*Profesor:* Alejandro Hevia
*Auxiliar:* Bryan Ortiz
*Ayudante:* David Contreras

CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE CHILE

# Tarea 2

*Encriptación Simétrica*

Fecha de Entrega: lunes 7 de octubre, 2024

**P1.** Sea $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ una familia de permutaciones PRF segura. Definimos un esquema de encriptación $H = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ que encripta mensajes de largo $\frac{n}{2}$ como sigue:

$$\mathsf{Enc}_K(M) : \left\{ R \xleftarrow{\$} \{0,1\}^{\frac{n}{2}}; \quad C \leftarrow F_K(R \| M); \quad \textbf{return } C \right\}$$

*a*) Entregue el algoritmo de desencriptación $\mathsf{Dec}_K(C)$.

*b*) Demuestre que si $F$ es PRF (segura) entonces $H$ es IND-CPA (segura).

**P2.** Sea $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ un esquema de encriptación simétrico. Definimos una nueva noción de securidad llamada REPCTXT. Intuitivamente, esta noción de seguridad busca asegurar que es "difícil" que un esquema de encriptación produzca dos veces el mismo texto cifrado.

Si $A$ un adversario REPCTXT para $\mathcal{SE}$, entonces participa en el siguiente juego:

Juego $\mathsf{REPCTXT}^A_{\mathcal{SE}}$:

```
PROC Inicializar:
    K ←$ 𝒦
    S ← ∅
    win ← false

PROC Finalizar():
    return win
```

```
PROC Enc(M):
    C ←$ E_K(M)
    if C ∈ S then
        win ← true
    S ← S ∪ {C}
    return C
```

Definimos la *ventaja REPCTXT* de un adversario $A$ como:

$$\mathbf{Adv}^{\mathsf{REPCTXT}}_{\mathcal{SE}}(A) = Pr[\mathsf{REPCTXT}^A_{\mathcal{SE}} \Rightarrow true]$$

El esquema de encriptación $\mathcal{SE}$ es REPCTXT seguro si todo $A$ razonable (ie: su tiempo $t$ y número de consultas $q$ son razonable) tiene una ventaja pequeña. Demuestre que si $\mathcal{SE}$ es IND-CPA seguro, entonces $\mathcal{SE}$ es REPCTXT seguro. Recuerde expresarlo como una relación entre las ventajas de adversarios en ambos experimentos. Indique los tiempos y número de preguntas de ambos adversarios.