Homework 2 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Georg Bocherer

26.10.2010

Exercise 5. Prove Proposition 7.5: Let $p > 3$ be prime, $p - 1 = \prod_{i=1}^{k} p_i^{t_i}$ the prime factorization of $p - 1$. Then

$$a \text{ is a primitive element modulo } p \Leftrightarrow a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p} \quad \forall i = 1, \ldots, k.$$

Exercise 6. Prove Proposition 8.3: Let $n = pq$, $p \neq q$ prime and x a nontrivial solution of $x^2 \equiv 1 \pmod{n}$, i.e., $x \not\equiv \pm 1 \pmod{n}$. Then

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

Exercise 7. Prove Proposition 9.2: (Euler's criterion) Let $p > 2$ be prime. $c \in \mathbb{Z}_p^*$ is a quadratic residue modulo p if and only if $c^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Exercise 8. In RSA, often small exponents are used for encryption. Identify assets and drawbacks of this method and suggest counter measures for the drawbacks.