ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN
CCPG1003 – INFORMATION ASSURANCE AND SECURITY
EXAMEN 2 - PRIMERA EVALUACIÓN - I TÉRMINO 2017-2018/ Junio 30, 2017

Nombre: _____ ***Matrícula:*** _____

COMPROMISO DE HONOR: Al firmar este compromiso, reconozco que el presente examen está diseñado para ser resuelto de manera individual, que puedo usar un lápiz o esferográfico; que sólo puedo comunicarme con la persona responsable de la recepción del examen; y, cualquier instrumento de comunicación que hubiere traído, debo apagarlo y depositarlo en la parte anterior del aula, junto con algún otro material que se encuentre acompañándolo. Además, no debo usar calculadora alguna, consultar libros, notas, ni apuntes adicionales a los que se entreguen en esta evaluación. Los temas debo desarrollarlos de manera ordenada.
Firmo el presente compromiso, como constancia de haber leído y aceptado la declaración anterior. "Como estudiante de ESPOL me comprometo a combatir la mediocridad y actuar con honestidad, por eso no copio ni dejo copiar".

_____
Firma

Tiempo de duración: 1 hora

Tema 1 (15 puntos)

Seleccione solo una (1) respuesta para cada una de las siguientes preguntas:

1. ¿Cuál de los siguientes algoritmos criptográficos no utiliza transposición?
   a. Vigenere's encryption
   b. Rail cipher
   c. AES
   d. DES

2. Se ha enterado que alguien ha diseñado un algoritmo eficiente para factorizar números grandes. ¿Cuál de los siguientes algoritmos dejaría de usar inmediatamente?
   a. RSA
   b. Diffie-Hellman
   c. AES
   d. Bin packing

3. ¿Cuál de los siguientes algoritmos es el más apropiado para verificar la integridad de archivos almacenados en sitios de descargas “espejo”?
   a. AES-CBC
   b. SHA-256
   c. DES-CBC
   d. HMAC-SHA1

4. ¿Para cuál de los siguientes casos es beneficioso añadir una sal (salt) a la contraseña?
   a. Prevenir un ataque en línea (online) a una cuenta de usuario específica.
   b. Prevenir un ataque en línea (online) distribuido a una cuenta de usuario específica.
   c. Prevenir un ataque en línea (online) a cualquier cuenta de usuario.
   d. Prevenir un ataque en línea (offline) a cualquier cuenta de usuario.

5. ¿Cuál de los siguientes algoritmos asimétricos es utilizado para generar de manera segura un secreto compartido, en protocolos de seguridad de redes comúnmente usados?
   a. RSA
   b. AES
   c. Bin packing
   d. Diffie-Hellman

Tema 2 (15 puntos)

Le han encargado diseñar un sistema de desafío-respuesta (challenge-response) para autenticar a los usuarios de un sistema. Su diseño debe seguir los principios básicos de desafío-respuesta es decir:

- El servidor inicia la conversación con un desafío y el usuario debe presentar la respuesta correcta
- Los desafíos y respuestas deben ser diferentes cada vez

a. Proponga una función de respuesta
b. ¿Qué información necesitan compartir anticipadamente el servidor (challenger) y el usuario (responder)?
c. Explique una limitación de su diseño

Sobre la calificación:
Tema 2

- Cada error grave será penalizado con 1 punto, hasta un máximo de 5 puntos por tema, adicional a otras penalizaciones normales (ejemplo: respuestas incompletas).
- Responda lo necesario. Una respuesta muy corta puede estar incompleta, pero al mismo tiempo, en una respuesta larga la probabilidad de cometer errores graves es mayor.