Tarea 1 criptografía

José Lara Hinojosa

Mayo 2021

Pregunta 1

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

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

Para demostrar esta pregunta lo que haremos será ocupar el teorema de Bayes en (2) para escribirlo de una manera que se entienda la trivialidad que sucede entre (1) y (2).

$$\frac{P(\mathrm{Enc}(k, m) = c_0 \mid m = m_0) \cdot P(m = m_0)}{P(\mathrm{Enc}(k, m) = c_0)} = P(m = m_0)$$

$$P(\mathrm{Enc}(k, m) = c_0 \mid m = m_0) \cdot P(m = m_0) = P(\mathrm{Enc}(k, m) = c_0) \cdot P(m = m_0)$$

$$P_{k\leftarrow K}(\mathrm{Enc}(k, m) = c_0 \mid m = m_0) = P_{\substack{k\leftarrow K \\ m\leftarrow M}}\left(\mathrm{Enc}(k, m) = c_0\right) \tag{3}$$

De esta ultima expresión obtenida de (2) notamos algo interesante, la probabilidad de que $\mathrm{Enc}(k, m) = c_0$ dado que $m = m_0$ es igual a la probabilidad de que la encriptación de cualquier llave o mensaje me de c_0, en particular, esto nos dice que si tengo $c_0 \in C, m_1, m_2 \in M$ arbitrarios entonces la probabilidad de que una encriptación con alguna llave y m_1 me de c_0 es la misma que para cualquier otro mensaje, en particular m_2.

Demostración formal

(1) $\implies$ (2):
Lo haremos por contradicción, asumiremos que (2) es falso y (1) es verdadero.
Tomemos c_0 arbitrario para esta demostración, como (2) es falso entonces sabemos que existe m_0 tal que

$$P_{k\leftarrow K}(\mathrm{Enc}(k, m) = c_0 \mid m = m_0) \neq P_{\substack{k\leftarrow K \\ m\leftarrow M}}\left(\mathrm{Enc}(k, m) = c_0\right)$$

, luego por (1) tenemos que para todo par de mensajes m_1 y m_2 en M con c_0 dado se cumple que

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

por lo tanto, todo par de mensajes debe cumplir esto, en particular m_0 junto a m_1, sin embargo, esto es una contradicción, ya que como (2) es falso implica que m_0 tiene una probabilidad distinta a los demás.

$$\Pr_{k\leftarrow K}\left[\mathrm{Enc}\left(k, m_0\right) = c_0\right] \neq \Pr_{k\leftarrow K}\left[\mathrm{Enc}\left(k, m_1\right) = c_0\right]$$

(2) $\Longrightarrow$ (1):
Al igual que en la demostración anterior lo haremos por contradicción, asumiremos (1) falso y (2) verdadero. Tomemos c_0 arbitrario para esta demostración, como (1) es falso sabemos que existe un par de mensajes m_1 y m_2 que no cumplen con que la probabilidad de que su encriptación sea igual a c_0 con cualquier llave sea igual, y de (2) sabemos que para todo mensaje dado este tiene que tener la misma probabilidad que los demás mensajes, en particular, para m_1 y m_2 debe cumplirse que

$$P_{k\leftarrow K}(\mathrm{Enc}(k, m) = c_0 \mid m = m_1) = P_{k\leftarrow K}(\mathrm{Enc}(k, m) = c_0 \mid m = m_2) = P_{\substack{k\leftarrow K \\ m\leftarrow M}}(\mathrm{Enc}(k, m) = c_0)$$

Sin embargo esto contradice que (1) sea falso, ya que la probabilidad de encriptación que tiene m_1 y m_2 es diferente.