Homework 7 in Cryptography

Prof. Dr. Rudolf Mathar, Markus Rothe, Milan Zivkovic

03.07.2014

Exercise 25. Prove the Chinese Remainder Theorem:
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

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

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

Exercise 26. There is the following system of linear congruences:

$$\begin{aligned} x &\equiv 3 \pmod{11} \\ x &\equiv 5 \pmod{13} \\ x &\equiv 7 \pmod{15} \\ x &\equiv 9 \pmod{17}. \end{aligned}$$

(a) Compute the smallest positive solution using the Chinese Remainder Theorem.

Exercise 27. We consider Wilsons' primality-criterion:

$$\text{An integer } n > 1 \text{ is prime} \Leftrightarrow (n-1)! \equiv -1 \pmod{n}.$$

(a) Prove Wilsons' primality-criterion (both "$\Rightarrow$" and "$\Leftarrow$").

(b) Check if 29 is a prime number by using the criterion above.

(c) Is it useful in practical applications?