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 6

Definición Experimento CPA

CPA: Chosen Plaintext Attack

Se define el *CPA indistinguishability experiment* para un adversario polinomial A, un esquema (Gen, Enc, Dec) y un parámetro de seguridad n de la siguiente manera:

1. El verificador genera una llave k con $Gen(1^n)$.
2. El adversario recibe 1^n y acceso a un oráculo $Enc_k(.)$ de uso libre. El adversario selecciona dos mensajes m_1 y m_2 y los entrega al verificador.
3. El verificador genera $b \in \{0,1\}$ de forma uniforme y le retorna $Enc_k(m_b)$ al adversario.
4. El adversario sigue teniendo acceso a su oráculo $Enc_k(.)$ y retorna $b' \in \{0,1\}$
5. Si $b = b'$ el adversario gana, en caso contrario el adversario pierde.

Definición CPA-Secure

Un esquema de encriptación Π se dice CPA-Secure si para todo adversario polinomial A:

$$P(A \text{ gana CPA-IE}_{\Pi,n}) \leq \frac{1}{2} + negl(n)$$

Función Pseudo Random

Se define Func_n como el conjunto de todas las funciones existentes que mapean de $\{0,1\}^n$ a $\{0,1\}^n$, es decir:

$$\text{Func}_n = \{f \quad | \quad f : \{0,1\}^n \longrightarrow \{0,1\}^n\}$$

Sea F una función de 2 variables, es decir $F : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n$. La primera variable de F es considerada una llave k, tal que $F(k,x) = F_k(x)$. Se dice que F es una función pseudo random si es que F_k (para un k elegido de manera uniforme) es indistinguible de una función $f \in \text{Func}_n$ elegida de forma uniforme desde Func_n, es decir, no existe un adversario eficiente que pueda distinguir si está interactuando con F_k o con f.

Preguntas

1. Demuestre que cualquier sistema de encriptación determinista no es CPA-Secure.
2. Construya un *template* básico de un sistema de encriptación randomizado utilizando la noción de función pseudo random y demuestre que un sistema con tales características es CPA-Secure.