# IIC3253: Criptografía y Seguridad Computacional - Tarea #1

Raimundo Herrera - rjherrera@uc.cl

2 de abril de 2018

## Problema 1

1. **Argumente si esta modificación es una buena o mala idea.**

   Esta modificación a primera vista pareciera ser una buena idea ya que evita entregar el mensaje idéntico al adversario, sin embargo, es una mala idea porque al eliminar la llave $0^n$, el adversario sabe a priori que el mensaje que le llegó **no** es el mensaje que se envió. De esta manera se le entrega más información al adversario, lo que es una mala idea.

   Desde el punto de vista de cuán secreto es el esquema, como se demostrará en la parte 2 de esta pregunta, es también una mala idea porque el esquema deja de ser secreto al eliminar dicha llave.

   Por último, si se siguiera la lógica de eliminar ciertas llaves, se podría eliminar por ejemplo la llave $1^n$ y otras llaves ya que para cada llave puede existir un argumento de que la llave modifica el mensaje de una manera muy obvia, pero esta lógica flaquea y entrega más información al adversario.

2. **¿Es el esquema resultante perfectamente secreto? Demuestre su respuesta.**

   El esquema resultante no es perfectamente secreto. Por el teorema visto en clases, un esquema es perfectamente secreto si y solo si el tamaño del espacio de mensajes es menor o igual al tamaño del espacio de llaves, esto es:

   $$|M| \leq |K|$$

   Donde $M$ y $K$ para One Time Pad son iguales a $\{0,1\}^n$.

   De este modo, en el esquema propuesto, al eliminar la llave $0^n$ el espacio de las llaves se reduce en un elemento, por lo que el tamaño de $K'$, correspondiente al espacio de llaves de este esquema es

   $$|K'| = |K| - 1$$

Y al mantenerse el espacio de mensajes inalterado, resulta que

$$|M| > |K'|$$

Por lo tanto no se cumple lo encunciado por el teorema, quedando demostrado que el esquema no es perfectamente secreto.

■

# Problema 2

1. **Demuestre que no existe un esquema de cifrado que sea seguro bajo la definición anterior.**

   Por construcción del esquema, sabemos que $c = c'$ implica que $m = m'$, ya que de otro modo, no se podría desencriptar un mensaje. El problema es que la igualdad de probabilidades propuesta, no excluye el caso en el que $c = c'$ y $m \neq m'$.

   De este modo, si tomamos $m, m' \in \mathcal{M}$ tales que $m \neq m'$ y $\Pr[M = m] > 0$ y $\Pr[M' = m'] > 0$, y tomamos $c, c' \in \mathcal{C}$ tal que $c = c'$ y $\Pr[C = c] > 0$, se tiene que

   $$\Pr[M = m \wedge M' = m'] \neq \Pr[M = m \wedge M' = m' | C = c \wedge C' = c']$$

   Ya que el lado izquierdo tiene una probabilidad mayor que 0 de ocurrir porque $m$ y $m'$ fueron extraidos independientemente con probabilidad mayor que 0. Y el lado derecho es igual a 0, esto porque con $m' \neq m$, no hay ninguna forma de que $c' = c$, caso del que partimos.

   Por lo tanto no existe esquema que satisfaga dicha definición.

2. **Proponga una modificación a la definición anterior tal que el resultado negativo de 1) sea inefectivo en la nueva definición.**

   La modificación consiste en excluir el caso en que eso ocurre, de modo que la definición queda:

   Un esquema es perfectamente secreto para 2 mensajes si $\forall m, m' \in \mathcal{M}$ con $m \neq m'$ y $\forall c, c' \in \mathcal{C}$ con $c \neq c'$ tales que $\Pr[C = c \wedge C' = c'] > 0$, se tiene que

   $$\Pr[M = m \wedge M' = m' | M \neq M'] = \Pr[M = m \wedge M' = m' | C = c \wedge C' = c']$$

   Notar que no se considera el caso en que $\Pr[M = m] = 0$ porque sino no se satisface ninguna definición.

3. **Proponga un esquema que satisfaga la definición en 2). Este esquema no puede mantener estado. Es decir, el "código" que se ejecuta es exactamente el mismo para cifrar ambos mensajes.**

   Para proponer el esquema, primero tomemos $\mathcal{K}$ como todas las permutaciones en $\mathcal{M}$, considerando que se entiende permutacion como biyeccion en el mismo conjunto, esto es, que cada $\pi \in \mathcal{K}$ corresponde a una biyección de $\mathcal{M} \to \mathcal{M}$.

   El esquema entonces es:

   - `Gen`: Elegir $\pi \xleftarrow{\$} \mathcal{K}$, retornar $\pi$. (Elección uniforme de $\pi$).
   - $Enc_\pi(m)$ : Output de $\pi(m) = c$

- $Dec_\pi(c)$ : Output de $\pi^{-1}(c) = m$

Ahora, solo falta demostrar que dicho esquema propuesto realmente satisface la definición, es decir

$$\Pr[M = m \wedge M' = m' | M \neq M'] = \Pr[M = m \wedge M' = m' | C = c \wedge C' = c']$$

De este modo, partiendo por el lado derecho, se tiene que, por probabilidades condicionales y algebra

$$\Pr[M = m \wedge M' = m' | C = c \wedge C' = c'] = \frac{\Pr[C = c \wedge C' = c' | M = m \wedge M' = m'] \cdot \Pr[M = m \wedge M' = m']}{\Pr[C = c \wedge C' = c']}$$

Llamemos (1) al primer factor del numerador, $\Pr[C = c \wedge C' = c' | M = m \wedge M' = m']$ y (2) al denominador $\Pr[C = c \wedge C' = c']$.

Desarrollando (1) se tiene que descondicionando al aplicar $\pi(x)$ sobre $m$ y $m'$,

$$\Pr[C = c \wedge C' = c' | M = m \wedge M' = m'] = \Pr[\pi(m) = c \wedge \pi(m') = c']$$

con $\pi$ proveniente del generador sobre $\mathcal{K}$. Ahora aplicando probabilidades condiconales sobre lo último se tiene que

$$\Pr[\pi(m) = c \wedge \pi(m') = c'] = \Pr[\pi(m) = c] \cdot \Pr[\pi(m') = c' | \pi(m) = c]$$

Así, el factor de la izquierda corresponde a $\frac{1}{|M|}$ ya que $\pi$ corresponde a una biyección sobre $M$, por lo que es uniforme en el tamaño de ese espacio. De la misma manera, el factor de la derecha, corresponde a una elección sobre un espacio análogo, pero como $m \neq m'$, entonces la probabilidad es $\frac{1}{|M|-1}$. Por lo que

$$\Pr[\pi(m) = c] \cdot \Pr[\pi(m') = c' | \pi(m) = c] = \frac{1}{|M|} \cdot \frac{1}{|M| - 1}$$

Siguiendo, ahora tomando (2), se tiene que

$$\Pr[C = c \wedge C' = c'] = \Pr[\pi(M) = c \wedge \pi(M') = c']$$

Lo que, como usualmente hacemos, sumando sobre $m$, se convierte en

$$\Pr[\pi(M) = c \wedge \pi(M') = c'] = \sum_{m,m'} \Pr[\pi(m) = c \wedge \pi(m') = c'] \cdot \Pr[M = m \wedge M' = m']$$

También sabemos que $m \neq m'$, por lo que la probabilidad anterior es igual a

$$= \sum_{m \neq m'} \Pr[\pi(m) = c \wedge \pi(m') = c'] \cdot \Pr[M = m \wedge M' = m']$$

Como ya calculamos la primera probabilidad (el primer factor) y no depende de $m$ sino que del largo de $|M|$.

$$\Pr[C = c \wedge C' = c'] = \frac{1}{|M|} \cdot \frac{1}{|M| - 1} \cdot \sum_{m \neq m'} \Pr[M = m \wedge M' = m']$$

Y la suma del final es equivalente a $\Pr[M \neq M']$

Reemplazando en la fracción inicial, se tiene ahora que, llamemos (3) a esta expresión

$$\Pr[M = m \wedge M' = m' | C = c \wedge C' = c'] = \frac{\frac{1}{|M|} \cdot \frac{1}{|M|-1} \cdot \Pr[M = m \wedge M' = m']}{\frac{1}{|M|} \cdot \frac{1}{|M|-1} \cdot \Pr[M \neq M']}$$

Finalmente, la probabilidad del denominador que resta por resolver, se puede expresar como dos casos separados, el caso en que $M = M'$ y el caso en que $M \neq M'$.

$$\Pr[M = m \wedge M' = m'] = \Pr[M = m \wedge M' = m' \wedge M = M'] + \Pr[M = m \wedge M' = m' \wedge M \neq M']$$

Pero sabemos por la condición impuesta inicialmente que $M \neq M'$ entonces el primer término es 0. Así, descondicionando el segundo término, se tiene que

$$\begin{aligned} \Pr[M = m \wedge M' = m'] &= \Pr[M = m \wedge M' = m' \wedge M \neq M'] \\ &= \Pr[M = m \wedge M' = m' | M \neq M'] \cdot \Pr[M \neq M'] \end{aligned}$$

Volviendo a la expresión (3), se tiene que

$$\Pr[M = m \wedge M' = m' | C = c \wedge C' = c']$$

$$= \frac{\frac{1}{|M|} \cdot \frac{1}{|M|-1} \cdot \Pr[M = m \wedge M' = m' | M \neq M'] \cdot \Pr[M \neq M']}{\frac{1}{|M|} \cdot \frac{1}{|M|-1} \cdot \Pr[M \neq M']}$$

Y despejando los términos similares se tiene que

$$= \Pr[M = m \wedge M' = m' | M \neq M']$$

Por lo que se obtiene la expresión que se buscaba, determinando que este esquema satisface la definición.

# Problema 3

Justificar formalmente si los siguientes esquemas son perfectamente secretos.

1. **El espacio de textos planos es $\mathcal{M} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, el espacio de llaves es $\mathcal{K} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.**

   Se omiten los detalles del esquema para evitar repetición.

   Este esquema **no** es perfectamente secreto, notar que para que lo fuese, lo siguiente

   $$\Pr[M = m|C = c] = \Pr[M = m]$$

   Debe cumplirse para todo $m \in \mathcal{M}$, $c \in \mathcal{C}$ y distribución $\mathcal{D}_{\mathcal{M}}$. En particular, si tomamos el caso $m = 1$ y $c = 0$, se tiene lo siguiente

   $$\Pr[M = 1|C = 0] \stackrel{?}{=} \Pr[M = 1]$$

   Partiendo por el lado izquierdo, se tiene que $m = 1$ dado que $c = 0$ ocurre solamente cuando $k = 9$ ya que $0 = 1 + 9$ mód 10. Como $k$ puede tomar valores entre 0 y 10, para una misma configuración de $m$ y $c$, existen 11 posibilidades. De este modo, como solo una de ellas mapea a lo pedido, por lo visto anteriormente, se tiene que:

   $$\Pr[M = 1|C = 0] = \frac{1}{11}$$

   Por otro lado, como dicha definición debe funcionar para toda distribución, si tomamos la distribución uniforme para los mensajes, la probabilidad de que $m = 1$ sin condicionar, corresponde a $\frac{1}{10}$ ya que se puede elegir cualquiera dentro de las 10 posibilidades de $\mathcal{M}$. Así se tiene

   $$\Pr[M = 1|C = 0] \neq \Pr[M = 1] \text{ ya que } \frac{1}{11} \neq \frac{1}{10}$$

   Por lo que al no cumplirse lo enunciado anteriormente, no es un esquema perfectamente secreto.

2. **El espacio de llaves es $\mathcal{M} = \{m \in \{0, 1\}^n |$ los últimos $\ell$ bits de $m$ son 1$\}$, el espacio de llaves es $\mathcal{K} = \{0, 1\}^{n-\ell}$.**

   Se omiten los detalles del esquema para evitar repetición.

   Este esquema **sí** es perfectamente secreto, por lo que debe cumplirse, para todo $m \in \mathcal{M}$, $c \in \mathcal{C}$ y distribución $\mathcal{D}_{\mathcal{M}}$ que:

   $$\Pr[C = c|M = m] = \Pr[C = c]$$

De este modo, desarrollando el lado izquierdo, se tiene que

$$\begin{aligned}\Pr[C = c|M = m] &= \Pr[Enc(k, M) = c|M = m] \\ &= \Pr[Enc(k, m) = c] \\ &= \Pr[m \oplus (k||0^\ell) = c]\end{aligned}$$

Ahora, por construcción de $m$, sea $m'$ los primeros $n$ dígitos de $m$ tales que $m = m'||1^\ell$. De este modo

$$\Pr[C = c|M = m] = \Pr[(m'||1^\ell) \oplus (k||0^\ell) = c]$$

Ahora, por asociatividad del operador `xor`, y dado que $0^r \oplus 1^r = 1^r$ para todo $r > 0$, se tiene que

$$\Pr[C = c|M = m] = \Pr[(m' \oplus k)||1^\ell = c]$$

Entonces, como los $\ell$ últimos dígitos de $(m' \oplus k)||1^\ell$ están fijos, la probabilidad de $c$ no depende de ellos. Sea $c'$ los primeros $n$ dígitos de $c$ tales que $c = c'||1^\ell$. Se tiene entonces

$$\Pr[C = c|M = m] = \Pr[(m' \oplus k)||1^\ell = c'||1^\ell]$$

Pudiéndolo reducir finalmente a

$$\Pr[C = c|M = m] = \Pr[m' \oplus k = c']$$

Lo que, aplicando `xor` a ambos lados de la igualdad dentro de la probabilidad de la derecha queda equivalente a

$$\Pr[C = c|M = m] = \Pr[k = c' \oplus m']$$

Teniendo entonces que, como $\mathcal{K}$ distribuye uniforme

$$\Pr[C = c|M = m] = \frac{1}{2^n}$$

Por otra parte, desarrollando el lado derecho, se tiene que

$$\begin{aligned}\Pr[C = c] &= \Pr[Enc(k, M) = c] \\ &= \Pr[M \oplus (k||0^\ell) = c] \\ &= \sum_{m \in M} \Pr[M \oplus (k||0^\ell) = c|M = m] \cdot \Pr[M = m]\end{aligned}$$

el primer factor de la suma lo calculamos recién, y es $\frac{1}{2^n}$, quedando entonces

$$\begin{aligned}\Pr[C = c] &= \frac{1}{2^n} \sum_{m \in M} \Pr[M = m] \\ &= \frac{1}{2^n} \cdot 1 \\ &= \frac{1}{2^n}\end{aligned}$$

Por lo tanto como $\Pr[C = c|M = m] = \frac{1}{2^n}$ y $\Pr[C = c] = \frac{1}{2^n}$

$$\Pr[C = c|M = m] = \Pr[C = c]$$

se cumple lo enunciado y el esquema es perfectamente secreto.

# Problema 4

**Demuestre que si un esquema de encriptación simétrico es perfectamente secreto para alguna distribución de mensajes $\mathcal{D}^*_{\mathcal{M}}$, entonces también es perfectamente secreto para cualquier distribución $\mathcal{D}_{\mathcal{M}}$ sobre $\mathcal{M}$.**

Lo pedido corresponde a demostrar que dado que para alguna distribución $\mathcal{D}^*$,

$$\Pr_{M\sim\mathcal{D}^*}[C = c|M = m] = \Pr_{M\sim\mathcal{D}^*}[C = c]$$

entonces, para cualquier distribución $\mathcal{D}$,

$$\Pr_{M\sim\mathcal{D}}[C = c|M = m] = \Pr_{M\sim\mathcal{D}}[C = c]$$

En primer lugar, se tiene que $\Pr_{M\sim\mathcal{D}^*}[C = c|M = m]$ no depende de la distribución $\mathcal{D}^*$, por lo tanto se tiene que, para cualquier distribución $\mathcal{D}$

$$\Pr_{M\sim\mathcal{D}^*}[C = c|M = m] = \Pr_{M\sim\mathcal{D}}[C = c|M = m]$$

De este modo, lo que se debe demostrar $\Pr_{M\sim\mathcal{D}}[C = c|M = m] = \Pr_{M\sim\mathcal{D}}[C = c]$, se reduce a demostrar, por transitividad de la igualdad, que

$$\Pr_{M\sim\mathcal{D}^*}[C = c] = \Pr_{M\sim\mathcal{D}}[C = c]$$

Desarrollando el lado derecho de la igualdad anteriormente descrita, por probabilidades totales, se tiene que

$$\Pr_{M\sim\mathcal{D}}[C = c] = \sum_{m\in\mathcal{M}} \Pr_{M\sim\mathcal{D}}[C = c|M = m] \cdot \Pr_{M\sim\mathcal{D}}[M = m]$$

Pero como se dijo anteriormente, $\Pr_{M\sim\mathcal{D}^*}[C = c|M = m] = \Pr_{M\sim\mathcal{D}}[C = c|M = m]$, de modo que ahora se tiene

$$\Pr_{M\sim\mathcal{D}}[C = c] = \sum_{m\in\mathcal{M}} \Pr_{M\sim\mathcal{D}^*}[C = c|M = m] \cdot \Pr_{M\ \sim\mathcal{D}}[M = m]$$

Y como para $\mathcal{D}^*$ el esquema es perfectamente secreto, se tiene que $\Pr_{M\sim\mathcal{D}^*}[C = c|M = m] = \Pr_{M\sim\mathcal{D}^*}[C = c]$, de modo que lo anterior se reduce a

$$\Pr_{M\sim\mathcal{D}}[C = c] = \sum_{m\in\mathcal{M}} \Pr_{M\sim\mathcal{D}^*}[C = c] \cdot \Pr_{M\sim\mathcal{D}}[M = m]$$

Como el primer elemento de la suma, esto es $\Pr_{M\sim\mathcal{D}^*}[C = c]$, no depende de $m$, se puede sacar de la suma como un factor, quedando

$$\Pr_{M\sim\mathcal{D}}[C = c] = \Pr_{M\sim\mathcal{D}^*}[C = c] \sum_{m\in\mathcal{M}} \Pr_{M\sim\mathcal{D}}[M = m]$$

Y trivialmente la suma de la derecha corresponde a la suma de todo el espacio de probabilidades, por lo que es 1, teniendo entonces finalmente que

$$\Pr_{M\sim\mathcal{D}}[C = c] = \Pr_{M\sim\mathcal{D}^*}[C = c] \cdot 1$$

$$\Pr_{M\sim\mathcal{D}}[C = c] = \Pr_{M\sim\mathcal{D}^*}[C = c]$$

■