Please answer the following questions, each of which is worth 10 points.

1. Show that if a hash function is strongly collision-resistant, then it is weakly collision-resistant.

2. Consider the Merkle Hash tree, which is an authenticated dictionary that prove that an element \( x \) belongs to a set \( S \) (of all the values associated with the leaves of the hash tree). Devise a scheme for extending the Merkle Hash tree so that it can prove that an element \( x \) is not in the set \( S \).

3. Define a hash function, \( h(x, y) = g^x h^y \mod p \), where \( p \) is a prime and \( g \) and \( h \) are generators of the group \( \mathbb{Z}_p^* \). Show that if you could find \( a, b, c, d \) such that \( a \neq b \) and \( c \neq d \) yet \( h(a, b) = h(c, d) \), then you can solve the corresponding discrete logarithm problem. That is, you can find \( z \) such that \( g^z \mod p = h \).

4. Alice has lost her private key for RSA encryption, but she still knows her public key. That is, she knows a number \( n = pq \), where \( p \) and \( q \) are large primes, and she knows an exponent \( e \) that is relatively prime to \( n \). But she has forgotten \( p \) and \( q \) and \( d \), the multiplicative inverse of \( e \mod \phi(n) \). Rather than throw away the values \( n \) and \( e \), Alice wants to now use encryption with her public key as a hash function. That is, for any message \( M \) (even one bigger than \( n \)), she wants to compute the hash of \( M \) as \( h(M) = M^e \mod n \). Is this hash function one-way?

5. Suppose Alice has forgotten her private information for El Gamal encryption. Explain why Alice cannot use El Gamal encryption using her public key as a hash function.