Criptografía - Tarea 1

Matías Correa
15634183

Pregunta 1

Se procede a demostrar la proposición en ambas direcciones.

$\longleftarrow$ Se asume $\Pr_{\substack{m\leftarrow M\\ k\leftarrow K}}(m=m_0 \mid Enc(m,k)=c_0) = \Pr_{m\leftarrow M}(m=m_0)$ (1)

Por el Teorema de Bayes, tenemos:

$$\Pr_{\substack{m\leftarrow M\\ k\leftarrow K}}(m=m_0 \mid Enc(m,k)=c_0) = \frac{\Pr_{\substack{m\leftarrow M\\ k\leftarrow K}}(Enc(m,k)=c_0 \mid m=m_0)\cdot \Pr_{m\leftarrow M}(m=m_0)}{\Pr_{\substack{m\leftarrow M\\ k\leftarrow K}}(Enc(m,k)=c_0)}$$

Por (1), los primer y último términos se cancelan:

$$\Pr_{\substack{m\leftarrow M\\ k\leftarrow K}}(Enc(m,k)=c_0) = \Pr_{\substack{m\leftarrow M\\ k\leftarrow K}}(Enc(m,k)=c_0 \mid m=m_0)$$

El término de la derecha equivale a $\Pr_{k\leftarrow K}(Enc(m_0,k)=c_0)$

Así: $\Pr_{k\leftarrow K}(Enc(m_0,k)=c_0) = \Pr_{\substack{m\leftarrow M\\ k\leftarrow K}}(Enc(m,k)=c_0)$

Y esa igualdad corresponde a la proposición por demostrar. //

$\Longrightarrow$ Ahora se asume que

$$\Pr_{k \leftarrow K}(Enc(m_1, k) = C_0) = \Pr_{k \leftarrow K}(Enc(m_2, k) = C_0) \quad (1)$$

Por demostrar:

$$\Pr_{\substack{k \leftarrow K \\ m \leftarrow M}}(m = m_0 \mid Enc(m, k) = C_0) = \Pr_{m \leftarrow M}(m = m_0)$$

Nuevamente, por Teorema de Bayes tenemos:

$$\Pr_{\substack{m \leftarrow M \\ k \leftarrow K}}(m = m_0 \mid Enc(m, k) = C_0) = \frac{\Pr(Enc(m, k) = C_0 \mid m = m_0) \cdot \Pr_{m \leftarrow M}(m = m_0)}{\Pr_{\substack{m \leftarrow M \\ k \leftarrow K}}(Enc(m, k) = C_0)} \quad (2)$$

Trivialmente, $\Pr_{\substack{m \leftarrow M \\ k \leftarrow K}}(Enc(m, k) = C_0 \mid m = m_0) = \Pr_{k \leftarrow K}(Enc(m_0, k) = C_0) \quad (3)$

Dado que (1) es válido para todo $m \in M$, el término (3) se cancela con su denominador en (2). Así:

$$\Pr_{\substack{m \leftarrow M \\ k \leftarrow K}}(m = m_0 \mid Enc(m, k) = C_0) = \Pr_{m \leftarrow M}(m = m_0)$$

Que es justamente el resultado por demostrar.

Q.E.D. //