Homework 8 in Advanced Methods of Cryptography

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

10.01.2014

Exercise 21. Prove part b) of Theorem 7.2 from the lecture:
If Z_n^* is a cyclic group, then there exist $\varphi(\varphi(n))$ primitive elements modulo n.

Exercise 22. Alice and Bob use the Diffie-Hellman key exchange protocol to agree upon a shared key. As system parameters they use the prime number $p = 101$ and the primitive element $a = 2$ modulo p. Alice chooses the random secret $x = 37$ and Bob chooses $y = 33$. Use the Square and Multiply algorithm to compute large integer powers.

(a) How does the protocol work? Which values are exchanged between Alice and Bob?

(b) Compute the shared key.

Exercise 23. Santa Claus still has to deliver a lot af presents. He cannot carry all presents at once, but wants to divide the presents in heaps with same quantity. Unfortunately, he has failed so far. While dividing the presents on 5, 7, 8, 9, and 11 heaps, there are 3, 2, 1, 2, and 5 presents left over. Please help Santa Claus and tell him, how many presents he has and which heap sizes are possible. Santa Claus knows that he has less than 50,000 presents.

Merry Christmas and a Happy New Year