Criptografía y Seguridad Computacional - IIC3253
Tarea 1
Solución pregunta 2

Sea $\ell > 0$ un número entero, sea $\mathcal{M}$ el siguiente espacio de mensajes:

$$\mathcal{M} \quad = \quad \{\varepsilon\} \cup \{0,1\} \cup \{0,1\}^2 \cup \{0,1\}^3 \cup \cdots \cup \{0,1\}^\ell,$$

donde ε es la palabra vacía, y sea $\mathcal{K} = \{0,1\}^{\ell+1}$. Defina un espacio de textos cifrados $\mathcal{C}$ que sea subconjunto de $\{0,1\}^*$, y un esquema criptográfico (Gen, Enc, Dec) sobre $\mathcal{K}$, $\mathcal{M}$ y $\mathcal{C}$ que sea perfectamente secreto.

Nota: En la definición de (Gen, Enc, Dec) debe suponer que Gen es la distribución uniforme sobre $\mathcal{K}$.

Solución. Dado $m \in \mathcal{M}$, definimos una función $f : \mathcal{M} \to \{0,1\}^{\ell+1}$ de la siguiente forma. Para cada $m \in \mathcal{M}$, se tiene que

$$f(m) \quad = \quad m10^{\ell-|m|}.$$

Vale decir, $f(m)$ es construido agregando a m un símbolo 1 seguido de $(\ell - |m|)$ símbolos 0. Nótese que f es una función inyectiva. Formalmente, dados $m_1, m_2 \in \mathcal{M}$ tales que $m_1 \neq m_2$, tenemos que $f(m_1) \neq f(m_2)$ por los siguientes casos.

- Si $|m_1| = |m_2| = k$, entonces $f(m_1)$ difiere de $f(m_2)$ en alguno de los primeros k símbolos, puesto que m_1 es prefijo de $f(m_1)$ y m_2 es prefijo de $f(m_2)$.
- Si $|m_1| < |m_2|$, entonces $f(m_1)$ defiere de $f(m_2)$ ya que $f(m_2)$ tiene un símbolo 1 en la posición $|m_2| + 1$, mientras que $f(m_1)$ tiene un símbolo 0 en la posición $|m_2| + 1$.
- Si $|m_2| < |m_1|$, entonces se concluye que $f(m_1)$ defiere de $f(m_2)$ como en el caso anterior.

Como f es una función inyectiva, denotamos como f^{-1} a su inversa.

Sea $\mathcal{C} = \{f(m) \mid m \in \mathcal{M}\}$, y defina las familias Enc y Dec de la siguiente forma. Dado $k \in \mathcal{K}$, se tiene que:

- para cada $m \in \mathcal{M}$: $Enc_k(m) = f(m) \oplus k$, y
- para cada $c \in \mathcal{C}$: $Dec_k(m) = f^{-1}(c \oplus k)$.

Nótese que para cada $k \in \mathcal{K}$ y $m \in \mathcal{M}$:

$$\begin{aligned} Dec_k(Enc_k(m)) &= Dec_k(f(m) \oplus k) \\ &= f^{-1}((f(m) \oplus k) \oplus k) \\ &= f^{-1}(f(m) \oplus (k \oplus k)) \\ &= f^{-1}(f(m) \oplus 0^{\ell+1}) \\ &= f^{-1}(f(m)) \\ &= m \end{aligned}$$

Por lo tanto el esquema criptográfico (Gen, Enc, Dec) está bien definido, y para terminar la pregunta sólo tenemos que demostrar que es perfectamente secreto. Vale decir, tenemos que demostrar que se cumple la siguiente propiedad, dada una distribución de probabilidades $\mathbb{D}$ para los mensajes en $\mathcal{M}$:

$$\forall m_0 \in \mathcal{M} : \quad \Pr_{\substack{m \sim \mathbb{D} \\ k \sim Gen}} [m = m_0 \mid Enc_k(m) = c_0] \quad = \quad \Pr_{m \sim \mathbb{D}}[m = m_0].$$

La demostración de que esta propiedad se cumple se puede hacer de la misma forma que como se hizo en clases para el caso de OTP. En particular, se debe considerar que Gen es la distribución uniforme sobre $\mathcal{K}$, y para todo $m \in \mathcal{M}$ y $c \in \mathcal{C}$ existe un único k tal que $Enc_k(m) = c$, por lo que se tiene que:

$$\sum_{k \in \mathcal{K} \,:\, Enc_k(m) = c} Gen(k) \quad = \quad \frac{1}{2^{\ell+1}}.$$