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

IIC3253 - Criptografía y Seguridad Computacional (I/2023)

Ayudantía 3

Ayudantes: Susana Figueroa (sfigueroa3@uc.cl)

Pregunta 1: Funciones despreciables

(a) Muestre que 2^{-n} y $n^{-log(n)}$ son funciones despreciables.

(b) Demuestre que si f y g son funciones despreciables, entonces $f + g$ y $f \cdot g$ son funciones despreciables.

Pregunta 2: Hash-Col

[2022 - Tarea 1] Considere el juego *Hash-Col*(n) mostrado en clases para definir la noción resistencia a colisiones. Utilizando este tipo de juegos, defina la noción de resistencia a preimagen para una función de hash (Gen, h). Además, demuestre que si (Gen, h) es resistente a colisiones, entonces (Gen, h) es resistente a preimagen.