ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN
CCPG1003 – INFORMATION ASSURANCE AND SECURITY
EXAMEN 2 - PRIMERA EVALUACIÓN - II TÉRMINO 2017-2018/ Diciembre 1, 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: 1.5 horas

Tema 1 (15 puntos)

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

1. Los atacantes lanzan amenazas mientras que los defensores son responsables de las vulnerabilidades.
   a. Verdadero
   b. Falso

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. Poder distribuir de forma segura claves (secretas) compartidas es mucho más difícil en el caso de criptografía asimétrica.
   a. Verdadero
   b. Falso

5. Suponga que una política de contraseñas requiere una contraseña de 9 caracteres que no puede terminar con un dígito. ¿Cuántas contraseñas soporta esta política? Para sus cálculos asuma un alfabeto antes de restricciones de 256 caracteres. Justifique su respuesta.
   a. 256^9
   b. 10^9
   c. 246×256^8
   d. 10×256^8
   e. Ninguna de las anteriores

Tema 2 (15 puntos)

Explique **dos** razones por las que no debería usar un algoritmo simétrico en modo **ECB**.

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.