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

Tarea 2: 02/04/2018

Evaluación Escrita: 13/04/2018, Entrega Final: 16/04/2018

Reglas

Las tareas se pueden discutir de a 2 estudiantes. 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`, `masanmartin@uc.cl`, `faflorenzano@uc.cl` y a `fekrell@uc.cl` con el asunto `[IIC3253] Entrega Tarea 2` 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 ayudantía del día Viernes 13 de Abril.

Problema 1: Generadores Pseudo-aleatorios 33pts

Sea $G : \{0,1\}^\lambda \to \{0,1\}^n$ un generador pseudo-aleatorio con $n \geq 2\lambda + 1$. Determine si las siguientes funciones G' son generadores pseudo-aleatorios. Justifique formalmente su respuesta (demuestre vía reducción en el caso afirmativo, y de un contraejemplo si G' no es pseudo-aleatoria).

- **11pts** $G' : \{0,1\}^{2\lambda} \to \{0,1\}^n,\ G'(x = x_1 x_2 \dots x_{2\lambda}) = G(x_1 x_2 \dots x_\lambda)$
- **11pts** $G' : \{0,1\}^\lambda \to \{0,1\}^{2n},\ G'(x) = G(x)||G(x+1)$
- **11pts** $G' : \{0,1\}^\lambda \to \{0,1\}^{n+1},\ G'(x) = G(x)||x_1$

Problema 2: Funciones Pseudo-aleatorias 33pts

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

- **11pts** $F' : \{0,1\}^\lambda \times \{0,1\}^{\lambda-1} \to \{0,1\}^{2\lambda},\ F'(k,x) = F(k,0||x)||F(k,1||x)$
- **11pts** $F' : \{0,1\}^\lambda \times \{0,1\}^{\lambda-1} \to \{0,1\}^{2\lambda},\ F'(k,x) = F(k,0||x)||F(k,x||1)$
- **11pts** $F' : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda,\ F'(k,x) = F(x,k)$

Problema 3: PRFs⇒PRGs (34pts)

Sea $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$ una función, y $G : \{0,1\}^\lambda \to \{0,1\}^{\ell \times \lambda}$ definida como $G(k) := F_k(1)||F_k(2)|| \ldots ||F_k(\ell)$. Demuestre que si F es una función pseudo-aleatoria, entonces G es un generador pseudo-aleatorio con expansión $\ell \times \lambda$.

Problema 4: Opcional (25pts válidos en cualquier tarea)

Sea F un cifrador de bloque (F es una permutación pseudo-aleatoria) con llaves de largo fijo n bits (ejemplo $n = 64$) con bloque de largo L bits. Dada la actual velocidad de procesadores y la gran capacidad de almacenamiento, la comunidad criptográfica ha recomendado utilizar cifradores de bloque con llaves de largo $2n$ bits.

Se propone el siguiente cifrador de bloque $F' : \{0,1\}^{2n} \times \{0,1\}^L \to \{0,1\}^L$ basado en F: Obtener 2 llaves k_1, k_2 independientes para F, generando una llave final $k = \langle k_1, k_2 \rangle$ de $2n$ bits. La función F' se define como $F'_{k_1,k_2}(x) = F_{k_1}(F_{k_2}(x))$.

Explique por qué el esquema propuesto no provee la seguridad deseada. Es decir, muestre un algoritmo distinguidor para F que requiera tiempo significativamente menor a 2^{2n} (pero no necesariamente polinomial en n). Asuma que F_k^{-1} es eficientemente computable.