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

IIC3253 - Criptografía y Seguridad Computacional (I/2023)

Ayudantía 2

Ayudantes: Susana Figueroa (sfigueroa3@uc.cl) Chris Klempau (christian.klempau@uc.cl)

Pregunta 1: OTP

(a) Correctitud de OTP

Demuestre que: $\forall_{k \in \mathcal{K}} \quad Dec_k(Enc_k(m)) = m$

(b) Modelos de ataque para OTP (al reutilizar llaves)

¿Bajo qué modelos de ataque es seguro OTP?
1. Texto cifrado
2. Texto plano
3. Texto plano elegido
4. Texto cifrado elegido

Pregunta 2: Perfect Secrecy

Demuestre las definiciones alternativas de *perfect secrecy*:

(a) **Definición alternativa 1:**

"La probabilidad de ver cualquier texto cifrado sin conocimiento previo es la misma que la probabilidad de ver dicho texto cifrado conociendo el mensaje de antemano."

(b) **Definición alternativa 2:**

"La distribución de probabilidad sobre los mensajes es independiente de la distribución de probabilidad sobre los textos cifrados."

Pregunta 3: PRP

[2022 - Tarea 1] Considere un esquema criptográfico (Gen, Enc, Dec) definido sobre los espacios $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^n$. Suponga además que Gen no permite claves cuyo primer bit sea 0, y que el resto de las claves son elegidas con distribución uniforme. Demuestre que este esquema no es una pseudo-random permutation con una ronda, si $\frac{3}{4}$ es considerada como una probabilidad significativamente mayor a $\frac{1}{2}$.