Pregunta 4

4. Se propone una definición de resistencia a preimagen en base al juego $Hash-Col(n)$ mostrado en clases de la siguiente forma:

   (a) El verificador toma una entrada 1^n y genera $s = Gen(1^n)$. Escoge con distribución uniforme un mensaje $m \in \mathcal{M}$, calcula $h^s(m) = c$ y entrega s y c al adversario.

   (b) El adversario escoge un mensaje m'.

   (c) El adversario gana si $h^s(m') = c$.

   Luego, se puede definir una función de hash (Gen, h) como resistente a preimagen si para todo adversario que funciona como un algoritmo aleatorizado de tiempo polinomial, existe una función despreciable $f(n)$ tal que: $Pr(Adversario\ gane\ el\ juegoparaunn) \leq f(n)$.

   Para demostrar que resistencia a colisiones implica resistencia a preimagen, se utlizará el método de contrapositivo. Luego, se demostrará que la no resistencia a preimagen implica no resistencia a colisiones.

   Se tiene entonces una función de hash que no es resistente a preimagen. Por definición, existe un algoritmo eficiente que dado $x \in \mathcal{H}$, encuentra $m \in \mathcal{M}$ tal que $h(m) = x$. Si se considera que existen colisiones, se puede utilizar dicho algoritmo para encontrar, a partir de una imagen x, una preimagen a de forma eficiente. Más aún, considerando existencia de colisiones, se puede encontrar otra preimagen b a partir del mismo algoritmo de forma eficiente, ya que, como se definió anteriormente, para que no sea resistente a preimagen, debe existir algoritmo aleatorizado de tiempo polinomial que pueda ganar el juego. Luego, utilizando más de una vez el algoritmo, es posible encontrar a y b tales que $h(a) = h(b)$ de forma eficiente, demostrando que resistencia de colisiones implica resistencia a preimagen.