Criptografía y Seguridad Computacional **2016-01**

Tarea 1: 16/03/2016

Entrega: 30/03/2016

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 a `fkrell@gmail.com` con el asunto `[cripto] Entrega Tarea1` a más tardar el día 30 de marzo de 2016 a las 3:30 pm. Cada estudiante sólo puede asumir que su tarea ha sido correctamente entregada si recibe un email de respuesta. Usted debe entregar un archivo pdf generado en LaTeX.

Problema 1 (5pts)

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. Es decir, Gen arroja como salida un string uniformemente aleatorio en $\{0,1\}^n \setminus \{0^n\}$.

- **2pts** ¿Es esto una buena idea? Justifique su respuesta.
- **3pts** ¿Es el esquema resultante perfectamente secreto?. Demuestre su respuesta.

Problema 2 (5pts)

Proponga un esquema de cifrados para $\mathcal{M} = \{0,1,2,3,4,5,6,7,8,9\}$, y demuestre que este es perfectamente secreto.

Problema 3 (5pts)

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.

Demuestre que no existe un esquema de cifrado que satisfaga la siguiente definición.

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* $K \leftarrow \mathsf{Gen}$.

Hint: Considere el caso $c = c'$, pero $m \neq m'$.

Problema 4: Cifradores para múltiples mensajes (10pts)

Diremos que un esquema tiene cifrados indistinguibles para múltiples mensajes si

$$\Pr[\mathtt{Exp}^{\text{m-ind}}_{\mathcal{A},\Pi} = 1] \leq 1/2 + \mathtt{negl}(\lambda)$$

en donde `negl` es una función negligible y $\mathtt{Exp}^{\text{m-ind}}_{\Pi,\mathcal{A}}(\lambda)$ es definido como

$\mathsf{Exp}^{\textbf{m-ind}}_{\Pi,\mathcal{A}}(\lambda)$**:**

1. $k \leftarrow \mathsf{Gen}(1^\lambda)$
2. $\vec{M}_0, \vec{M}_1 \leftarrow \mathcal{A}(1^\lambda)$, en donde $\vec{M}_0 = \{m_0^1, m_0^2, ..., m_0^n\}$, $\vec{M}_1 = \{m_1^1, m_1^2, ..., m_1^n\}$ y $|m_0^i| = |m_1^i|$
3. $b \xleftarrow{\$} \{0, 1\}$
4. $b' \leftarrow \mathcal{A}(\mathsf{Enc}(k, m_b^1), \mathsf{Enc}(k, m_b^2), ..., \mathsf{Enc}(k, m_b^n))$
5. Output 1 si y sólo si $b = b'$

Figura 1: Experimento $\mathsf{Exp}^{\text{m-ind}}_{\Pi,\mathcal{A}}$

1. **5pts** Demuestre que existen esquemas con cifrados indistinguibles para un solo mensaje, es decir, que cumplen con la definición vista en clases, pero que NO tienen cifrados indistinguibles para múltiples mensajes (hint, encuentre un ejemplo para $n = 2$).

2. **5pts** Demuestre que si Enc es determinista (no aleatorio) y no mantiene estado (cada ejecución es independiente de las anteriores), entonces el esquema no puede tener cifrados indistinguibles para múltiples mensajes.

Problema 5: Generadores Pseudo-aleatorios (15pts)

Sea $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ un generador pseudo-aleatorio con expansión $\ell(n) > 2n$. Determine si las siguientes funciones son también generadores pseudo-aleatorios. Justifique su respuesta formalmente (demuestre en el caso afirmativo, y de un contraejemplo en el caso negativo).

- (**5pts**) $G'(s) = G(s_1, s_2, \ldots, s_n)$, donde $s \in \{0,1\}^{2n}$.
- (**5pts**) $G'(s) = G(1^{n/2}||s)$ para $s \in \{0,1\}^{n/2}$
- (**5pts**) $G'(s) = G(s)||G(s+1)$

Problema 6: Funciones Pseudo-aleatorias 10pts

Sea $F : 0,1^\lambda \times \{0,1\}^n \to \{0,1\}^n$ una función pseudo-aleatoria. Determine si las siguientes funciones $F' : \{0,1\}^\lambda \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$ son también psuedo-aleatorias. Justifique su respuesta formalmente (demuestre en el caso afirmativo, y de un contraejemplo si F' no es pseudo-aleatoria).

- **5pts** $F'(k,x) = F(k,0||x)||F(k,1||x)$
- **5pts** $F'(k,x) = F(k,0||x)||F(k,x||1)$

Problema (Opcional)

El archivo `ciphertext` corresponde a un texto que sido cifrado usando el One-Time Pad con un pad aleatoreo de 80 bytes. Descifre el archivo y léalo. Escriba en la solución algún párrafo del texto, y si usted lo desea de su opinión.

Problema Opcional

Demuestre que un esquema de cifrados Π es perfectamente secreto si y sólo si sus cifrados son perfectamente indistinguibles ($\Pr[\mathtt{Exp}^{\mathrm{ind}_{\mathcal{A},\Pi}} = 1] = 1/2$ para todo algoritmo $\mathcal{A}$)