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.

   Respuesta: No, OTP no es un protocolo autentificado ya que el receptor no puede asegurar que los mensajes que recibe no han sido modificados. Por ejemplo, si recibe un número encriptado, un atacante con acceso a la red podría haber modificado dicho número (cambiando ciertos bits del mensaje) sin necesidad de conocer la llave ni el contenido del mensaje.

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.

   Respuesta: El número b determina si el Verificador va a utilizar una permutación al azar o un protocolo criptográfico durante el resto del juego.

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.

   Respuesta: No, si los usuarios generan contraseñas aleatorias de 256 bits y se utiliza SHA-256, que tiene como salida un string de 256 bits, entonces no es posible realizar un ataque basado en rainbow tables, ya que en este escenario para que el ataque sea efectivo se debe tener una rainbow table con 2^{256} filas (o un número cercano a esto).

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.

   Respuesta: Sí, dado que podemos calcular d (el inverso multiplicativo de e en módulo $\phi(N)$) utilizando el algoritmo extendido de Euclides. Con eso tenemos el par (e, N), que es la llave privada.

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?

   Respuesta: La principal razón para hacer esto es que, para encriptar mensajes, lo protocolos simétricos son más eficientes que los protocolos asimétricos.

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.

   Respuesta: Se pide que q sea un número *grande* porque si no lo fuera entonces el problema del logaritmo discreto en $\langle g \rangle$ se podría resolver por fuerza bruta.

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.

   Respuesta: Se pide que q sea un número primo para que cualquier persona pueda verificar que q es efectivamente el orden del subgrupo generado por g. Para esto basta verificar que $g^q = e$ (el elemento neutro de G) y que q es efectivamente un número primo.