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

Criptografía y Seguridad Computacional – IIC3253
Examen
6 de Julio, 2023

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.

Preguntas

1. ¿Es OTP un protocolo autentificado? Justifique su respuesta.

2. En el juego para definir una PRP, el Verificador comienza generando un número $b \in \{0, 1\}$ al azar. Explique qué es lo que determina este número b.

3. En clases se discutió que no era buena idea guardar en una base de datos el hash de la contraseña de los usuarios. Suponiendo que usamos como función de hash SHA-256: ¿Sigue siendo esto cierto si suponemos que los usuarios generarán contraseñas aleatorias de 256 bits? Responda sí o no y justifique su respuesta.

4. Suponga que conoce una llave pública RSA (e, N) y se filtra el número $\phi(N)$. ¿Podría usted en base a este número obtener la llave privada? Justifique su respuesta.

5. Aún teniendo protocolos asimétricos tales como RSA y ElGamal, en la práctica utilizamos el protocolo de Diffie-Hellman para compartir llaves que son luego utilizadas en protocolos de criptografía simétrica tales como AES. ¿Cuál es la principal razón para hacer esto?

6. En el protocolo de ElGamal, suponemos dados un grupo G, un elemento g de dicho grupo, y un número q tal que el orden del subgupo generado por g es q (es decir, $|\langle g \rangle| = q$).

   Adicionalmente se pide que q sea un número *grande*. Explique por qué.

7. Al usar firmas de Schnorr, suponemos dados un grupo G, un elemento g de dicho grupo, y un número q tal que el orden del subgupo generado por g es q (es decir, $|\langle g \rangle| = q$).

   Adicionalmente se pide que q sea un número primo. Explique por qué.