

Tarea 1

Pregunta 1

Por Demostrar:

$$\forall c_0 \in C, \forall m_1, m_2 \in M, Pr_{k \leftarrow K}[Enc(k, m_1) = c_0] = Pr_{k \leftarrow K}[Enc(k, m_2) = c_0] \quad (1)$$

$$\Leftrightarrow$$

$$\forall c_0 \in C, \forall m_0 \in M, Pr_{k \leftarrow K, m \leftarrow M}[m = m_0 | Enc(k, m) = c_0] = Pr_{m \leftarrow M}[m = m_0] \quad (2)$$

Solución:

(\Rightarrow) **Por Contra-positivo:** Asumimos que (2) no se cumple, por lo tanto, los eventos $m = m_0$ y $Enc(k, m) = c_0$ son dependientes.

Sean $m_1, m_2 \in M$ y $c_0 \in C$, tenemos que:

$$Pr_{m \leftarrow M}[m = m_1] = Pr_{m \leftarrow M}[m = m_2] \quad (3)$$

$$Pr_{k \leftarrow K, m \leftarrow M}[m = m_1 | Enc(k, m) = c_0] \neq Pr[m = m_1] \quad (4)$$

$$Pr_{k \leftarrow K, m \leftarrow M}[m = m_2 | Enc(k, m) = c_0] \neq Pr[m = m_2] \quad (5)$$

de (3), (4) y (5) concluimos que:

$$Pr_{k \leftarrow K, m \leftarrow M}[m = m_1 | Enc(k, m) = c_0] \neq Pr_{k \leftarrow K, m \leftarrow M}[m = m_2 | Enc(k, m) = c_0] \quad (6)$$

Además podemos escribir las probabilidades de (6) como:

$$Pr_{k \leftarrow K, m \leftarrow M}[m = m_1 | Enc(k, m) = c_0] = \frac{Pr_{k \leftarrow K}[Enc(k, m) = c_0 | m = m_1] Pr[m = m_1]}{Pr_{k \leftarrow K, m \leftarrow M}[Enc(k, m) = c_0]} \quad (7)$$

$$Pr_{k \leftarrow K, m \leftarrow M}[m = m_2 | Enc(k, m) = c_0] = \frac{Pr_{k \leftarrow K}[Enc(k, m) = c_0 | m = m_2] Pr[m = m_2]}{Pr_{k \leftarrow K, m \leftarrow M}[Enc(k, m) = c_0]} \quad (8)$$

Reemplazando (7) y (8) en (6):

$$\frac{Pr_{k \leftarrow K}[Enc(k, m) = c_0 | m = m_1] Pr[m = m_1]}{Pr_{k \leftarrow K, m \leftarrow M}[Enc(k, m) = c_0]} \neq \frac{Pr_{k \leftarrow K}[Enc(k, m) = c_0 | m = m_2] Pr[m = m_2]}{Pr_{k \leftarrow K, m \leftarrow M}[Enc(k, m) = c_0]}$$

Simplificando:

$$Pr_{k \leftarrow K}[Enc(k, m) = c_0 | m = m_1] \neq Pr_{k \leftarrow K}[Enc(k, m) = c_0 | m = m_2]$$

$$Pr_{k \leftarrow K}[Enc(k, m_1) = c_0] \neq Pr_{k \leftarrow K}[Enc(k, m_2) = c_0]$$

Llegamos a que si (2) no se cumple, entonces (1) no se cumple, por lo tanto, (1) \Rightarrow (2)

(\Leftarrow) **Por demostración directa:** Asumimos que (2) se cumple, por lo tanto, los eventos $m = m_0$ y $Enc(k, m) = c_0$ son independientes.

Sean $m_1, m_2 \in M$ y $c_0 \in C$, tenemos que:

$$Pr_{m \leftarrow M}[m = m_1] = Pr_{m \leftarrow M}[m = m_2] \quad (9)$$

Por lo tanto, de (2) y (9) concluimos que :

$$Pr_{k \leftarrow K, m \leftarrow M}[m = m_1 | Enc(k, m) = c_0] = Pr_{k \leftarrow K, m \leftarrow M}[m = m_2 | Enc(k, m) = c_0] \quad (10)$$

Reemplazando con (7) y (8):

$$\frac{Pr_{k \leftarrow K}[Enc(k, m) = c_0 | m = m_1] Pr[m = m_1]}{Pr_{k \leftarrow K, m \leftarrow M}[Enc(k, m) = c_0]} = \frac{Pr_{k \leftarrow K}[Enc(k, m) = c_0 | m = m_2] Pr[m = m_2]}{Pr_{k \leftarrow K, m \leftarrow M}[Enc(k, m) = c_0]}$$

Simplificando:

$$Pr_{k \leftarrow K}[Enc(k, m) = c_0 | m = m_1] = Pr_{k \leftarrow K}[Enc(k, m) = c_0 | m = m_2]$$

$$Pr_{k \leftarrow K}[Enc(k, m_1) = c_0] = Pr_{k \leftarrow K}[Enc(k, m_2) = c_0]$$