Exercise 1 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Markus Rothe

2014-10-24

Problem 1. *(Euler's criterion)* Prove Euler's criterion (Proposition 9.2): Let $p > 2$ be prime, then

$$c \in \mathbb{Z}_p^* \text{ is a quadratic residue modulo } p \Leftrightarrow c^{\frac{p-1}{2}} \equiv 1 \mod p\,.$$

Problem 2. *(baby-step giant-step algorithm)* Consider the following algorithm to compute the discrete logarithm:

Algorithm 1 Baby-step Giant-step Algorithm

Input: p prime, α is a primitive element mod p, $\beta = \alpha^x \mod p$ 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 *baby-steps* $b_j = \alpha^j \mod p$ for all indices $j \in \mathbb{Z}$ with $0 \leq j < m$.

(3) Compute a table of *giant-steps* $g_i = \beta\alpha^{-im} \mod p$ for indices $i \in \mathbb{Z}$ with $0 \leq i < m$, until you find a pair (i, j) such that $b_j = g_i$ holds.

return $x \equiv mi + j \mod p - 1$.

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

b) Why is α a primitive element modulo p?

c) Compute the discrete log for $\alpha^x \equiv \beta \mod p$ with $\alpha = 3$, $\beta = 13$ and $p = 29$ using the given algorithm.

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

Problem 3. *(exponential congruences)* Let $x, y \in \mathbb{Z}, a \in \mathbb{Z}_n^\star \setminus \{1\}$, and $\text{ord}_n(a) = \min\{k \in \{1, \dots, \varphi(n)\} \mid a^k \equiv 1 \mod n\}$. Show that

$$a^x \equiv a^y \mod n \iff x \equiv y \mod \text{ord}_n(a)\,.$$