HW10  20 points  Due Oct 7

1) List two disputes that can arise in the message authentication (The ones we have covered in class).

Suppose that John sends an authenticated message to Mary. The following disputes that could arise:

a) Mary may forge a different message and claim that it came from John. Mary would simply have to create a message and append an authentication code using the key that John and Mary share.

b) John can deny sending the message. Because it is possible for Mary to forge a message, there is no way to prove that John did in fact send the message.

2) What is the difference between MAC and one way hash function?

A hash function, by itself, does not provide message authentication. A secret key must be used in some fashion with the hash function to produce authentication. A MAC, by definition, uses a secret key to calculate a code used for authentication.

3) What is the difference between strong and weak collision resistance?

Weak Collision resistance:
For any given block x, it is computationally infeasible to find y ≠ x with \( H(y) = H(x) \).

Strong collision resistance:
It is computationally infeasible to find any pair (x, y) such that \( H(x) = H(y) \).

4) What is the role of the compression function in a hash function?

A typical hash function uses a compression function as a basic building block, and involves repeated application of the compression function.