Pontificia Universidad Católica de Chile
Departamento de Ciencias de la Computación
IIC3253 – Criptografía y Seguridad Computacional
Primer Semestre del 2025

Ayudantía 04

MAC

Ayudante: Martín Orrego – martinorregosilva@uc.cl

Problema 1

Suponga que usted posee un *tag* t generado a partir de un mensaje M y una llave k. Analice las siguientes situaciones e indique cuales presentan una cierta vulnerabilidad, y, en caso de tenerla, indique el ataque que podría ser ejecutado y si existe algun supuesto de seguridad que eliminaria el riesgo.

1. t no depende del primer bit del mensaje M.
2. $t = M \oplus k$, considerando que k es del mismo largo que M y sigue una distribución uniforme.

Problema 2

Considere el siguiente procedimiento para obtener un MAC para mensajes de largo $l(n) = 2n - 2$ utilizando una función pseudoaleatoria F:

- El mensaje se define como $m = m_0||m_1$, con m_0 y m_1 de largo $n - 1$ y la llave $k \in \{0,1\}^n$.
- El tag se define como $t = F_k(0||m_0)||F_k(1||m_1)$.
- $Verify$ se define de la forma natural, es decir, dado un mensaje m y una llave k, $t' = F_k(0||m_0)||F_k(1||m_1)$ y se verifica si $t = t'$.

¿Es este procedimiento un MAC seguro? Justifique su respuesta.