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

Tarea 3: 8/05/2017

*Entrega: 17/05/2017*

## 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, está 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 3` a las 15:30 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.
- Todos los problemas son *obligatorios*. Es decir, cada problema de esta tarea es un requisito para aprobar el curso.

## Problema 1: naive HMAC (20pts)

Sea $H^s : \{0,1\}^* \to \{0,1\}^n$ una función de hash resistente a colisiones.

1. a) Demuestre que el siguiente código de autenticación de mensajes NO es necesariamente seguro.
   - $\mathsf{Gen}(1^\lambda)$: Output $k \sim U_\lambda$.
   - $\mathsf{Mac}_k(m)$: Output $t = H^s(k||m)$.
   - $\mathsf{Vrfy}_k(m,t)$: Output 1 si y sólo si $t = H^s(k||m)$.

Hint: Piense que $H$ esta construida usando la transformación de Merkle-Damgärd sobre una función $h^s : \{0,1\}^{n'} \to \{0,1\}^n$ resistente a colisiones.

2. b) Un oráculo aleatorio $O(\cdot)$ es una función pública (todos los participantes, incluyendo al adversario tienen acceso a ella) que puede ser consultada como "caja negra" y que tiene la propiedad de que para cada consulta nueva $x$, el valor $O(x)$ es uniformemente aleatorio. Demuestre que si asumimos que $H$ es un oráculo aleatorio, entonces la construcción anterior sí es un código de auntenticación de mensajes seguro.

## Problema 2: Definiciones para Funciones Hash (20pts)

Demuestre que cualquier función de hash $H^s : \{0,1\}^m \to \{0,1\}^n$ resistente a colisiones, es resistente a segunda preimagen, y que cualquier función resistente a segunda preimagen es resiste a preimagen. Es decir, si para $H^s$ es infactible encontrar $x_1 \neq x_2$ tales que $H^s(x_1) = H^s(x_2)$, entonces dado $x$ uniforme en $\{0,1\}^m$ es infactible también encontrar $x' \neq x$ tal que $H^s(x) = H^s(x')$. A la vez, si dado $x$ uniforme en $\{0,1\}^m$ es infactible encontrar $x' \neq x$ tal que $H^s(x) = H^s(x')$, entonces si $y$ es uniforme en $\{0,1\}^n$ también es infactible encontrar $x$ tal que $H^s(x) = y$.

## Problema 3: Árboles de Merkle (20pts)

1. Describa el escenario de interés visto en clases para árboles de Merkle.
2. De una definición formal de seguridad para este escenario.
3. Describa formalmente la construcción vista en clases.
4. Demuestre su seguridad.