Question 1 (70 points, 10 points each)

State whether the following statements are True or False:

(a) Subtraction (i.e. \( f(x, y) = x - y \)) is associative. \( \text{False} \)

(b) The function \( f(x, y) = 1^{|x|} \cdot 1^{|y|} \) (where \( 1^a \) represents the string 1 repeated \( a \) times, and \( x \cdot y \) represents \( x \) concatenated with \( y \)), is commutative. \( \text{False} \)

(c) The function \( f(x, y) = \begin{cases} 1y, & |x| \text{ is odd} \\ 0y, & |x| \text{ is even} \end{cases} \) is total. \( \text{True} \)

(d) These two statements are equivalent:
1. 2-ary one-way functions exist.
2. \( P \neq NP \). \( \text{True} \)

(e) One-way functions exist if and only if strongly noninvertible, total, commutative, associative, 2-ary one-way functions exist. \( \text{True} \)

(f) For any function \( h(x) \), 2-ary function \( f(x, y) = h(x) \) is associative. \( \text{False} \)

(g) If \( P \neq NP \) then there exists a one-way function \( f \) with fixed point.
\( (\exists x_0 \in \text{domain}(f) : f(x_0) = x_0) \) \( \text{True} \)
Question 2 (30 points, 10 points each)

Fill in the blanks based on the material covered in the previous class:

1. A total 2-ary function \( f \) is associative exactly if for all \( x, y, z \in \Sigma^* \), \( f(f(x, y), z) = f(x, f(y, z)) \).

2. A total, 2-ary function \( f \) is commutative exactly if for all \( x, y \in \Sigma^* \), \( f(x, y) = f(y, x) \).

3. In the slides, we looked at a potential application of one-way functions in cryptography. Specifically, we outlined a possible key agreement protocol. This protocol assumed the existence of a 2-ary, one-way function \( f \) with two properties. These properties were that \( f \) is strongly noninvertible and associative.