Exercise 26. In the verification algorithm of the ElGamal-Signature one first checks, whether $1 \leq r < p$. Show that an attacker can generate a signature for an arbitrary message $m'$ by intercepting one valid signature $(r, s)$ for a message $m$ if this step is omitted.

Hint: Assume that $h(m)$ and $h(m')$ are invertible modulo $p - 1$.

Exercise 27. 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 28. Suggest a probabilistic algorithm to determine a pair of primes $p, q$ with

$$2^{159} < q < 2^{160},$$

$$2^{1023} < p < 2^{1024},$$

$$q \mid p - 1.$$ 

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 $q$. 