The University of North Carolina at Greensboro
CSC 580: Cryptography and Security in Computing
Prof. Stephen R. Tate

Handout 16
March 22, 2018

Homework 7 – Due Tuesday, March 27

1. The basic Diffie-Hellman key exchange protocol is vulnerable to a "man-in-the-middle" attack, as explained in the textbook. Describe this attack.

2. Consider a cryptographic hash function $f : \{0,1\}^n \to \{0,1\}^h$ that satisfies the preimage resistance property and second preimage resistance property, even though it only works on fixed-size input blocks. Joe needs a function like this, but it has to work on *pairs* of n-bit inputs, so he defines $g : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^h$ as

$$g(x, y) = f(x \oplus y).$$

   Is this function preimage resistant? Does it satisfy the second preimage resistance property? Justify both answers!

3. Prove that a hash function that satisfies the collision resistance property also satisfies the second preimage resistance property. (*Hint: Write the statement you're trying to prove as an implication, and then prove the logical contrapositive.*)