PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN

Criptografía y Seguridad Computacional - IIC3253
1er semestre - 2022
Lothar Droppelmann

Ayudantía 2

Pregunta 1

Pregunta 4 de la Tarea 1 del año 2021.

Sean M, K y C espacios de mensajes, llaves y textos cifrados, respectivamente, tales que $M = K = C = \{0,1\}^n$ con $n \geq 1$. Para un sistema criptográfico (Enc, Dec) sobre M, K y C, se define el siguiente juego con parámetros $r, q \geq 1$:

(1) El verificador escoje $b \in \{0,1\}$ con distribución uniforme.

  (1.1) Si $b = 0$, entonces el verificador escoje con distribución uniforme $K' \subseteq K$ tal que $|K'| = r$.

  (1.2) Si $b = 1$, entonces el verificador escoje con distribución uniforme una permutación $\pi : M \to M$.

(2) Para $i = 1, 2, \ldots, q$ se realizan los siguientes pasos.

  (2.1) El adversario elije un mensaje $m_i \in M$.

  (2.2) Si $b = 0$, entonces el verificador responde de la siguiente forma. Si $m_i \neq m_j$ para cada $j \in \{1, \ldots, i-1\}$, entonces el verificador escoje $k \in K'$ con distribución uniforme y entrega la respuesta $Enc(k, m_i)$. Si $m_i = m_j$ para algún $j \in \{1, \ldots, i-1\}$, entonces el verificador entrega la misma respuesta que en el paso j (vale decir, la misma respuesta que para el mensaje m_j).

  (2.3) Si $b = 1$, entonces el verificador entrega la respuesta $\pi(m_i)$.

(3) El adversario indica si $b = 0$ o $b = 1$, y gana si su elección es la correcta.

El sistema criptográfico (Enc, Dec) se dice un r-pseudorandom permutation (r-PRP) si no existe un adversario que pueda ganar el juego anterior con una probabilidad significativamente mayor a $\frac{1}{2}$. Nótese que el concepto de pseudorandom permutation visto en clases corresponde con esta noción para $r = 1$.

Considerando $M = K = C = \{0,1\}^{128}$, demuestre que OTP no es un 1000-PRP si consideramos un juego con 40 rondas ($q = 40$) y una probabilidad que gane el adversario mayor o igual a $\frac{3}{4}$ (en este caso $\frac{3}{4}$ se considera significativamente mayor a $\frac{1}{2}$).