Solution to Exercise 37.

(a) $\gcd(a, p - 1) \in \{1, 2, q, 2q\}$ for all $a \in \mathbb{N}$ since the factorization is $p - 1 = 1 \cdot 2 \cdot q$.

(b) $p, q$ are prime with $p = 2q + 1$ ($\Rightarrow$ Sophie-Germain primes), $a, b$ are primitive elements, and $0 \leq m \leq q^2 - 1$. The hash function is defined by:

$$h(m) = a^{x_0}b^{x_1} \mod p$$

with $0 \leq x_0, x_1 \leq q - 1 \land m = x_0 + x_1q$. The given function is slow but collision-free.

Proof: Assume there is a collision, i.e., at least one pair of messages satisfies:

$$m \neq m' \land h(m) = h(m').$$

It is to show that the discrete logarithm $k = \log_a(b) \mod p$ can be determined if a collision is known. The two different messages are as in Ex. 10.2:

$$m = x_0 + x_1q,$$
$$m' = x_0' + x_1'q,$$

and the common hash-value is:

$$h(m) = h(m').$$

Ex. 10.2 $\iff k(x_1 - x_1') \equiv x_0' - x_0 \pmod{p - 1}.$$

(1)

Furthermore, $x_1 - x_1' \neq 0 \pmod{p - 1}$, otherwise it would follow that $m = m'$.

To determine $k$, assume both $0 \leq k, k' < p - 1$ fulfil (1). Then

$$k(x_1 - x_1') \equiv x_0' - x_0 \pmod{p - 1} \land$$
$$k'(x_1 - x_1') \equiv x_0' - x_0 \pmod{p - 1}$$

$$\Rightarrow (k - k')(x_1 - x_1') \equiv 0 \pmod{p - 1}.$$ (2)

It holds:

$$-(p - 1) < k - k' < p - 1 \land x_1 \neq x_1' \land -(q - 1) \leq x_1 - x_1' \leq q - 1.$$ (3)

Let $d = \gcd(x_1 - x_1', p - 1)$, then it follows from (1) that $d \mid (x_0' - x_0)$:
1) $d = 1 \Rightarrow k - k' \equiv 0 \mod{p - 1} \Rightarrow k \equiv k' \mod{p - 1}$, i.e., there is the solution:

$$k = (x_1 - x'_1)^{-1}(x'_0 - x_0) \mod{(p - 1)}.$$ 

2) $d > 1$:

\[
\tag{1}
k \left( \frac{x_1 - x'_1}{d} \right) \equiv \left( \frac{x'_0 - x_0}{d} \right) \left( \mod{\frac{p - 1}{d}} \right).
\]

It holds $\gcd\left( \frac{x_1 - x'_1}{d}, \frac{p - 1}{d} \right) = 1$ \xrightarrow{1)} (3) has exactly one solution $k_0 < \frac{p - 1}{d}$:

\[
\tag{3}
k_0 = \left( \frac{x_1 - x'_1}{d} \right)^{-1} \left( \frac{x'_0 - x_0}{d} \right) \left( \mod{\frac{p - 1}{d}} \right).
\]

For the solution of (1), this yields multiple candidates: $k_l = k_0 + \left( \frac{p - 1}{d} \right) \cdot l$, with $l = 0, \ldots, d - 1$.

Recall from (a) that $p - 1 = 2q \Rightarrow d \in \{1, 2, q, 2q\} \Rightarrow d \in \{1, 2\}$ as $(x_1 - x'_1) \leq q - 1 \Rightarrow d = 2$ as $d > 1$.

Check all candidates $k_0, k_1$, i.e., check if $a^{k_0} \equiv b \mod{p}$ or if $a^{k_0 + \frac{p - 1}{2}} \equiv b \mod{p}$ holds.

The candidate fulfilling the congruence is $\log_a(b)$.

Altogether, finding collisions is hard because the determination of a discrete logarithm is computationally extensive.