NOMBRE: Jeremias Molina Riquelme

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

IIC3253 — Criptografia y Seguridad Computacional — 1' 2022

Tarea 1 – Respuesta Pregunta 4

Definimos el juego Hash-pre(n):
1. El verificador genera $s = Gen(1^n)$ y encripta un mensaje $h^s(m) = m'$ y le envia m' al adversario
2. El adversario elige pre-imagen de m' = p
3. Si $h^s(p) = m'$ entonces el adversario gana el juego.

Formalizando se dice que (Gen, h) es resistente a colisiones si para todo adversario que funciona como algoritmo aleatorizado de tiempo polinomial, existe funcion despreciable f(n) tal que:
Pr(adversario gane Hash-pre(n)) $\leq f(n)$