

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

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier
17.01.2014

Solution to Exercise 25.

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

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

Recall

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

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

Proof:

$$,, \Rightarrow \text{“ } a \text{ is a PE modulo } p \stackrel{(2)}{\Leftrightarrow} \text{ord}_p(a) = \varphi(p) = p - 1 \stackrel{(1)}{\Rightarrow} a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p} \quad \forall i = 1, \dots, k$$

$$,, \Leftarrow \text{“ Assume } a \text{ is not a PE modulo } p \stackrel{(2)}{\Rightarrow} \text{ord}_p(a) = k < p - 1 \wedge k \mid p - 1 \quad (\text{cf. Ex. 24})$$

$$\Rightarrow \exists c \neq 1 \text{ with } p - 1 = k \cdot c$$

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

$$\Rightarrow a^{\frac{p-1}{p_i}} = a^{\frac{k \cdot c}{p_i}} = \underbrace{(a^k)^{\frac{c}{p_i}}}_{\stackrel{(1)}{\equiv} 1} \equiv 1 \pmod{p} \quad \nexists \blacksquare$$