CSE 40622 Cryptography, Spring 2018
Written Assignment 05 (Lecture 14)

Name: **Jasmine Walker**

1. (20 pts) Formally define the second pre-image resistance and pre-image resistance of hash functions by designing a game and showing the relationship between the adversary's advantage and a negligible function of the security parameter. In other words, try to mimic what I did in Definition 2.

   Answer:
   For second pre-image resistance, the game is:

   - The challenger chooses the security parameter 1^k and a seed $s \leftarrow KeyGen(1^k)$ for some key generation function $KeyGen$. The challenger also chooses some x. The challenger publishes 1^k, s, and x.
   - The adversary chooses a x' which does not equal x.

   If for all PPTA $\mathcal{A}$ there exists some negligible function $negl(k)$ such that the following is true, we say $H(.,.)$ is second pre-image resistant.

   $$Adv^{\mathcal{A}}_{secpre} = Pr[H(x,s) = H(x',s) | x \neq x', x' \leftarrow \mathcal{A}(1^k, s)] \leq negl(k)$$

   where $Adv^{\mathcal{A}}_{secpre}$ denotes the adversary's advantage.

   For pre-image resistance, the game is:

   - The challenger chooses the security parameter 1^k and a seed $s \leftarrow KeyGen(1^k)$ for some key generation function $KeyGen$. The challenger also chooses some x and computes $H(x,s)$. The challenger publishes 1^k, s, and $H(x,s)$.
   - The adversary chooses a x'.

   If for all PPTA $\mathcal{A}$ there exists some negligible function $negl(k)$ such that the following is true, we say $H(.,.)$ is pre-image resistant.

   $$Adv^{\mathcal{A}}_{pre} = Pr[H(x,s) = H(x',s) | x' \leftarrow \mathcal{A}(1^k, s)] \leq negl(k)$$

   where $Adv^{\mathcal{A}}_{pre}$ denotes the adversary's advantage.