Problem 1. *(Variations of the ElGamal signature scheme)* The ElGamal signature scheme computes the signature as \( s = k^{-1}(h(m) - xr) \mod (p - 1) \). Consider the following variations of the ElGamal signature scheme.

- **a)** Consider the signing equation \( s = x^{-1}(h(m) - kr) \mod (p - 1) \).
  Show that \( a^{h(m)} \equiv y^s r^r \mod p \) is a valid verification procedure.

- **b)** Consider the signing equation \( s = xh(m) + kr \mod (p - 1) \).
  Propose a valid verification procedure.

- **c)** Consider the signing equation \( s = xr + kh(m) \mod (p - 1) \).
  Propose a valid verification procedure.

Problem 2. *(DSA parameter generation algorithm)* Consider the parameter generation algorithm of DSA. It provides a prime \( 2^{159} < q < 2^{160} \) and an integer \( 0 \leq t \leq 8 \) such that for prime \( p \), \( 2^{511+64t} < p < 2^{512+64t} \) and \( q \mid p - 1 \) holds.

The following scheme is given:

1. Select a random \( g \in Z_p^* \)
2. Compute \( a = g^{\frac{p-1}{q}} \mod p \)
3. If \( a = 1 \), go to label (1) else return \( a \)

Prove that \( a \) is a generator of the cyclic subgroup of order \( q \) in \( Z_p^* \).

Problem 3. *(DSA hash function)* For the security of 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:** A related attack is provided in the lecture notes for the ElGamal signature scheme.
Problem 4. (Probabilistic algorithm for a pair of primes for DSA)

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

\[
2^{159} < q < 2^{160},
\]
\[
2^{1023} < p < 2^{1024},
\]
\[
q \mid p - 1.
\]

b) What is the success probability of your algorithm?

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