Homework 8 in Cryptography II

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Steven Corroy
29.06.2010

Exercise 22.

We consider the parameter generation algorithm of DSA.

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

Given the followin algorithm:

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

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

Exercise 23.

Sign the message with the hash value $h(m) = 18723$ with a DSA signature using artificially small numbers. For the public key use $p = 27583, q = 4597, a = 504, y = 23374$. The private key is $x = 1860$.

Afterwards, verify the signature.

Exercise 24.

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

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

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.