PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

IIC3253 - Criptografía y Seguridad Computacional
1er semestre del 2021
Vicente Merino

Tarea 1

Parte 1

Debemos mostrar que un sistema criptográfco satsaface (1) si y sólo si, satisface (2).

(1) $\Rightarrow$ (2)

Suponga que un sistema criptográfico satisface (1), es decir, se cumple que:

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

Lo primero que haremos es tomar (y mirar) la siguiente probabilidad:

$$\underset{\substack{k \leftarrow K \\ m \leftarrow M}}{Pr}[m = m_0 \mid Enc(k, m) = c_0]$$

Por teorema de Bayes, sabemos que se cumpla la siguiente igualdad:

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

Para llegar a (2), necesitamos que se cumpla la siguiente relación:

$$\frac{\underset{\substack{k \leftarrow K \\ m \leftarrow M}}{Pr}[Enc(k, m) = c_0 \mid m = m_0]}{\underset{\substack{k \leftarrow K \\ m \leftarrow M}}{Pr}[Enc(k, m) = c_0]} = 1$$

O equivalentemente, que

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

Notar, que el lado izquierdo, reemplazamos m por m_0, ya que es el valor que tiene m en la condicional. Luego, independientemente del m que se elija al lado derecho, dado que sabemos que la relación (1) se cumple, la relación recién enunciada también es verdadera, y por consiguiente, tenemos que se cumple que:

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

Con esto demostramos que (1) $\Rightarrow$ (2).

(2)⇒ (1)

Suponga que un sistema criptográfico satisface (2), es decir, se cumple que:

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

Si miramos la probabilidad de la izquierda, podemos, por teorema de Bayes, establecer la siguiente relación:

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

Igualando ambas expresiones, se tiene que

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

Reduciendo la expresión, se llega a la relación:

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

Como m_0 se eligió de forma arbitraria, podemos establecer la equivalencia:

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

Si reemplazamos las variables condicionales, estas dos relaciones se reducen a:

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

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

Al igualar estas expresiones, tenemos que:

$$\forall c_0 \in C, \forall m_0, m_1 \in M, \quad \Pr_{k \leftarrow K}[Enc(k,m_0) = c_0] \quad = \Pr_{k \leftarrow K}[Enc(k,m_1) = c_0]$$

Con esto, entonces queda demostrado que se cumple (1), y con esto que (2) ⇒ (1)

Luego, queda demostrado que un sistema criptográfico cumple (1) si y sólo si, cumple (2).