Криптографија

`Други колоквијум`, 16.05.2011.

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. (20 поена)

Користећи Полиг-Хелманов алгоритам, наћи рјешење дискретног логаритма

$$g^x = a \text{ у } \mathbb{F}_p,$$

гдје су $p = 433,\ g = 7,\ a = 166$.

Помоћ: Ред броја 7 у модуло 433 аритметици је $432 = 2^4 3^3$.

j	1	2	3	4	5	6	7	8	9	10
$6^j \pmod{109}$	6	36	107	97	37	4	24	35	101	61
j	11	12	13	14	15	16	17	18	19	20
$6^j \pmod{109}$	39	16	96	31	77	26	47	64	57	15
j	21	22	23	24	25	26	27	28	29	30
$6^j \pmod{109}$	90	104	79	38	10	60	33	89	98	43

Задатак 2. (15 поена)

Наћи рјешење једначине

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

користећи Полард-ро алгоритам.

Задатак 3. (10 поена)

Нека су познати параметри RSA, бројеви $\phi(pq) = 640$ и $p + q = 58$.

а. Који је од следећих параметара $e_1 = 32,\ e_2 = 49,\ e_3 = 25$ валидан RSA експонент? Објаснити избор.

б. За претходно добијени експонент и пресретнуту енкриптовану поруку $C = 5$, израчунати послату поруку.

Задатак 4. (10 поена)

Нека су $N = 143$ и $e = 23$ дати параметри за RSA. Енкрипцијом поруке M добијена је вриједност $C = 9$. Израчунати све параметре (јавне и тајне) система и израчунати M.

Задатак 5. (15 поена)

Претпоставимо да Оскар има **magic box** (оракл) који за дати RSA систем (N, e), избаца два пара бројева $(e_1, d_1),\ (e_2, d_2),\ e_1 \neq e,\ e_2 \neq e$, тако да

$$e_1 d_1 \equiv 1 \pmod{\phi(N)}, \quad e_2 d_2 \equiv 1 \pmod{\phi(N)}.$$

Како је могуће искористити овај оракл за факторизацију броја N?

Задатак 6. (15 поена)

а. Дефинисати појам Милер-Рабиновог свједока.

б. Примјенити Милер-Рабинов тест за број 11663. Наћи бар једног Милер-Рабиновог свједока претходног броја или обезбиједити бар 10 бројева који нису.

Задатак 7. (15 поена)

Наћи вриједности a и b који задовољавају $a^2 \equiv b^2 \pmod{N}$, а затим израчунати **нзд**$(N, a - b)$ у циљу факторизације броја $N = 61063$. Искористити следеће податке

$$1882^2 \equiv 270 \pmod{N} \quad \text{и} \quad 270 = 2 \cdot 3^3 \cdot 5,$$

$$1898^2 \equiv 60750 \pmod{N} \quad \text{и} \quad 60750 = 2 \cdot 3^5 \cdot 5^3.$$