Pontificia Universidad Católica de Chile
Departamento de Ciencia de la computación
IIC325 - Criptografia y Seguridad Computacional3

# Tarea 1

24 de abril de 2021

1º semestre 2021

José Manuel Domínguez - 17637449

---

## Pregunta 1

debemos demostrar que

$$\forall c_0 \in C, \forall m_1, m_2 \in M, \underset{k \leftarrow K}{Pr}[Enc(k, m_1) = c_0] = \underset{k \leftarrow K}{Pr}[Enc(k, m_2) = c_0]$$

si y solo si

$$\forall c_0 \in C, \forall m_0 \in M, \underset{\substack{k \leftarrow K \\ m \leftarrow M}}{Pr}[m = m_0 | Enc(k, m) = c_0] = \underset{m \leftarrow M}{Pr}[m = m_0]$$

Primero demostraremos hacia la izquierda. Dado:

$$\forall c_0 \in C, \forall m_0, m_1 \in M, \underset{k \leftarrow K}{Pr}[Enc(k, m_0) = c_0] = \underset{k \leftarrow K}{Pr}[Enc(k, m_1) = c_0]$$

PD:

$$\forall c_0 \in C, \forall m_0 \in M, \underset{\substack{k \leftarrow K \\ m \leftarrow M}}{Pr}[m = m_0 | Enc(k, m) = c_0] = \underset{m \leftarrow M}{Pr}[m = m_0]$$

Nota: voy a omitir los $k \leftarrow K$ y $m \leftarrow M$ por simplicidad :)

Por probabilidad conjunta tenemos que:

$$Pr[m = m_0 | Enc(k, m) = c_0] = \frac{Pr[m = m_0] \cap Pr[Enc(k, m) = c_0]}{Pr[Enc(k, m) = c_0]} = \frac{Pr[m = m_0] Pr[Enc(k, m_0) = c_0]}{Pr[Enc(k, m) = c_0]}$$

Ahora hay que probar que:

$$\frac{Pr[Enc(k, m_0) = c_0]}{Pr[Enc(k, m) = c_0]} = 1$$

que es lo mismo que:

$$Pr[Enc(k, m_0) = c_0] = Pr[Enc(k, m) = c_0]$$

Por definición:

$$Pr[Enc(k, m) = c_0] = \sum_{m_1 \in M} Pr[m = m_1] Pr[Enc(k, m_1) = c_0]$$

Dado el supuesto inicial esto nos queda:

$$Pr[Enc(k, m) = c_0] = \sum_{m_1 \in M} Pr[m = m_1] Pr[Enc(k, m_0) = c_0]$$

el termino $Pr[Enc(k, m_0) = c_0]$ se puede sacar de la sumatoria lo que nos deja:

$$Pr[Enc(k, m) = c_0] = Pr[Enc(k, m_0) = c_0] \sum_{m_1 \in M} Pr[m = m_1]$$

por último, $\sum_{m_1 \in M} Pr[m = m_1] = 1$

$$Pr[Enc(k, m) = c_0] = Pr[Enc(k, m_0) = c_0]$$

Con esto queda demostrado que:

$$\forall c_0 \in C, \forall m_0 \in M, \underset{\substack{k \leftarrow K \\ m \leftarrow M}}{Pr}[m = m_0 | Enc(k, m) = c_0] = \underset{m \leftarrow M}{Pr}[m = m_0]$$

Ahora para el lado derecho:

Dado:

$$\forall c_0 \in C, \forall m_0 \in M, \underset{\substack{k \leftarrow K \\ m \leftarrow M}}{Pr}[m = m_0 | Enc(k, m) = c_0] = \underset{m \leftarrow M}{Pr}[m = m_0]$$

PD:

$$\forall c_0 \in C, \forall m_0, m_1 \in M, \underset{k \leftarrow K}{Pr}[Enc(k, m_0) = c_0] = \underset{k \leftarrow K}{Pr}[Enc(k, m_1) = c_0]$$

Supongamos que hay solo 2 mensajes $m_0$ y $m_1$. Esto nos dice que:

$$Pr[m = m_0] = Pr[m = m_1] = \frac{1}{2}$$

Dado lo inicial:

$$Pr[m = m_0|Enc(k, m) = c_0] = Pr[m = m_1|Enc(k, m) = c_0]$$

Por probabilidad conjunta tenemos que:

$$Pr[m = m_0|Enc(k, m) = c_0] = \frac{Pr[m = m_0] \cap Pr[Enc(k, m) = c_0]}{Pr[Enc(k, m) = c_0]} = \frac{Pr[m = m_0]Pr[Enc(k, m_0) = c_0]}{Pr[Enc(k, m) = c_0]}$$

$$\frac{\frac{1}{2}Pr[Enc(k, m_0) = c_0]}{Pr[Enc(k, m) = c_0]}$$

De la misma forma

$$\frac{\frac{1}{2}Pr[Enc(k, m_1) = c_0]}{Pr[Enc(k, m) = c_0]}$$

Esto nos deja con:

$$\frac{\frac{1}{2}Pr[Enc(k, m_0) = c_0]}{Pr[Enc(k, m) = c_0]} = \frac{\frac{1}{2}Pr[Enc(k, m_1) = c_0]}{Pr[Enc(k, m) = c_0]}$$

Cancelamos $\frac{1}{2}$ y $Pr[Enc(k, m) = c_0]$ a ambos lados y nos deja que:

$$Pr[Enc(k, m_0) = c_0] = Pr[Enc(k, m_1) = c_0]$$

Con esto queda demostrado que

$$\forall c_0 \in C, \forall m_1, m_2 \in M, \underset{k \leftarrow K}{Pr}[Enc(k, m_1) = c_0] = \underset{k \leftarrow K}{Pr}[Enc(k, m_2) = c_0]$$

si y solo si

$$\forall c_0 \in C, \forall m_0 \in M, \underset{\substack{k \leftarrow K \\ m \leftarrow M}}{Pr}[m = m_0|Enc(k, m) = c_0] = \underset{m \leftarrow M}{Pr}[m = m_0]$$