Homework 3 in Cryptography II

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

07.05.2009

Exercise 8. Prove Euler's criterion:
Let $p > 2$ be prime. $c \in \mathbb{Z}_p^*$ is a quadratic residue modulo p iff $c^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Are $36, 102, 213$ and 331 quadratic residues modulo 727?

Exercise 9. Determine four square roots $\pm x$ and $\pm y$ of 49 modulo n, with $n = 83 \cdot 71$.

Exercise 10. Assume an efficient algorithm for finding square roots modulo $n = p \cdot q$, where p and q are unknown.

Find an efficient algorithm for factoring n.