Pregunta 2

2. Considerando el esquema criptográfico (Gen, Enc, Dec), para demostrar que no es una pseudo-random permutation (PRP), se demostrará que existe un adversario que puede ganar el juego para definir una PRP con una probabilidad significativamente mayor a 1/2.

   Luego, el adversario propuesto sigue la siguiente estrategia. Dado que para la definición del juego no impusieron restricciones en las capacidades del adversario, este tiene capacidad computacional 'infinita'.

   Por enunciado, las llaves del esquema criptográfico no admite llaves que comiencen con bit 0, por lo tanto, si en el espacio original se tenían a lo más 2^n posibles llaves, con la restricción hay 2^{n-1} llaves posibles.

   Entonces, lo primero que realiza el adversario es enviar un mensaje cualquiera al verificador, sea el mensaje $m = 0^n$ y recibe $c = f(y)$. Segundo, calcula todas las llaves posibles, que son 2^{n-1}. Y, asumiendo el principio de Kerckhoffs, el algoritmo de encriptación y decriptación es conocido, por lo tanto es posible encriptar y decriptar usando las llaves calculadas recientemente. Tercero, el adversario verifica si es que existe una llave k que decripta tal que $m = Dec(k, c)$. Si existe dicha llave k, entonces retorna $b = 0$, en caso contrario, realiza otro paso extra. El adversario verifica si es que hay llave k tal que $c = Enc(k, m)$, esto porque al ser el espacio de llaves posibles más pequeño que el total de llaves de largo n, hay encriptaciones que no son alcanzables por la función de encriptación, pero si por la función de permutación. A partir de esto, el adversario retorna $b = 1$ cuando no existe llave k que encripte m como c, y retorna $b = 1$ en caso contrario.

   Por último, se debe calcular la probabilidad de que este adversario gane el juego. Esta probabilidad se puede representar como

$$Pr(Adv\ gane) = Pr(Adv\ gane|b = 0) * Pr(b = 0) + Pr(Adv\ gane|b = 1) * Pr(b = 1)$$
$$Pr(Adv\ gane) = Pr(Adv\ gane|b = 0) * \tfrac{1}{2} + Pr(Adv\ gane|b = 1) * \tfrac{1}{2}$$

   Ahora, es claro que si $b = 0$, entonces existe una llave k que es tal que $m = Dec(k, c)$, puesto que m debe haber sido encriptado por alguna llave k perteneciente al espacio de llaves. Por lo tanto, $Pr(Adv\ gane|b = 0) = 1$. Falta calcular $Pr(Adv\ gane|b = 1)$.

   Supuesto Para realizar este cálculo se hará un supuesto, y este es que Enc encripta con distribución uniforme los mensajes, esto es, que los mensajes no convergen a una codificación en particular. Este supuesto facilita los cálculos y también corresponde al peor caso, puesto que este tipo de encriptaciones se ven más como una permutación, siendo la forma más difícil de diferenciar para este caso. Lo anterior debido a que como el algoritmo de encriptación se asume como conocido, se pueden ocupar mejores técnicas personalizadas para ganar el juego, tal como se hizo en el primer ejemplo de PRP en clases. **Fin Supuesto**

   Para que el adversario gane cuando $b = 1$, tiene que ocurrir que ninguna entrada en la tabla de permutaciones tiene como resultado una encriptación por alguna llave de las llaves válidas. Por enunciado, las llaves válidas corresponden a la mitad de las llaves posibles, por lo tanto, considerando el supuesto de que las codificaciones distribuyen uniformemente y que el adversario tiene calculadas todas las llaves válidas, entonces conoce la mitad de

las codificaciones posibles para un mensaje. Luego, la probabilidad de que la función de permutación entregue

, sin embargo, se calculará el equivalente que sería $1 - Pr(Adv\ pierda|b = 1)$. Esto ocurre cuando el adversario retorna $b = 1$, pero era $b = 0$, esto es, cuando existe una llave k tal que $m = Dec(k, c)$, y además al aplicar la permutación sobre m resulta c. Para calcularlo, se puede ver como la probabilidad de que la permutación correspondiente a la entrada m de un total de 2^n entradas tenga como valor de llegada c. Entonces dicha probabilidad es $\frac{1}{2^n}$.

Entonces se tiene

$$1 - Pr(Adv\ pierda|b = 1) = 1 - \frac{1}{2^n}$$

, cuyo mayor valor es para $n = 1$ (el mínimo para que tenga sentido), resultando en$\frac{1}{2}$. Por lo tanto,

$$Pr(Adv\ gane) = Pr(Adv\ gane|b = 0) * \frac{1}{2} + Pr(Adv\ gane|b = 1) * \frac{1}{2} = 1 * \frac{1}{2} + \frac{1}{2} * \frac{1}{2} = \frac{3}{4}$$

que es significativamente mayor que $\frac{1}{2}$, demostrando así que el esquema no es una PRP.