Homework 8 in Cryptography

Prof. Dr. Rudolf Mathar, Markus Rothe, Milan Zivkovic

11.07.2014

Exercise 28. We examine the properties of the discrete logarithm.

(a) Compute the discrete logarithm of 18 and 1 in the group $\mathbb{Z}_{79}^*$ with generator 3 (by trial and error if necessary).

(b) How many trails would be necessary to determine the discrete logarithm in the worst case?

Exercise 29. 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 $a \in \mathbb{Z}_p^*$ is a primitive element modulo $p \Leftrightarrow a^{\frac{p-1}{p_i}} \not\equiv 1 (\bmod p)$ for all $i \in \{1, \ldots, k\}$.

Exercise 30. 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.