NOMBRE: Ignacia Baeza Nº LISTA:

PUNTAJE:

Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación

IIC3253 — Criptografía y Seguridad Computacional — 1' 2022

Tarea 1 – Respuesta Pregunta 4

Para definir la noción de resistencia a preimagen, se propone un juego análogo al juego visto en clases para la noción de resistencia a colisiones.
El juego es el siguiente:

- El verificador genera $S = Gen(1^n)$ y se lo entrega al adversario.
- El adversario usa h^s para elegir un mensaje m.
- El verificador entrega al adversario x tal que $h^s(m) = x$.
- El adversario elige un mensaje $m_1 \neq m$.
- El adversario gana si $h^s(m_1) = x$, lo ue significa que el adversario puede saber cual es el mensaje sabiendo el mensaje hasheado.

Este juego describe la noción de preimagen.
Para demostrar que si (Gen, h) es resistente a colisiones es resistente a preimagen, lo haremos por contradicción, diciendo que si (Gen, h) es resistente a colisiones entonces (Gen, h) no es resistente a preimagen.
Si (Gen, h) es resistente a colisiones sabemos que no pueden existir dos mensajes m_1, m_2 con $m_1 \neq m_2$ tal que $h^s(m_1) = h^s(m_2)$.
Queremos demostrar que (Gen, h) no es resistente a preimagen, es decir que el adversario, teniendo un mensaje m_1 y $h^s(m_1) = x$, puede encontrar otro mensaje m_2 con $m_1 \neq m_2$ tal que $h^s(m_2) = x$. Esto es una contradicción ya que si (Gen, h) es resistente a colisiones no pueden existir dos mensajes m_1, m_2 con $m_1 \neq m_2$ tal que $h^s(m_1) = h^s(m_2)$, por lo que si (Gen, h) es resistente a colisiones, debe ser resistente a preimagen.