IIC3253: Criptografía y Seguridad Computacional **2017-01**

Tarea 1: 20/03/2017

Entrega: 04/04/2017

Reglas

Las tareas se pueden discutir de a 2 personas. Sin embargo, cada estudiante tiene la obligación de escribir su propia solución. La entrega 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 23:59 pm 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.

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.

Requisitos 0pts, pero OBLIGATORIO

Genere su par de llaves GPG utilizando RSA de al menos 2048 bits. Una vez generada su llave, envíe un correo al cuerpo docente con su llave pública. Lleve a la siguiente clase el *fingerprint* de su llave para que el profesor la verifique. Utilice *thunderbird* como administrador de correo e instale el plugin Enigmail para facilitar su uso. Para configurar su cuenta `@uc.cl`, el servidor IMAP es, puerto 143 y protolo STARTTLS. Para servidor de salida utilice smpt.uc.cl en el puerto 587 con protocolo STARTTLS.

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** Discuta si esta modificación es una buena idea.
- **15pts** ¿És el esquema resultante perfectamente secreto?. Demuestre su respuesta.

Problema 2 (25pts)

Hemos visto en clases que 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 satisfaga 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).

Problema 3 (25 pts)

Justificar formalmente si los siguientes esquemas son perfectamente secretos.

1. **13pts.** El espacio de llaves 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 $\mathcal{M} = \{m \in \{0,1\}^n |$ primer bit de m es $0\}$, el espacio de llaves es $\mathcal{K} = \{0,1\}^{n-1}$. El esquema es:

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

Problema 4 (25pts)

Sea $t \in N$, $t \geq 1$. Demuestre que si autorizamos $\Pr[\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m] \geq 2^{-t}$ *para todo* $m \in \mathcal{M}$ (en donde la probabilidad esta tomada sobre la elección aleatoria de la llave k y las decisiones aleatorias internas del algoritmo Enc), entonces es posible tener espacio de llaves menor al espacio de textos planos. Es decir, proponga un esquema perfectamente secreto en donde $\Pr[\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m] \geq 2^{-t}$ y $|\mathcal{K}| < |\mathcal{M}|$.

Extra (5 pts): Demuestre una cota inferior a $|\mathcal{K}|$ en función de t y el tamaño de $\mathcal{M}$. Hint: Suponga distribución uniforme sobre $\mathcal{M}$, y utilice definición de seguridad.