Homework 9 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Georg Böcherer, Henning Maier

14.12.2010

Exercise 29. We consider the parameter generation algorithm of DSA.

It provides prime $2^{159} < q < 2^{160}$ and integer $0 \leq t \leq 8$ such that prime $2^{511+64t} < p < 2^{512+64t}$ and $q|p-1$.

Given the following algorithm:

1) Select $g \in \mathbb{Z}_p^*$,
2) Compute $a = g^{\frac{p-1}{q}} \pmod p$,
3) If $a == 1$, go to label 1),
4) Else return a,

prove that a is a generator of the cyclic subgroup of order q in $\mathbb{Z}_p^*$.

Exercise 30.

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

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

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 31.

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