IIC3253: Criptografía y Seguridad Computacional **2018-01**

Tarea 1: 14/03/2018

Evaluación Escrita: 28/04/2018, Entrega Final: 02/04/2018

Reglas

Las tareas se pueden discutir de a 2 personas. Sin embargo, cada estudiante tiene la obligación de escribir su propia solución. La entrega final de la tarea se realiza mediante correo electronico firmado a `gnmonsalve@uc.cl` y con copia a `fekrell@uc.cl` con el asunto `[IIC3253] Entrega Tarea 1` a las 17:00 del día de la entrega. Cada estudiante sólo puede asumir que su tarea ha sido correctamente entregada si recibe un correo electrónico de respuesta correctamente firmado por algún miembro del cuerpo docente. Usted debe entregar un archivo pdf generado en LaTeX. Se sugiere utilizar el template publicado en la página web del curso. La evaluación aleatoria es obligatoria y se realizará en la clase del día Miercoles 28 de Marzo.

Notación

- $a \mod b$: módulo o resto de la división entera entre a y b (ambos enteros positivos).
- $\oplus$: XOR (o suma módulo 2) bit a bit.
- $||$: concatenación.
- $\xleftarrow{\$} S$ elección uniformemente aleatoria sobre el conjunto S.

Problema 1 (25pts)

Dado que $m \oplus 0^n = m$ para todo $m \in \{0,1\}^n$, se ha sugerido que 0^n sea eliminado como posible llave para el One-time Pad. Es decir, Gen entrega como salida un string uniformemente aleatorio en $\{0,1\}^n \setminus \{0^n\}$.

- **10pts** Argumente si esta modificación es una buena o mala idea.
- **15pts** ¿Es el esquema resultante perfectamente secreto? Demuestre su respuesta.

Problema 2 (25pts)

El OTP es inseguro si la misma llave es utilizada más de una vez. Sin embargo, el OTP es perfectamente secreto según la definición vista en clases. Considere la siguiente definición para 2 mensajes.

Definición 1. *Un esquema es* perfectamente secreto para 2 mensajes *si* $\forall m, m' \in \mathcal{M}\ \forall c, c' \in \mathcal{C}$*, tales que* $\Pr[C = c \wedge C' = c'] > 0$*,*

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

en donde tanto M *como* M' *se distribuyen independientemente en* $\mathcal{M}$ *y* C, C' *son variables aleatorias definidas como* $C = Enc(K, M)$ *y* $C' = \mathsf{Enc}(K, M')$ *para* $K \leftarrow \mathsf{Gen}$*.*

1. **10pts.** Demuestre que no existe un esquema de cifrado que sea seguro bajo la definición anterior.
2. **5pts.** Proponga una modificación a la definición anterior tal que el resultado negativo de 1) sea inefectivo en la nueva definición.
3. **10pts.** 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.

Problema 3 (25 pts)

Justificar formalmente si los siguientes esquemas son perfectamente secretos.

1. **13pts.** El espacio de textos planos es $\mathcal{M} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, el espacio de llaves es $\mathcal{K} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. El esquema es:
   - Gen: Elegir $k \xleftarrow{\$} \mathcal{K}$, retornar k. (Elección uniforme de la llave k).
   - $\mathsf{Enc}(k, m)$: Computar $c = m + k \mod 10$, retornar c.
   - $\mathsf{Dec}(k, c)$: Computar $m = c - k \mod 10$, retornar m.
2. **12pts.** El espacio de llaves es $\mathcal{M} = \{m \in \{0,1\}^n |$ los últimos ℓ bits de m son $1\}$, el espacio de llaves es $\mathcal{K} = \{0,1\}^{n-\ell}$. El esquema es:

- Gen: Elegir $k \xleftarrow{\$} \mathcal{K}$, retornar k.
- $\mathsf{Enc}(k, m)$: Computar $c = m \oplus (k||0^\ell)$, retornar c. .
- $\mathsf{Dec}(k, c)$: Computar $m = c \oplus (k||0^\ell)$, retornar m.

Problema 4 (25pts)

Sea $\mathcal{M}$ el espacio de textos planos para un esquema de encriptación simétrico $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$. Demuestre que si un esquema de encriptación simétrico es perfectamente secreto para *alguna* distribución de mensajes $D^*_{\mathcal{M}}$, entonces también es perfectamente secreto para cualquier distribución $D_{\mathcal{M}}$ sobre $\mathcal{M}$. Concluya relajando la definición vista en clases.