Homework 1 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Georg Böcherer, Henning Maier

19.10.2010

Exercise 1. 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 2. Factorize $n = 3149$ with the knowledge that $412^2 \equiv 459^2 \equiv 2847 \mod n$.

Exercise 3. Let $a \in \mathbb{Z}_n^\star$ be an element of order k, i.e. $a^k \equiv 1 \pmod{n}$, and $x, y \in \mathbb{Z}$. Show that

$$a^x \equiv a^y \pmod{n} \iff x \equiv y \pmod{k}$$

if and only if $x \equiv y(\mathrm{mod}(\mathrm{ord(a)}))$.

Exercise 4. Given $a^x \equiv 17 \mod 31$ and $x = 13$, calculate basis a.