NOMBRES: Benjamín Lepe

N.ALUMNO: 17641756

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

IIC3253 — Criptografía y Seguridad Computacional — 1' 2022

Tarea 1 - Pregunta 2

Se debe demostrar que la probabilidad de que un adversario gane sea mayor o igual a 3/4. Para esto se debe calcular la siguiente probabilidad:

$$P(G) = \text{Probabilidad de que el adversario gane}$$

$$P(G) = P(G \cap b = 0) + P(G \cap b = 1)$$

Estas dos probabilidades dependen además del valor que se obtenga en el primer bit de la llave k_1, por lo tanto, debemos calcular estas probabilidades por separado:

$$\begin{aligned}
P(G \cap b = 0) &= P(G|k_1 = 0) \cdot P(k_1 = 0|b = 0) \cdot P(b = 0) + P(G|k_1 = 1) \cdot P(k_1 = 1|b = 0) \cdot P(b = 0) \\
&= 0 + 2/3 \cdot 1 \cdot 1/2 \\
&= 1/3 \\
P(G \cap b = 1) &= P(G|k_1 = 0) \cdot P(k_1 = 0|b = 1) \cdot P(b = 1) + P(G|k_1 = 1) \cdot P(k_1 = 1|b = 1) \cdot P(b = 1) \\
&= 1 \cdot 1/2 \cdot 1/2 + 2/3 \cdot 1/2 \cdot 1/2 \\
&= 1/4 + 1/6 \\
&= 5/12
\end{aligned}$$

Finalmente si sumamos estas dos probabilidades nos entregará la probabilidad de que el adversario gane:

$$P(G) = P(G \cap b = 0) + P(G \cap b = 1) = 3/4$$

Al ser mayor o igual a 3/4 significa que el usuario tiene una probabilidad significante de ganar y, por lo tanto, (Gen, Enc, Dec) no es una PRP.