**Criptografía y Seguridad Computacional** **2016-01**

Tarea 4: 5/05/2016

*Entrega: 18/05/2016*

## 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 electrónico a `fkrell@gmail.com`, y con copia a `jsnavar1@uc.cl`, con el asunto `[cripto] Entrega Tarea4` a más tardar el día Miercoles 18 de Mayo de 2016 a las 23:59. Cada estudiante sólo puede asumir que su tarea ha sido correctamente entregada si recibe confirmación del profesor o del ayudante. Usted debe entregar un archivo formato PDF generado en LaTeX. Para su conveniencia puede usar el template en la página web del curso.

Si utiliza referencias, es obligación agregarlas al final de su solución.

## Problema 1 (15pts)

Sea $N, e, d$, generados por $\mathsf{GenRSA}$. Imagine que utilizamos el siguiente padding para el cifrador RSA: con input $m$, se retorna $0x00||r||0x00||m$, en donde $r$ tiene largo $||N||/2 - 16$ y el largo de $m$ es exactamente $||N||/2$.

1. **10pts**. Demuestre que RSA usando este padding no es CCA seguro (es decir, el adversario puede distinguir entre el cifrado 2 mensajes $m_0$ y $m_1$ si tiene acceso al oráculo de descifrado). Hint: Dado el texto cifrado $c = \mathsf{Enc}_{pk}(m_b)$, multiplique $c$ por una constante elegida cuidadosamente, y espere que que el oráculo no arroje "error de padding".

2. **5pts**. ¿Por qué su ataque no es posible en el esquema de padding visto en clases?

## Problema 2 (10pts)

Sea $H = (\mathsf{Gen}, \mathsf{Hash})$ una función de hash definida como:

- $\mathsf{Gen}(1^\lambda) : \mathbb{G}, q, g \leftarrow \mathcal{G}(1^\lambda)$, con $q = |\mathbb{G}|$ primos, $a, b \xleftarrow{\$} \mathbb{Z}_q$ y retorna $s = \langle q, g, a, b \rangle$.
- $\mathsf{Hash}^s(x_1, x_2, x_3)$: retorna $g^{x_1} \cdot g^{a \cdot x_2} \cdot g^{b \cdot x_3}$

Demuestre que si existe un algoritmo PPT $\mathcal{A}$ que encuentra colisiones en $H$, entonces existe un algoritmo PPT que distingue si $T$ es uniforme en $\mathbb{G}$ o es $g^{ab}$ dado el siguiente input

$$q, g, g^a, g^b, g^{a^2}, g^{b^2}, T$$

con $q = |\mathbb{G}|$ primo, $g$ un generador para $\mathbb{G}$, y $a, b$ uniformes en $\mathbb{Z}_q$. (Similar a DDH, pero además el distinguidor tiene acceseo a $g^{a^2}$ y $g^{b^2}$).

## Problema 3 (20pts)

En este problema vamos a demostrar que el supuesto DDH no se cumple en el grupo $\mathbb{Z}_p^*$ ($p$ primo). Sea $\mathsf{RC} = \{x | x = y^2 \mod p,\ y \in \mathbb{Z}_p^*\}$. Es decir, $\mathsf{RC}$, es el conjunto de residuos cuadrados de $\mathbb{Z}_p^*$ (elementos que son el cuadrado de algún otro).

1. **5pts**. Demuestre que $\mathsf{RC}$ es un subgrupo de $\mathbb{Z}_p^*$ bajo la misma operación (es un grupo, y además es subconjunto de $\mathbb{Z}_p^*$).
2. **5pts**. Describa un algoritmo de tiempo polinomial para saber si un elemento $y$, pertenece a $\mathsf{RC}$.
3. **10pts**. Construya un algoritmo PPT que quiebre DDH en $\mathbb{Z}_p^*$. Es decir, dado un generador $g$ para $\mathbb{Z}_p^*$, $g^a$, $g^b$ y $T$, construya un algoritmo que decida si $T = g^{ab}$, o $T$ es uniforme en $\mathbb{Z}_p^*$. Hint: utilize el algoritmo del problema 3.2.

## Problema 4 (15pts)

Se ha visto en clases que si el supuesto DDH se cumple para un grupo $\mathbb{G}$, con generador $g$ y orden $q$, entonces existe un protocolo de intercambio de llaves para 2 participantes (la llave final es $g^{a \cdot b}$, en donde un participante elige $a$ y el otro elige $b$, ambos uniformemente distribuídos en $\mathbb{Z}_q$).

Imagine que, además de $\mathbb{G}$, existe un grupo $\mathbb{G}_T$ con generador $g_t$ y una función computable en tiempo polinomial $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, tal que

- $e(h_1^a, h_2^b) = e(h_1, h_2)^{a \cdot b}$ para todo $h_1, h_2 \in \mathbb{G}$ (bilineal)
- $e(g, g) = g_t$ (no degenerado)

1. **5pts**. Demuestre que el supuesto DDH no se cumple en $\mathbb{G}$.
2. **5pts**. Proponga un protocolo de intercambio de llaves para 3 participantes en donde el output de los participantes es un elemento en $\mathbb{G}_T$ (asumma que a pesar de que DDH no se cumple en $\mathbb{G}$, DLog sigue siendo un supuesto razonable).
3. **5pts**. Extienda el supuesto DDH para este nuevo protocolo. Hint: ¿Qué elemento hay que agregarle al input del distinguidor? ¿Cuál es la forma de $T$ cuando no es uniformemente aleatorio?

## Problema 5 (Opcional)

Este es un problema de investigación. Busque applicaciones criptográficas adicionales de los mapeos bilineales (bilinear maps o parings en inglés) vistos en el problema 4.