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?

   Solución. No, si h es SHA-256, la función definida como $HMAC(k, m) = h(k\|m)$ no es un buen hash-based message authentication code, ya que SHA-256 es susceptible a ataques de extensión de largo. Por lo tanto, sin necesidad de tener acceso a la llave k, dado $HMAC(k, m)$ es posible construir $HMAC(k, m')$ donde m es un prefijo de m'.

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.

   Solución. No, en la base de datos de un servicio web sería muy extraño encontrar contraseñas encriptadas. Lo que se encuentra es un checksum (generalmente en forma de PBKDF o un hash salteado) que permite, dada la contraseña, verificar que esa contraseña es correcta. Notar que esto es distinto de tener las contraseñas encriptadas, puesto que a partir de lo que hay en la base de datos no es posible "desencriptar" las contraseñas de los usuarios.

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.

Solución. El protocolo de Diffie-Hellman sirve para compartir una llave simétrica en un canal público. Una ejecución se ve de la siguiente forma: A genera un número secreto $x \in \{1, \ldots, q\}$ y envía a B el elemento g^x. B genera un número secreto $y \in \{1, \ldots, q\}$ y envía a A el elemento g^y. La llave simétrica compartida será $g^{x \cdot y}$, que A calcula como $(g^y)^x$ y B calcula como $(g^x)^y$.

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.

Solución. El Teorema de Lagrange dice que dado un grupo finito G y un subgrupo H de G, el orden de H divide al orden de G. Para verificar que el orden de $\langle g \rangle$ es efectivamente q lo que hacemos es verificar que g sea distinto de la identidad y que g^q sea la identidad. Como g^q es la identidad, el orden de $\langle g \rangle$ es menor o igual a q. Pero como $\langle g \rangle$ es un grupo, su orden tendría que ser un divisor de q. Como q es primo y $2 \leq |\langle g \rangle| \leq q$, tenemos que $|\langle g \rangle| = q$.

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.

Solución. Para desencriptar (c, r) basta con calcular $(c^d \cdot r^{-1}) \bmod N$, puesto que esto es equivalente a $(c^d \bmod N \cdot r^{-1}) \bmod N$ y sabemos que $c^d \bmod N = m \cdot r \bmod N$. Dado que r es primo relativo con N, podemos obtener r^{-1} usando el algoritmo extendido de Euclides.

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?

Solución.

(a) Sí, ya que las firmas de anillo permitirían asegurar que los mensajes fueron enviados por alguien del curso, pero sin saber quién. Hay que considerar, eso sí, que cada alumno podría enviar tantos mensajes anónimos como quiera.

(b) No, puesto que en una votación esperamos que cada persona pueda votar a lo más una vez, cosa que no podemos garantizar con el protocolo de firmas de anillos visto en este curso. Dicho de otra forma, si recibimos 100 votos, no podemos estar seguros de que esos 100 votos sean de 100 personas distintas. De hecho, una sola persona podría haber emitido esos 100 votos.

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

Solución. Un minero de Bitcoin está intentando generar un bloque bien formado, sin transacciones inválidas, y que tenga un header cuyo hash, al ser interpretado como un número natural, caiga dentro de un rango predeterminado.