Homework 10 in Advanced Methods of Cryptography

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

10.01.2012

Exercise 29.

(a) Suggest a probabilistic algorithm to determine a pair of primes p, q with

$$\begin{array}{rcccl} 2^{159} & < & q & < & 2^{160}, \\ 2^{1023} & < & p & < & 2^{1024}, \\ q & & \mid & & p-1. \end{array}$$

(b) What is the success probability of your algorithm?

Hint: Assume the unproven statement that the number of primes of the form $k\,q+1$, $k \in \mathbb{N}$, is asymptotically the number given by the „prime number theorem“ divided by q.

Exercise 30. For the security of DSA a hash-function is mandatory.

(a) Show that it is possible to forge a signature of a modified scheme where no cryptographic hash function is used.

Hint: This attack is provided in the lecture notes for the ElGamal signature scheme.

Exercise 31. Discuss the following properties of Lamport's protocol:

(a) Show that the one-way function is not required to be secret.

(b) Which properties must a hash function fulfill to be usable as a one-way function in the protocol?

(c) Propose a function that could be used as the one-way function, assuming that the discrete logarithm is hard to solve in $\mathbb{Z}_p^*$ for a usable p. Describe Lamport's protocol for this special case.

(d) How can an attacker get access to a one-time password using an active attack?

Merry Christmas and a Happy New Year