Homework 9 in Cryptography I

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

30.06.2011

Exercise 27. Let $\varphi : \mathbb{N} \to \mathbb{N}$ the Euler φ-function, i.e., $\varphi(n) = |\mathbb{Z}_n^*|$.

(a) Determine $\varphi(p)$ for a prime p.

(b) Determine $\varphi(p^k)$ for a prime p and $k \in \mathbb{N}$.

(c) Determine $\varphi(p \cdot q)$ for two different primes $p \neq q$.

(d) Determine $\varphi(4913)$ and $\varphi(899)$.

Exercise 28.

(a) Use the Miller-Rabin Primality Test to prove that 341 is composite.

(b) The Miller-Rabin Primality Test comprises a number of successive squarings. Suppose a 300-digit number n is given. How many squarings are needed in worst case during a single run of this primality test?

Exercise 29. Show that 1031 is invertible modulo 2227 and compute the inverse 1031^{-1} in the ring $\mathbb{Z}_{2227}$.

Exercise 30. Prove the Chinese Remainder Theorem:
Suppose $m_1, \dots, m_r$ are pairwise relatively prime, $a_1, \dots, a_r \in \mathbb{N}$. The system of r congruences

$$x \equiv a_i \pmod{m_i}, \qquad i = 1, \dots, r,$$

has a unique solution modulo $M = \prod_{i=1}^{r} m_i$ given by

$$x = \sum_{i=1}^{r} a_i \, M_i \, y_i \pmod{M},$$

where $M_i = M/m_i$, $y_i = M_i^{-1} \pmod{m_i}$, $i = 1, \dots, r$.

Exercise 31. Solve the following system of linear congruences using the Chinese Remainder Theorem and compute the smallest positive solution:

$$\begin{aligned}
x &\equiv 3 \pmod{11} \\
x &\equiv 5 \pmod{13} \\
x &\equiv 7 \pmod{15} \\
x &\equiv 9 \pmod{27}.
\end{aligned}$$