Exercise 9 in Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Jose Angel Leon Calvo

2015-07-02

Problem 28. (*modulo Order of Generator*) Let $x, y \in \mathbb{Z}, a \in \mathbb{Z}_n^* \setminus \{1\}$, and $\text{ord}_n(a) = \min\{k \in \{1, \dots, \varphi(n)\} \mid a^k \equiv 1 \mod n\}$.

$$\text{Show that } a^x \equiv a^y \mod n \Leftrightarrow x \equiv y \mod \text{ord}_n(a).$$

Problem 29. *(prove Proposition 7.5)* Prove Proposition 7.5 from the lecture, which gives a possibility to generate a primitive 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,

$$a \in \mathbb{Z}_p^* \text{ is a primitive element modulo } p \Leftrightarrow a^{\frac{p-1}{p_i}} \not\equiv 1 (\text{mod}\, p) \text{ for all } i \in \{1, \dots, k\}.$$

Problem 30. (*number of Primitive Elements Modulo n*) Prove the following statement:

If there exists a primitive elements modulo n, then there are $\varphi(\varphi(n))$ many.

Problem 31. *(Diffie-Hellman key exchange)* Alice and Bob perform a Diffie-Hellman key exchange with prime $p = 107$ and primitive element $a = 2$. Alice chooses the random number $x_A = 66$ and Bob the random number $x_B = 33$.

a) Calculate the shared key for both users.

b) Show that $b = 103$ is also a primitive element mod p.