Exercise 26.

There exist many variations of the ElGamal signature scheme which do no compute the
signing equation as \( s = k^{-1}(h(m) - xr) \mod (p - 1) \).

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

Exercise 27.

Consider the Digital Signature Algorithm (DSA) using artificially small numbers. For the
public key use \( p = 27583, q = 4597, a = 504, y = 23374 \). For the private key use \( x = 1860 \)
and the random secret number \( k = 1773 \).

(a) Sign the message with the hash value \( h(m) = 18723 \) and verify the signature.

Exercise 28.

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

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