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

Handout 19
March 30, 2017

Homework 9 – Due Tuesday, April 4

1. Consider a cryptographic hash function $f : \{0,1\}^n \rightarrow \{0,1\}^h$ 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 $g : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^h$ as

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

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

2. 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.*)

3. Does a hash function that has second preimage resistance also satisfy the preimage resistance property? To answer this question, consider a hash function $H(x)$ that produces k-bit hash codes, and satisfies all three of the hash function security properties. Now construct a hash function $H'(x)$ that produces $(k+1)$-bit hash codes as follows: If x is exactly k bits long, then output $0\|x$ (a single 0 bit followed by x); otherwise output $1\|H(x)$ (a single 1 bit followed by the H-hash code of x). Is $H'(x)$ second preimage resistant? Is it preimage resistant? Justify your answers!