# Homework 1 in Cryptography II

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Michael Reyer

23.04.2009

**Exercise 1.** In RSA, often small exponents are used for encryption. Identify assets and drawbacks of this method and suggest counter measures for drawbacks.

**Exercise 2.** Factorize $n = 3149$ with the knowledge that $412^2 \equiv 459^2 \equiv 2847 \mod n$.

**Exercise 3.** Given $a^x \equiv 17 \mod 31$ and $x = 13$, calculate $a$.

**Exercise 4.** Prove proposition 8.3 from the lecture notes: Let $n = pq$, $p \neq q$ prime and $x$ a nontrivial solution of $x^2 \equiv 1 \mod n$, i.e., $x \not\equiv \pm 1 \mod n$. Then

$$\gcd(x + 1, n) \in \{p, q\}.$$