6. přednáška a cvičení (31. března 2009)

Co jsme dělali na přednášce?
Sekci 2.13 ze skript.

Co jsme dělali na cvičení?
Popsali jsme si systém RSA (sekce 2.14 ze skript) a počítali příklady z minula.

Příklady
1. Můj modul pro RSA je 33, veřejný klíč je 7. Přišla mi zakódovaná zpráva 1, 2, 27, 10. Dekóduj ji.

2. Ať $p_1, \ldots, p_r$ jsou po dvou různá prvočísla. Dokaž, že nejmenší číslo $m > 0$ takové, že pro všechna $a \in \mathbb{Z}_{p_1 \cdots p_r}$ platí $a^{m+1} \equiv a \pmod{p_1 \cdots p_r}$, je $\operatorname{nsn}(p_1 - 1, \ldots, p_r - 1)$.