Criptografía y Seguridad Computacional **2016-01**

Tarea 6: 7/06/2016

Entrega: 15/06/2016

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 Tarea6` a más tardar el día Miércoles 15 de Junio 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.

Realice la tarea por cuenta propia. Pero si usted utiliza material externo, es obligación agregar las referencias correspondientes. Además usted debe escribir su propia solución. Es decir, usted debe tener la capacidad de responder preguntas con respecto a su solución.

Problema 1 (15pts)

Sea $\mathbb{G}$ un grupo de orden primo p donde DDH se cumple, y sea $H : \{0,1\}^* \to \mathbb{Z}_p$ un oráculo aleatorio. Demuestre como falsificar firmas en el siguiente esquema de firmas digitales:

- $\mathsf{Gen}(1^\lambda)$: $x \sim \mathbb{Z}_p$, output $PK = g^x$, $SK = x$.
- $\mathsf{Sign}_{SK}(m)$: $k \sim \mathbb{Z}_p$, $e = H(m)$, $s = k - SK \cdot e$, output $\sigma = (g^k, s)$.
- $\mathsf{Vrfy}_{PK}(m, \sigma = \langle r, s \rangle)$: Output 1 si, y sólo si, $g^s \cdot PK^{H(m)} = g^k$

Problema 2 (15pts)

Proponga un protocolo para la demostración de conocimiento sin divulgación para el logaritmo discreto de un valor $y = g^x$ en un grupo en donde

DLOG es computacionalmente difícil. Tanto el algoritmo verificador V como el demostrador P tienen que correr en tiempo polinomial. Demuestre que su protocolo cumple:

- Completeness: $\Pr[P(\mathbb{G}, g, p, x) \leftrightarrow V(\mathbb{G}, g, p, y = g^x) = 1] \geq 2/3$.
- Soundness: Para todo PPT $P^* \Pr[P^*(\mathbb{G}, g, p) \leftrightarrow V(y = g^x) = 1] \leq 1/3$.
- Zero-Knowledge: Para todo PPT V^* existe un simulador probabilístico de tiempo esperado polinomial tal que $\mathsf{view}^P_{V^*} \equiv S(\mathbb{G}, g, p, y = g^x)$. Es decir, la vista de V^* al interactuar con P es simulable por un algoritmo efficiente que no tiene acceso al secreto x.

Problema 3 (15pts)

En el protocolo de Yao para la evaluación segura de circuitos booleanos, cada compuerta g con entradas u, v y salida w es codificada cifrando las llaves correspondientes a w (K^0_w, K^1_w) con un cifrador simétrico utilizando las llaves correspondientes a los cables u y v. Es decir, sea $g : \{0,1\}^2 \to \{0,1\}$ la función que describe la compuerta booleana y sean $(K^0_u, K^1_u), (K^0_v, K^1_v)$ las posibles de llaves de entrada, entonces cada una de las 4 filas $(g(0,0), g(0,1), g(1,0), g(1,1))$ de la compuerta es cifrada como

$\mathsf{Enc}_{K^0_u \| K^0_v}(K^{g(0,0)}_w)$
$\mathsf{Enc}_{K^0_u \| K^1_v}(K^{g(0,1)}_w)$
$\mathsf{Enc}_{K^1_u \| K^0_v}(K^{g(1,0)}_w)$
$\mathsf{Enc}_{K^1_u \| K^1_v}(K^{g(1,1)}_w)$

y luego la tabla es permutada.

Si el evaluador tiene las llaves $K^{b_u}_u$ y $K^{b_v}_v$, entonces puede decifrar la fila que contiene $\mathsf{Enc}_{K^{b_u}_u \| K^{b_v}_v}(K^{g(b_u,b_v)}_w)$. Sin embargo, el evaluador no sabe cual es la fila que corresponde a sus llaves, por lo que una opción es decifrar las 4 entradas y quedarse con la correcta. A continuación, veremos de qué manera el evaluador puede saber cuál de los 4 valores decifrados corresponde a $K^{g(b_u,b_v)}_w$, y cuales valores son "basura". Sea $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ un cifrador simétrico.

1. **9pts.** Proponga un cifrador simétrico $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ tal que $\forall m$

   a) $\mathsf{Dec}'_k(\mathsf{Enc}'_k(m)) = m$, pero

b) $\forall k_1 \neq k_2 \ \mathsf{Dec}'_{k_2}(\mathsf{Enc}'_{k_1}(m)) = \perp$.

Realize los supuestos necesarios sobre el espacio de textos planos y textos cifrados para el cifrador original Π.

2. **6pts.** Verdadero o falso, justifique informalmente su respuesta. El cifrador simétrico utilizado en YAO:

   - Puede ser perfectamente secreto.
   - Debe tener cifrados indistinguibles.
   - Debe ser CPA-seguro.

Problema 4 (15pts)

Genere un par de llaves asimétricas GPG, y utilícelas para firmar el envío de su solución. La llave pública del profesor y ayudante pueden ser encontradas en la página web del curso. Puede utilizar Thunderbird con Enigmail plugin.

Verifique las huellas de las llaves:

fkrell@gmail.com	F16D 9606 3D2B 487D 965A A0D9 DFF2 4787 A7C2 1672
jsnavar1@uc.cl	9DD8 9AC6 6A7C 9624 3732 15EA 98FE AD1A 2586 175B