Homework 8 in Advanced Methods of Cryptography

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

04.12.2012

Exercise 22. Suppose $m_1, \ldots, m_r$ are pairwise relatively prime, $a_1, \ldots, a_r \in \mathbb{N}$. The system of r congruences

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

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

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

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

(a) Prove the Chinese Remainder Theorem given above.

Exercise 23.

Let $x, y \in \mathbb{Z}$, $a \in \mathbb{Z}_n^* \backslash \{1\}$, and $\mathrm{ord}_n(a) = \min\{k \in \{1, \ldots, \varphi(n)\} \mid a^k \equiv 1 \mod n\}$.

(a) Show that $a^x \equiv a^y \pmod{n} \iff x \equiv y \pmod{\mathrm{ord_n(a)}}$.

Exercise 24.

Prove, that if there exists a primitive elements modulo n, then there are $\varphi(\varphi(n))$ many.