# Homework 9 in Advanced Methods of Cryptography

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

11.12.2012

**Exercise 25.** 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 26.** Alice and Bob use the Diffie-Hellman key exchange protocol to agree upon a shared key. As system parameters they use the prime number $p = 101$ and the primitive element $a = 2$ modulo $p$. Alice chooses the random secret $x = 37$ and Bob chooses $y = 33$. Use the Square and Multiply algorithm to compute large integer powers.

(a) How does the protocol work? Which values are exchanged between Alice and Bob?

(b) Compute the shared key.

**Exercise 27.** Prove Proposition 7.5 from the lecture, which provides a possibility to check whether $a$ is a primitve element modulo $n$:

Let $p > 3$ be prime, $p - 1 = \prod_{i=1}^{k} p_i^{t_i}$ the prime factorization of $p - 1$. Then, $a \in \mathbb{Z}_p^*$ is a primitive element modulo $p \Leftrightarrow a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p}$ for all $i \in \{1, \ldots, k\}$.

**Exercise 28.** Alice and Bob are using the Shamir's no-key protocol to exchange a secret message. They agree to use the prime $p = 31337$ for their communication. Alice chooses the random number $a = 9999$ while Bob chooses $b = 1011$. Alice's message is $m = 3567$.

(a) Calculate all exchanged values $c_1$, $c_2$, and $c_3$ following the protocol.
**Hint**: You may use $6399^{1011} \mod 31337 = 29872$.