Chapter 4: Cryptographic Hash Functions
Exercises 4.6, 4.7, 4.9(a), 4.12.

Chapter 7: Digital Signatures
Exercises 7.1, 7.2, 7.3.

Additional question 1
Let \( p = 14747 \), \( q = 101 \), and \( \alpha = 4789 \). Note \( q \mid p - 1 \) and \( \alpha \) is an element of order \( q \) in \( \mathbb{Z}_p \).
Let \( \beta = 3430 \). Solve \( \beta \equiv \alpha^a \mod p \) for \( a \) using any means.

Using the Schnorr Signature algorithm (page 294) with the above values for \( p, q, \alpha, \beta \), and the secret value \( a \) you computed, together with \( k = 11 \) and hash function \( h(z) = 2^z \mod p \), compute the signature for \( x = 1234 \) and verify it using the verification formula.

Additional question 2
Let \( p \) and \( q \) be two large primes of the form \( p = 2r + 1 \), \( q = 2s + 1 \) where \( r \) and \( s \) are also prime. Let \( n = pq \). Suppose \( \alpha \) is a primitive element modulo \( p \) and modulo \( q \). What is the order of \( \alpha \) modulo \( n \)?

Now find the first \( p > 100 \), the first \( q > p \), and the first \( \alpha > 1 \) satisfying these requirements and verify your answer for the order of \( \alpha \).

Consider the public hash function \( h(x) = \alpha^x \mod n \) where \((n, \alpha)\) are public but \((p, q)\) are secret and \((n, \alpha)\) satisfy the requirements from the first part of this question. Prove that \( h(x) \) is collision resistant by showing that if you could find collisions in \( h(x) \) then you could determine \( \phi(n) \) and hence factor \( n \). Notice that \( h(x) \) exploits square-and-multiply.

Illustrate your method by determining \( \phi(n) \) for the \( n \) you found in the first part of this question. You will need to generate collisions for \( h(x) \) on a suitable range for \( x \). Do this as follows. Compute \( h(x_1), h(x_2), ... \) until you find \( x_i \neq x_j \) with \( h(x_i) = h(x_j) \) where \( x_1, x_2, ... \) are generated at random from \([0, 10^6])\).