Homework 9 in Advanced Methods of Cryptography - Proposal for Solution -

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

11.12.2012

Solution to Exercise 27.

Let $p > 3$ be prime and $p-1 = \prod_{i=1}^{k} p_i^{t_i}$ the prime factorization of $p-1$. Show:

$$a \in \mathbb{Z}_p^* \text{ is a primitive element(PE) modulo } p \Leftrightarrow a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p} \ \forall i = 1, \ldots, k.$$

Recall

$$\text{ord}_n(a) = \min\{k \in \{1, \ldots, \varphi(n)\} \mid a^k \equiv 1 \pmod{n}\} \tag{1}$$

$$a \text{ is PE modulo } n \Leftrightarrow \text{ord}_n(a) = \varphi(n) \tag{2}$$

Proof:

„ $\Rightarrow$ " a is PE modulo $p \overset{(2)}{\Leftrightarrow} \text{ord}_p(a) = \varphi(p) = p-1 \overset{(1)}{\Rightarrow} a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p} \ \forall i = 1, \ldots, k$

„ $\Leftarrow$ " Assume a is not PE modulo $p \overset{(2)}{\Rightarrow} \text{ord}_p(a) = k < p-1 \wedge k \mid p-1$

$\Rightarrow \exists\, c \neq 1$ with $p-1 = k \cdot c$

$\Rightarrow \exists\, i : p_i \mid c$

$\Rightarrow a^{\frac{p-1}{p_i}} = a^{\frac{k \cdot c}{p_i}} = (\underbrace{a^k}_{\overset{(1)}{\equiv} 1})^{\frac{c}{p_i}} \equiv 1 \pmod{p}$ Contradiction!