Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación
IIC3253 — Criptografía y Seguridad Computacional 2021-1

NOMBRE: Matías Duhalde

Tarea 4

1 Pregunta 1

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

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

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

Primero, dado que en la expresión $\Pr_{m \leftarrow M}[m = m_0]$ se elige un valor aleatoriamente de M, y por definición, $m_0 \in M$, entonces $\Pr_{m \leftarrow M}[m = m_0] > 0$. Además, en la expresión $\Pr_{\substack{k \leftarrow K \\ m \leftarrow M}}[Enc(k, m) = c_0]$, c_0 es extraído desde C, y el conjunto C corresponde aquellos c tales que $Enc(k, m) = c$, con $m \in M$ y $k \in K$, se deduce que $\Pr_{\substack{k \leftarrow K \\ m \leftarrow M}}[Enc(k, m) = c_0] > 0$.

Comenzando desde (2), tenemos que por teorema de Bayes:

$$\Pr_{\substack{k \leftarrow K \\ m \leftarrow M}}[m = m_0 | Enc(k, m) = c_0] = \Pr_{m \leftarrow M}[m = m_0] \quad / \cdot \frac{\Pr[Enc(k, m) = c_0]}{\Pr[m = m_0]}$$

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

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

A partir de (2) y esta última expresión, se puede desprender que el evento $m = m_0$ es independiente de $Enc(k, m) = c_0$, y viceversa. También, la expresión anterior es equivalente a lo siguiente:

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

Debido a que m_0 surge al elegir un mensaje m cualquiera dentro del espacio M de mensajes. Equivalentemente, para dos $m_1, m_2 \in M$ elegidos aleatoriamente por distribución uniforme y de manera independiente, se llega a lo siguiente:

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

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

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

Por lo tanto, se comprueba que si el sistema criptográfico satisface (2), entonces satisface (1).

Comenzando desde (1), se tiene que en la expresión se eligen m_1 y m_2 arbitrariamente desde M ($\forall m_1, m_2 \in M$). Así, se puede reescribir (1) como:

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

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

Sin pérdida de generalidad, dado que m_1 es elegido de manera uniforme sobre todo el espacio M de mensajes, la expresión anterior se puede generalizar a lo siguiente:

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

Por Bayes:

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

Finalmente, se comprueba que el sistema criptográfico satisface (1) si y sólo si satisface también (2).