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

Tarea 2: 6/04/2017

Entrega: 18/04/2017

Reglas

- Las tareas se pueden discutir de a 2 personas. Sin embargo, cada estudiante tiene la obligación de escribir su propia solución.
- Cualquier material no visto en clases utilizado para solucionar la tarea debe ser citado. Dicho esto, estas completamente prohibido buscar soluciones a los problemas en la web.
- La entrega de la tarea se realiza mediante correo electrónico firmado a `gnmonsalve@uc.cl` y con copia a `fekrell@uc.cl` con el asunto `[IIC3253] Entrega Tarea 2` 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.
- Usted puede elegir 4 de los primeros 5 probemas a resolver, el sexto es *obligatorio*.

Problema 1: Funciones Pseudo-aleatorias 16pts

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 2: PRF incondicional (16pts)

Describa una función aleatoria con llaves de largo n^2 bits, entrada de largo $\log n$ bits y output de largo n bits. Muestre que la ventaja de cualquier algoritmo distinguidor para su función es 0.

Problema 3: Doble DES(16pts)

Sea F un cifrador de bloque (F es una permutación pseudo-aleatoria) con llaves de largo fijo n bits (ejemplo $n = 64$). 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 $F' : \{0,1\}^{2n} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ 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} (no necesariamente polinomial en n). Hint: Asuma que F_k^{-1} es eficientemente computable.

Problema 4: Modo CBC (16pts)

Sea $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$ una permutación pseudo-aleatoria. Muestre que el modo de operación CBC, utilizando F como cifrador de bloque, tiene cifrados indistinguibles bajo ataques de texto plano escogido (CPA-seguro) para mensajes de largo arbitrario pero multiplo de λ. Hint: utilice el argumento híbrido.

Problema 5: PRFs⇒PRGs (16pts)

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 6: PRF débiles (20pts, obligatorio)

Para cualquier función $O(\cdot)$, definimos el oráculo O^* como: al ser llamado genera un input r uniforme en el dominio de O y retorna el par $\langle r, O(r)\rangle$. Una función (permutación) $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$ es una función (permutación) psuedo-aleatoria *débil* si: $\forall$ PPT $\mathcal{D}$ $\exists$ función negligible nelg, tal que

$$|\Pr_{k\sim U_\lambda}[D^{F_k^*}=1] - \Pr_{f\sim \mathcal{F}_\lambda}[D^{f^*}=1]| = \mathsf{nelg}(\lambda)$$

En donde $\mathcal{F}_\lambda$ es el conjunto de todas las funciones (permutaciones) de $\{0,1\}^\lambda$ a $\{0,1\}^\lambda$.

1. Demuestre que si F es pseudo-aleatoria, entonces también es pseudo-aleatoria débil.

2. Sea F' pseudo-aleatoria, y sea F definida como : $F(x) = F'(x)$ si x es impar y $F(x) = F'(x+1)$ si x es par. Demuestre que F no es necesariamente pseudo-aleatoria, pero sí es psuedo-aleatoria débil.

3. ¿Qué modos de operación de los vistos en clases siguen siendo seguros cuando utilizamos una función pseudo-aleatoria débil? Justifique su respuesta.