PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

Criptografía y Seguridad Computacional – IIC3253
Examen
4 de Julio, 2022

Instrucciones

Este examen consta de 6 preguntas conceptuales sobre la materia vista durante el curso. Cada respuesta correcta suma dos puntos y cada respuesta incorrecta resta un punto. La respuesta a cada pregunta no puede tener más de 10 lineas. Este examen se aprueba con 4 puntos o más.

Preguntas

Utilizaremos la notación vista en clases, en particular || representa la concatenación.

1. Sea H una función de hash criptográfica (resistente a colisiones y pre-imágenes). Una de las siguientes aseveraciones es falsa. Indique cuál es y explique por qué es falsa.

   (a) La función $f(x) := H(x \mid\mid x)$ no es resistente a colisiones.

   (b) La función $H(x \mid\mid H(x))$ es también una función de hash criptográfica.

2. Suponga que encuentra en la calle un papel que en un lado tiene un par ordenado de números y en el otro dice literalmente "El par ordenado al reverso representa un número que ha sido encriptado con ElGamal sobre $\mathbb{Z}_p^*$, donde p vale 553402322211286548 47".

   ¿Es la información disponible suficiente para decriptar el número original? De no ser así: ¿Qué información faltaría?

3. Suponga que necesita tener una base de datos con información que permita autentificar usuarios en base a un password que los mismos usuarios proveen (como suele ocurrir en la Web). Explique por qué **no** sería una buena idea almacenar pares $(e, H(p))$, donde e es el correo del usuario, H es una función de hash criptográfica y p es el password del usuario. *Hint: Comience su respuesta con "Si se filtra la base de datos [...]"*

4. Explique la estructura de un par de llaves RSA y la relación entre ellas.

5. Un Message Authentication Code es una función para autentificar mensajes en base a una llave simétrica. Esta función toma una llave k y un mensaje m para generar un tag t. Intuitivamente, esperamos que una persona con la llave k pueda verificar que el tag t es válido para el mensaje m, y que alguien sin acceso a dicha llave no pueda autentificar mensajes que no se han autentificado antes. Para formalizar esta noción, en clases definimos un *juego* que constaba de cinco pasos.

   (a) El verificador genera una llave k al azar.

   (b) El adversario envía un mensaje m al verificador.

   (c) ...

   (d) Los pasos 2 y 3 se repiten tantas veces como quiera el adversario.

   (e) ...

   Escriba los dos pasos faltantes, y luego explique cuándo decimos que el adversario gana el juego.

6. Ciertos documentos son aceptados por instituciones cuando están verificados por un notario y el notario asegura que el documento se puede utilizar en dicha entidad. A modo de ejemplo, la Universidad Católica aceptará una fotocopia de un título profesional siempre que un notario firme un mensaje que diga "Esta fotocopia de su título es válida, y se puede utilizar en la Universidad Católica".

   Suponga que se quiere digitalizar lo explicado arriba bajo los siguientes supuestos:

   - Existe un solo notario que tiene una llave secreta y una llave pública.
   - Todo el mundo conoce la llave pública del notario.
   - Cada entidad E tiene un string identificador ID_E conocido por todos. Todos estos identificadores tienen el mismo largo.

   Ahora, cuando una entidad E pida a un cliente un documento firmado y autorizado por el notario, se usará el siguiente protocolo.

   (a) El cliente genera el documento d y encripta $\text{ID}_E||d$ con la llave pública del notario (suponemos que el documento es también un string). El texto cifrado resultante, que llamaremos c, es enviado al notario.

   (b) El notario verifica que el documento es válido y se puede utilizar en la entidad correspondiente. De no ser así se termina el protocolo.

   (c) El notario genera una firma f para c con su llave privada y le envía f al cliente.

   (d) Finalmente, el cliente envía (c, f) a la entidad E.

   Para tener esta pregunta correcta deberá responder correctamente a las siguientes tres preguntas: (1) ¿Por qué el protocolo no satisface lo esperado? (2) ¿Cómo podemos modificar el último paso para arreglarlo? (3) ¿Qué complejidad innecesaria tiene el protocolo?