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

Tarea 4: 01/06/2018

Entrega Final: 15/06/2018

Reglas

TODOS LOS PROBLEMAS SON OBLIGATORIOS

Las tareas se pueden discutir de a 2 estudiantes. Sin embargo, cada una/o tiene la obligación de escribir su propia solución. La entrega final de la tarea se realiza mediante correo electrónico firmado a `gnmonsalve@uc.cl`, `masanmartin@uc.cl`, `faflorenzano@uc.cl` y a `fekrell@uc.cl` con el asunto `[IIC3253] Entrega Tarea 4` a las 22:00 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, y que la solución para cada pregunta quede en una hoja distinta.

HINT: UTILICE HORARIOS DE CONSULTA Y FORO PIAZZA

Problema 1 [15pts]

Un esquema de cifrados de llave pública es *maleable* si dado un texto cifrado sobre un mensaje m es posible generar un texto cifrado para el mensage $f(m)$ para alguna función f.

1. Muestre que dado un texto cifrado ElGamal $\langle c_1, c_2 \rangle$ para un mensaje m es posible construir texto cifrado $\langle c'_1, c'_2 \rangle$ para el mensaje $\alpha \cdot m$ para cualquier α en $\mathbb{G}$.

2. Muestre que también se puede hacer con la restricción $c'_1 \neq c_1$ y $c'_2 \neq c_2$

3. Discuta si maleabilidad es siempre una propiedad negativa.

Problema 2 [5pts]

Un esquema de cifrados de llave pública es *key-private* si el texto cifrado no revela información alguna sobre la llave pública. Argumente si ElGamal y RSA con *key-private* o no.

Problema 3 [15pts]

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

1. **5pts**. Describa un algoritmo de tiempo polinomial para saber si un elemento y pertenece a QR.

2. **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 3.1.

Problema 4 [5pts]

Sea Π un protocolo de intercambio de llaves para 2 participantes en donde el elemento acordado a un grupo $\mathbb{G}$, y en donde cada participante envía un solo mensaje (El protocolo Diffie-Hellman visto en clases cumple esta propiedad). Muestre como transformar Π en un esquema de cifrados de llave pública.

Problema 5 [10pts]

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 distribuidos 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).

Problema 6 [10pts]

Ordene los siguientes supuestos de acuerdo a que tan fuertes/débiles son: $P \neq NP$, DDH, RSA, DLog, CDH, existen funciones unidireccionales, existen generadores pseudo-aleatorios, Factorización.