Pregunta 2

Consideremos la siguiente estrategia:

- Elegimos $y = 0^N$ y nos entregan $f(y)$
- Como el primer bit de la clave siempre es 1, tenemos 2^{N-1} posibles claves para encriptar.

Procedemos a encriptar 0^N con todas las 2^{N-1} llaves utilizando Enc, obteniendo 2^{N-1} mensajes encriptados.

Luego, revisamos si $f(y)$ se encuentra en los mensajes que encriptamos. Si es así, retorna $b=0$. Sino, responde $b=1$

Ahora analicemos la probabilidad $P(win)$ de que gane el Adversario

$$P(win) = P(win|b=0)\cdot\frac{1}{2} + P(win|b=1)\cdot\frac{1}{2}$$

- Si $b=0$, entonces necesariamente $f(y)$ se encuentra dentro de las 2^{N-1} llaves que generamos, por lo que siempre se responde $b=0$. Por lo tanto:

$$P(win|b=0) = 1$$

- Si $b=1$, se nos entrega una de las 2^N posibles permutaciones, de las cuales 2^{N-1} nos equivocamos ya que corresponden a las que generamos y dijimos $b=0$. Así:

$$P(win|b=1) = \frac{\#Favorables}{\#totales} = \frac{2^{N-1}}{2^N} = \frac{1}{2}$$

Finalmente,

$$P(win) = \underbrace{\frac{1}{2} \cdot 1}_{P(win|b=0)} + \underbrace{\frac{1}{2} \cdot \frac{1}{2}}_{P(win|b=1)} = \frac{3}{4} \; //$$

Por lo tanto, con 1 sola ronda demostramos que este esquema no es una PRP ya que $P(win) = \frac{3}{4} >> \frac{1}{2}$