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 2

Definimos la siguiente estrategia: Enviamos cualquier string (podria ser 0000 por ejemplo) y recibimos f(y), aca tenemos dos opciones:
Si f(y) parte con 1 elegimos b=0
Si f(y) parte con 0 elegimos b=1
Con esta estrategia las probabilidad de ganar son:
Pr(Adversario gane el juego — b=0) =1/2, si la clave parte con 0 hay una mitad de probabilidades que haya sido generada por Gen o la mitad de probabilidades que haya sido generada por una permutacion, como siempre votamos en este caso por b=0 (Gen), entonces solo tenemos un medio de probabilidad de acertar.
Pr(Adversario gane el juego — b=1) = 1 debido a que elegimos b=1 cuando parte con 0 nunca nos equivocaremos ya que Gen no genera claves que comiencen con 0.
Finalmente 1/2*Pr(Adversario gane el juego — b=0)+1/2Pr(Adversario gane el juego —b=1)= 1/2 + 1/4 = 3/4
Demostrando asi lo pedido.