Homework 1 in Advanced Methods of Cryptography

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

18.10.2011

Exercise 1.

(a) Compute $11^{213} \pmod{42}$.

(b) Compute $16^{512} \pmod{17}$ without using the square-and-multiply-algorithm.

Exercise 2.

Consider the following algorithm to compute the discrete logarithm:

Algorithm 1 Babystep-Giantstep-Algorithm

Input: p prime, α as a primitive element mod p, $\beta \equiv \alpha^x \bmod p$ with $\beta \in \mathbb{Z}_p^*$ for an unknown $x \in \{0, \dots, p-1\}$

Output: $x = \log_\alpha \beta$,

(1) $m \leftarrow \lceil \sqrt{p} \rceil$

(2) Compute a table of *babysteps* $b_j = \alpha^j \bmod p$ for all indices $j \in \mathbb{Z}$ in $0 \leq j < m$.

(3) Compute a table of *giantsteps* $g_i = \beta\alpha^{-im} \bmod p$ for indices $i \in \mathbb{Z}$ in $0 \leq i < m$,

(4) until you find a pair (i, j) such that $b_j = g_i$ holds.

return $x = mi + j \bmod (p-1)$.

(a) Prove that the given algorithm calculates the discrete logarithm.

(b) Why is α a primitive element mod p?

(c) Compute the discrete log of $\alpha^x \bmod p = \beta$ with $\alpha = 3$, $p = 29$ and $\beta = 13$.

Remark: The *ceiling-function* is defined as $\lceil x \rceil = \min\{k \in \mathbb{Z} | k \geq x\}$.

Exercise 3.

Let $x, y \in \mathbb{Z}$, $a \in \mathbb{Z}_n^* \backslash \{1\}$, and $\text{ord}_n(a) = \min\{k \in \{1, \dots, \varphi(n)\} | a^k \equiv 1 \mod n\}$.

(a) Show that $a^x \equiv a^y \pmod{n} \iff x \equiv y \ (\text{mod}(\text{ord}_\text{n}(\text{a})))$.

Exercise 4. Solve $a^{13} \equiv 17 \mod 31$. Note that 31 is prime.