



Tarea 1

Pregunta 2

Sea (Gen, Enc, Dec) un sistema criptográfico definido sobre $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0, 1\}^n$. Se utilizará el juego para demostrar que el sistema dado no es una PRP si se tiene Gen tal que $Gen(0\{0, 1\}^{n-1}) = 0$ y $Gen(1\{0, 1\}^{n-1}) = 1$.

i) Verificador elige $b \in \{0, 1\}$ uniformemente y define $f(x)$.

ii) Adversario elige $y = 0^n$.

iii) Verificador responde con $f(y)$.

iv) Adversario calcula $Enc(k, y)$ para todo $k \in 0\{0, 1\}^{n-1}$. Si ocurre que $Enc(k, y) = f(y)$ para algún k responde $b = 1$, de lo contrario $b = 0$.

Normalmente que el adversario calcule todas las posibles encriptaciones no entrega nada de información. Esto porque la función encriptadora y la función generadora de claves distribuyen uniformemente. Si embargo, en este caso se tiene que Gen le asigna probabilidad 0 a la mitad de las llaves. Esto último es terrible para el sistema, ahora solo la mitad de las codificaciones pueden ser producidas.

En la práctica, para cada mensaje m , al elegir llaves según Gen sólo se terminarán utilizando 2^{n-1} llaves. Por lo tanto, cada m puede codificarse en 2^{n-1} codificaciones distintas. El adversario se aprovecha de esto para ganar. Lo que intenta encontrar es si el verificador produjo una codificación inalcanzable por Enc . Si la codificación es inalcanzable responde que se usó una permutación, de lo contrario adivina que se usó la encriptación.

El cálculo de la probabilidad de ganar será:

$$\begin{aligned} Pr(\text{Adversario gane}) &= Pr(\text{Adversario gane} \mid b = 0) \times Pr(b = 0) + Pr(\text{Adversario gane} \mid b = 1) \times Pr(b = 1) \\ Pr(\text{Adversario gane}) &= Pr(\text{Adversario gane} \mid b = 0)/2 + Pr(\text{Adversario gane} \mid b = 1)/2 \end{aligned}$$

$Pr(\text{Adversario gane} \mid b = 0) = 1$ porque el verificador no producirá una codificación inalcanzable y el adversario responderá $b = 0$.

$Pr(\text{Adversario gane} \mid b = 1) = 1/2$ porque el verificador utilizará una permutación y esta tiene una probabilidad de $1/2$ de producir un mensaje que vendría de encriptar con una llave que empieza por 1 y una probabilidad de $1/2$ para una llave que empieza por 0. Si la permutación produce una codificación inalcanzable (la mitad de las veces), entonces el adversario responderá $b = 1$ y ganará.

Retomando el cálculo final se tiene que: $Pr(\textit{Adversario gane}) = Pr(\textit{Adversario gane} \mid b = 0)/2 + Pr(\textit{Adversario gane} \mid b = 1)/2$ $Pr(\textit{Adversario gane}) = 1/2 + 1/2 \times 1/2 = 3/4$. Luego, $3/4$ es significativamente mayor a $1/2$ por lo que este esquema no es una pseudo-random permutation.