PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN

Criptografía y Seguridad Computacional - IIC3253
1er semestre - 2022
Lothar Droppelmann

Ayudantía 4

Pregunta 1

Sean (Gen_1, H_1) y (Gen_2, H_2) dos funciones de hash criptográficas. Se define (Gen, H) como: Gen corre Gen_1 y Gen_2 y obtiene las llaves s_1 y s_2, luego $H^{s_1,s_2}(x) = H^{s_1}(x)||H^{s_2}(x)$.

1. Demuestre que si al menos una de (Gen_1, H_1) ó (Gen_2, H_2) es resistente a colisiones, entonces (Gen, H) también lo es.

2. Pruebe si al menos una de (Gen_1, H_1) ó (Gen_2, H_2) es resistente a preimagen, entonces (Gen, H) también lo es.

Pregunta 2

Sea (Gen, H) una función de hash criptográfica con resistencia a colisiones. Se define $(Gen, \hat{H})$ como: $\hat{H}^s(x) = H^s(H^s(x))$. Pruebe si $(Gen, \hat{H})$ es resistente a colisiones.