Exercise 41.
Consider the RSA signature scheme with the public key \((n, e) = (2491, 1367)\).

(a) Factorize the public key \(n\).

(b) Compute the RSA signature for the message \(m = 100\).

(c) Verify the signature.

Exercise 42.
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 \(h(m) = 18723\).

(b) Verify the signature.

Exercise 43.
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:

\[
\begin{align*}
(1) & \text{ Select a random } g \in \mathbb{Z}_p^* \\
(2) & \text{ Compute } a = g^{\frac{p-1}{q}} \mod p \\
(3) & \text{ If } a = 1, \text{ go to label (1) else return } a \\
\end{align*}
\]

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