Homework 7 in Advanced Methods of Cryptography - Proposal for Solution -

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

20.12.2013

Solution to Exercise 20.

Chinese Remainder Theorem

Let $m_1, \ldots, m_r$ be pair-wise relatively prime, i.e., $\gcd(m_i, m_j) = 1$ for all $i \neq j \in \{1, \ldots, r\}$, and furthermore let $a_1, \ldots, a_r \in \mathbb{N}$. Then, the system of congruences

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

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

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

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

(a) Show that (1) is a valid solution for the system of congruences:

Let $i \neq j \in \{1, \ldots, r\}$. Since $m_j \mid M_i$ holds for all $i \neq j$, it follows:

$$M_i \equiv 0 \pmod{m_j}. \tag{2}$$

Furthermore, we have $y_j M_j \equiv 1 \pmod{m_j}$.

Note that from coprime factors of M, we obtain:

$$\gcd(M_j, m_j) = 1 \Rightarrow \exists\, y_j \equiv M_j^{-1} \pmod{m_j}, \tag{3}$$

and the solution of (1) modulo a corresponding m_j can be simplified to:

$$x \equiv \sum_{i=1}^{r} a_i M_i y_i \overset{(2)}{\equiv} a_j M_j y_j \overset{(3)}{\equiv} a_j \pmod{m_j}.$$

(b) Show that the given solution is unique for the system of congruences:

Assume that two different solutions y, z exist:

$$\begin{aligned} & y \equiv a_i \pmod{m_i} \;\wedge\; z \equiv a_i \pmod{m_i}, \; i = 1, \ldots, r, \\ & \Rightarrow 0 \equiv (y - z) \pmod{m_i} \\ & \Rightarrow m_i \mid (y - z) \\ & \Rightarrow M \mid (y - z), \text{ as } m_1, \ldots, m_r \text{ are relatively prime for } i = 1, \ldots, r, \\ & \Rightarrow y \equiv z \pmod{M}. \end{aligned}$$

This is a contradiction, therefore the solution is unique.