Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencias de la Computación

IIC3253 - Criptografía y Seguridad Computacional

Sebasthian von Bergen (15635635)

Tarea 1 – Respuesta Pregunta 1

Perfect secrecy se puede definir como:

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

Queremos demostrar que esto es equivalente a decir:

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

Elijamos un m_1 tal que:

$$Enc(k, m_1) = c_0$$

Por el la ecuacion (2), podemos decir que:

$$Pr[m = m_1 | Enc(k, m_1) = c_0] = Pr[m = m_1] \ (3)$$

Por teorema de bayes

$$\frac{Pr[Enc(k, m1) = c_0]}{Pr[Enc(k, m_1) = c_0 | m = m_1]} = \frac{Pr[m = m_1]}{Pr[m = m_1 | Enc(k, m_1) = c_0]}$$

Podemos simplificar el lado derecho de la ecuacion, con (3).

$$\frac{Pr[Enc(k, m1) = c_0]}{Pr[Enc(k, m_1) = c_0 | m = m_1]} = 1$$
$$Pr[Enc(k, m_1) = c_0] = Pr[Enc(k, m_1) = c_0 | m = m_1]$$

Esto implica que la probabilidad de ver un texto cifrado c_0 no depende del mensaje elegido. Entonces eligiendo otro mensaje cualquiera m_2:

$$Pr[Enc(k, m_1) = c_0] = Pr[Enc(k, m_2) = c_0]$$

Lo que nos lleva a la afirmacion de perfect secrecy.