Homework 11 in Cryptography I

Prof. Dr. Rudolf Mathar, Michael Naehrig
21.01.2008

Exercise 31. Show, that 1111 is invertible modulo 2041 and compute the inverse 1111^{-1} in the ring $\mathbb{Z}_{2041}$.

Exercise 32.

(a) 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

$$x \equiv a_i (\bmod m_i), \qquad i = 1, \dots, r,$$

has a unique solution modulo $M = m_1 \cdots m_r$ given by

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

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

(b) Solve the following system of linear congruences using the Chinese Remainder Theorem and compute the smallest positive solution:

$$\begin{aligned} x &\equiv 17 \pmod{29} \\ x &\equiv 13 \pmod{15} \\ x &\equiv 5 \pmod{16} \\ x &\equiv 8 \pmod{23}. \end{aligned}$$

Exercise 33. Suppose, Alice and Bob are using the Diffie-Hellman key agreement protocol with a prime $p = 376373$ and primitive root 2 modulo p as parameters. Alice uses the random number 21767, Bob uses 9973.

Conduct the key agreement protocol and compute the common key. What does Alice send to Bob, what does Bob send to Alice?