① Se demuestra en ambas direcciones:

Partimos con (1) → (2)

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

A la vez:

$$\Pr[Enc(K, m) = c_0] = \sum_{m'' \in M} \Pr[m = m''] \cdot \Pr[Enc(K, m'') = c_0]$$

Por (1):

$$\Pr[Enc(K, m) = c_0] = \sum_{m'' \in M} \Pr[m = m''] \cdot \Pr[Enc(K, m') = c_0]$$

$$\Pr[Enc(K, m) = c_0] = \Pr[Enc(K, m') = c_0] \cdot \sum_{m'' \in M} \Pr[m'', m''] \quad (1)$$

Luego:

Considerando $\Pr[m = m_1] = \Pr[m = m_2]$ (Prob. conforme)

$$\Pr[m = m_1] \cdot \Pr[Enc(K, m_1) = c_0] = \Pr[m = m_2] \cdot \Pr[Enc(K, m_2) = c_0]$$

Dividiendo por $P(Enc(K, m) = c_0)$ y sustituyendo:

$$\frac{\Pr[m = m_1] \cdot \Pr[Enc(K, m_1) = c_0]}{\Pr[Enc(K, m) = c_0]} = \frac{\Pr[m = m_2] \cdot \Pr[Enc(K, m_2) = c_0]}{\Pr[Enc(K, m) = c_0]}$$

$$\frac{\Pr[m = m_1] \cap \Pr[Enc(K, m) = c_0]}{\Pr[Enc(K, m) = c_0]} = \frac{\Pr[m = m_2] \cdot \Pr[Enc(K, m) = c_0]}{\Pr[Enc(K, m) = c_0]}$$

~~$\Pr[m = m_1]$~~.

$$\Pr[m = m_1 \mid Enc(K, m) = c_0] = \Pr[m = m_2] = \Pr[m = m_1]$$

Lo que analogando para m_0:

$$\Pr[m = m_0 / Enc(K, m) = c_0] = \Pr[M = m_0]$$

(1) Se demuestra en ambas direcciones.

1.1 (2) → (1)

PARTIMOS CON:

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

Entonces:

$$\frac{\Pr[m = m_0] \cap \Pr[Enc(k,m) = c_0]}{\Pr[Enc(k,m) = c_0]} = \Pr[m = m_0] \quad (3)$$

A LA VEZ:

$\Pr[m = m_1] = \Pr[m = m_2]$ y aplicando (2) y (3)

$$\frac{\Pr[m = m_1] \cap \Pr[Enc(k,m) = c_0]}{\Pr[Enc(k,m) = c_0]} = \frac{\Pr[m = m_2] \cap \Pr[Enc(k,m) = c_0]}{\Pr[Enc(k,m) = c_0]}$$

$$\frac{\Pr[m = m_1] \cdot \Pr[Enc(k,m_1) = c_0]}{\Pr[Enc(k,m) = c_0]} = \frac{\Pr[m = m_2] \cdot \Pr[Enc(k,m_2) = c_0]}{\Pr[Enc(k,m) = c_0]}$$

Debido a ∩ de m

Como se mencionó antes $\Pr[m = m_1] = \Pr[m = m_2]$ por lo que simplificando:

$$\Pr[Enc(k,m_1) = c_0] = \Pr[Enc(k,m_2) = c_0]$$

■