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

Criptografía y Seguridad Computacional – IIC3253
Examen
4 de Julio, 2025

Instrucciones

Este examen consta de 7 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 puede tener a lo más de 10 lineas. Este examen se aprueba con 5 puntos o más.

En el examen sólo se pueden hacer preguntas sobre los enunciados y deben hacerse en voz alta. No se permiten preguntas en la primera media hora y en la última media hora del examen.

Preguntas

1. Una HMAC puede ser definida de la siguiente forma $HMAC(k, m) = h(k\|m)$, donde k es la clave secreta compartida por dos usuarios, m es el mensaje que se necesita autentificar, y h es una función de hash. ¿Puede ser esta considerada una buena HMAC si h es la función de hash SHA-256?

2. "En la base de datos de un servicio web generalmente se encuentran encriptadas las contraseñas de los usuarios." ¿Es correcta esta afirmación? Justifique su respuesta.

3. Suponga dado un grupo G, un generador g y un número natural q tal que $|\langle g \rangle| = q$. Explique para qué sirve el protocolo de Diffie-Hellman y muestre una ejecución de este protocolo para dos usuarios A y B.

4. Enuncie el Teorema de Lagrange, y explique cómo este teorema nos ayuda a verificar que el orden de un grupo generado $\langle g \rangle$ es efectivamente un número q, cuando q es primo.

5. Al usar RSA como sistema criptográfico, tenemos el problema de que si encriptamos el mismo mensaje dos veces, obtenemos el mismo texto cifrado. Para evitar este problema, suponiendo que las llaves pública y secreta son $P_A = (e, N)$ y $S_A = (d, N)$, respectivamente, se encripta un mensaje $m \in \{0, \ldots, N-1\}$ seleccionando al azar un número $r \in \{1, \ldots, N-1\}$ que sea primo relativo con N, y definiendo $Enc_{P_A}(m) = ((m \cdot r)^e \bmod N,\ r) = (c, r)$. Explique cómo se puede desencriptar (c, r) teniendo acceso a la llave secreta S_A.

6. Suponga que está en un curso con 150 alumnos donde se necesita realizar las siguientes tareas:

   T1 Permitir a los alumnos enviar comentarios sobre el curso de manera anónima.

   T2 Votar de manera voluntaria y anónima sobre algún aspecto del curso (por ejemplo, el cambio del horario de ayudantía)

   Para realizar estas tareas los profesores quieren utilizar el protocolo de firmas de anillo visto en el curso e implementado en la tarea 4. Conteste las siguientes preguntas, justificando su respuesta.

   (a) ¿Es una buena idea usar firmas de anillo para la tarea T1?

   (b) ¿Es una buena idea usar firmas de anillo para la tarea T2?

7. Explique qué problema está tratando de resolver un minero de Bitcoin.