$ такође редуковани систем остатака.

Задатак 4. (15 поена)

а. Користећи кинеску теорему о остацима, ријешити систем конгруенција

$$\begin{aligned} x &\equiv 4 \pmod 7 \\ x &\equiv 2 \pmod 4 \\ x &\equiv 11 \pmod{15} \end{aligned}$$

б. Навести Ојлерову теорему, а затим наћи $7^{100} \pmod{15}$.

Задатак 5. (5 поена)

а. Шта је основни сигурносни проблем супституционог крипто-система?

б. Описати Виженеров крипто-систем.

в. У чему је основна разлика између супституционог и Виженеровог крипто-система?

Задатак 6. (15 поена)

а. Нека је LFSR генерисан са задатим коефицијентима $(p_2 = 1, p_1 = 0, p_0 = 1)$ и почетним стањем $c_2 = 1, c_1 = 0, c_0 = 0$. Дакле, рекурентна формула је

$$c_{i+3} = p_0 c_i + p_1 c_{i+1} + p_2 c_{i+2} \quad i \geq 0.$$

Извршити енкрипцију помоћу датог LFSR-а ријечи **HAL**, при чему користимо ASCII кодни систем

H	01001000
A	01000001
L	01001100

б. Која је основна слабост LFSR система? Описати један успјешан напад на LFSR.

Задатак 7. (15 поена)

Наћи рјешење једначине

$$3^x \equiv 13 \pmod{19},$$

користећи Шанксов алгоритам. Симулирати у потпуности алгоритам, односно приказати сваки његов корак.

Задатак 8. (5 поена)

а. Шта је Дифи-Хелманов (ДХ) проблем?

б. Да ли је тежи ДЛОГ или ДХ? Објасни.

Задатак 9. (10 поена)

Алиса и Боб се договоре да јавни параметри ЕлГамал система буду $p = 13$ и примитивни коријен $g = 2$. Алиса бира $a = 3$ за њен приватни кључ. Боб жели да пошаље поруку $m = 5$ Алиси, користећи свој приватни кључ $k = 5$ и дате параметре ЕлГамал система. Описати све кораке одвијања протокола. Приказати како Боб врши процес енкрипције, а Алиса процес декрипције.

Задатак 10. (10 поена)

Претпоставимо да Ева има "оракл" којим декриптује ЕлГамал. Доказати да се тај "оракл" може користити за рјешавање Дифи-Хелмановог (ДХ) проблема?