Enunciado Pregunta 1

En clases se definió la noción de *perfect secrecy* bajo la intuición de que, si un atacante ve sólo un texto cifrado, para él todo par de textos planos debiesen ser equiprobables. Formalmente, si tenemos un sistema criptográfico cuya función de encriptación es *Enc* sobre espacios de llaves, mensajes, y textos cifrados M, K y C, respectivamente, entonces:

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

Consideremos ahora otra noción de seguridad basada en la siguiente intuición: Si un atacante piensa que Alice le puede enviar a Bob un mensaje m_0 con una cierta probabilidad, al ver pasar un texto cifrado c_0 dicha probabilidad no cambia. Esta noción la podemos formalizar utilizando probabilidades condicionales de la siguiente forma:

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

Demuestre que esta segunda noción es equivalente a la noción de *perfect secrecy* vista en clases, es decir que un sistema criptográfico satisface (1) si y sólo si satisface (2).

Solución Pregunta 1

(1) $\Rightarrow$ (2) Sean $c_0 \in C$, $m_0 \in M$ un texto cifrado y un texto plano arbitrarios, respectivamente. En la demostración de esta dirección va a ser útil la siguiente propiedad:

$$\begin{aligned}
\Pr_{\substack{k \leftarrow K \\ m \leftarrow M}}[Enc(k, m) = c_0] &= \sum_{m' \in M} \Pr_{\substack{k \leftarrow K \\ m \leftarrow M}}[Enc(k, m) = c_0 \mid m = m'] \cdot \Pr_{m \leftarrow M}[m = m'] \\
&= \sum_{m' \in M} \Pr_{k \leftarrow K}[Enc(k, m') = c_0] \cdot \Pr_{m \leftarrow M}[m = m'] \\
&= \sum_{m' \in M} \Pr_{k \leftarrow K}[Enc(k, m_0) = c_0] \cdot \Pr_{m \leftarrow M}[m = m'] \qquad \text{por (1)} \\
&= \Pr_{k \leftarrow K}[Enc(k, m_0) = c_0] \sum_{m' \in M} \Pr_{m \leftarrow M}[m = m'] \\
&= \Pr_{k \leftarrow K}[Enc(k, m_0) = c_0] \qquad (3)
\end{aligned}$$

Con esta propiedad podemos demostrar que la igualdad (1) es válida:

$$\begin{aligned}
\Pr_{\substack{k\leftarrow K\\ m\leftarrow M}}[m = m_0 \mid Enc(k,m) = c_0] &= \frac{\Pr_{\substack{k\leftarrow K\\ m\leftarrow M}}[m = m_0 \wedge Enc(k,m) = c_0]}{\Pr_{\substack{k\leftarrow K\\ m\leftarrow M}}[Enc(k,m) = c_0]} \\
&= \frac{\Pr_{\substack{k\leftarrow K\\ m\leftarrow M}}[m = m_0 \wedge Enc(k,m) = c_0]}{\Pr_{\substack{k\leftarrow K\\ m\leftarrow M}}[Enc(k,m) = c_0] \cdot \Pr_{m\leftarrow M}[m = m_0]} \cdot \Pr_{m\leftarrow M}[m = m_0] \\
&= \frac{\Pr_{\substack{k\leftarrow K\\ m\leftarrow M}}[Enc(k,m) = c_0 \mid m = m_0]}{\Pr_{\substack{k\leftarrow K\\ m\leftarrow M}}[Enc(k,m) = c_0]} \cdot \Pr_{m\leftarrow M}[m = m_0] \\
&= \frac{\Pr_{k\leftarrow K}[Enc(k,m_0) = c_0]}{\Pr_{\substack{k\leftarrow K\\ m\leftarrow M}}[Enc(k,m) = c_0]} \cdot \Pr_{m\leftarrow M}[m = m_0] \\
&= \frac{\Pr_{k\leftarrow K}[Enc(k,m_0) = c_0]}{\Pr_{k\leftarrow K}[Enc(k,m_0) = c_0]} \cdot \Pr_{m\leftarrow M}[m = m_0] \qquad \text{por (3)} \\
&= \Pr_{m\leftarrow M}[m = m_0]
\end{aligned}$$

Esto concluye la demostración de la primera dirección de la equivalencia.

(2) $\Rightarrow$ (1) Sean $c_0 \in C$, $m_1, m_2 \in M$ un texto cifrado y un par de textos plano arbitrarios, respectivamente. En primer lugar, tenemos que:

$$\begin{aligned}
\Pr_{k\leftarrow K}[Enc(k,m_1) = c_0] &= \Pr_{\substack{k\leftarrow K\\ m\leftarrow M}}[Enc(k,m) = c_0 \mid m = m_1] \\
&= \frac{\Pr_{\substack{k\leftarrow K\\ m\leftarrow M}}[Enc(k,m) = c_0 \wedge m = m_1]}{\Pr_{m\leftarrow M}[m = m_1]} \\
&= \frac{\Pr_{\substack{k\leftarrow K\\ m\leftarrow M}}[Enc(k,m) = c_0 \wedge m = m_1]}{\Pr_{m\leftarrow M}[m = m_1] \cdot \Pr_{\substack{k\leftarrow K\\ m\leftarrow M}}[Enc(k,m) = c_0]} \cdot \Pr_{\substack{k\leftarrow K\\ m\leftarrow M}}[Enc(k,m) = c_0] \\
&= \frac{\Pr_{\substack{k\leftarrow K\\ m\leftarrow M}}[m = m_1 \mid Enc(k,m) = c_0]}{\Pr_{m\leftarrow M}[m = m_1]} \cdot \Pr_{\substack{k\leftarrow K\\ m\leftarrow M}}[Enc(k,m) = c_0] \\
&= \frac{\Pr_{m\leftarrow M}[m = m_1]}{\Pr_{m\leftarrow M}[m = m_1]} \cdot \Pr_{\substack{k\leftarrow K\\ m\leftarrow M}}[Enc(k,m) = c_0] \qquad \text{por (2)} \\
&= \Pr_{\substack{k\leftarrow K\\ m\leftarrow M}}[Enc(k,m) = c_0] \qquad (4)
\end{aligned}$$

De la misma forma, podemos demostrar que:

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

De esta igualdad y (4) deducimos que:

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

Esto concluye la demostración de la segunda dirección de la equivalencia.