

**Universidad Simón Bolívar**  
**Departamento de Computación y**  
**Tecnología de la Información**  
**Enero-Marzo 2009**  
**CI-6352**

Nombre:  
 Carnet:

1er Parcial RESPUESTAS (45 %)

**I. Verdadero o Falso (35 puntos)**

Para cada una de las siguientes 35 aseveraciones, diga si es Verdadera o Falsa. Cada pregunta vale 1 punto. Toda pregunta tiene una respuesta única, verdadera o falsa.

Coloque sus respuestas en la tabla a continuación, marcando con una **X** en el recuadro correspondiente a **Verdadero** o **Falso** para cada pregunta. **NO SE TOMARAN EN CUENTA RESPUESTAS QUE NO APAREZCAN EN LA TABLA.**

<b>Preguntas</b>	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
<b>Verdadero</b>															
<b>Falso</b>															

<b>Preguntas</b>	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
<b>Verdadero</b>															
<b>Falso</b>															

<b>Preguntas</b>	31	32	33	34	35
<b>Verdadero</b>					
<b>Falso</b>					

1. (V) Observar el tráfico en una red puede constituir una violación a la seguridad
2. (F) No revelar las técnicas utilizadas en un servicio de seguridad permite alcanzar mayores niveles de seguridad
3. (V) Alterar la identificación del emisor de un mensaje sin alterar su contenido es un ataque a la integridad
4. (F) El servicio de no-repudio requiere confidencialidad
5. (F) La negación de servicio implica una violación de la confidencialidad
6. (V) AES es más rápido que RSA

7. (V) El criptoanálisis permite descubrir posibles fallas de un algoritmo criptográfico
8. (V) Cifrado es computacionalmente seguro si el costo de romperlo excede valor de información
9. (V) Si se tiene una máquina capaz de realizar 1 millón de descifrados por segundo, y se usan claves de 20 bits, demoraría menos de dos segundos en descifrarse un mensaje
10. (V) DES está basado en la estructura de Feistel
11. (V) AES acepta claves de más de 128 bits
12. (F) El cifrado en bloques es más seguro que el cifrado de flujo
13. (F) La clave de sesión debe ser escogida por uno de los entes que desea comunicarse
14. (V) El servicio de autenticación implica que una alteración del mensaje es detectada
15. (V) Se puede usar *Blowfish* para autenticación
16. (F) Es posible encontrar una función de resumen criptográfico con la propiedad de salida de tamaño fijo (y finito) que no tenga colisiones
17. (F) Si se concatena un valor secreto (sólo conocido por emisor y receptor) al mensaje original, luego se le calcula el resumen criptográfico y se envía, se puede garantizar la integridad
18. (F) Para verificar la integridad de un mensaje, el receptor calcula la inversa del resumen criptográfico incluido en dicho mensaje
19. (V) MD5 acepta entradas de cualquier tamaño
20. (V) En los ataques a los algoritmos de resumen criptográfico, denominados de colisión propiamente dicha, el atacante se limita a buscar dos valores  $m$  y  $m'$  que colisionen, pero desconoce tanto sus valores como el del resumen criptográfico
21. (F) HMAC utiliza criptografía asimétrica
22. (V) RSA permite que los mensajes cifrados con la clave pública sean descifrados con la clave secreta, y viceversa, que los cifrados con la secreta puedan ser descifrados con la pública
23. (F) La fortaleza del algoritmos de Diffie-Hellman se basa en la dificultad de la factorización de números discretos
24. (F) Claves RSA mayores de 128 bits se consideran seguras actualmente 1
25. (V) Los certificados X.509 permiten evitar los ataques de “hombre en el medio” en criptografía pública
26. (V) Si A tiene un certificado firmado por la autoridad certificadora  $AC_1$  ( $AC_1 \ll A \gg$ ), el de B lo firma  $AC_2$  ( $AC_2 \ll B \gg$ ), y existen certificados  $AC_3 \ll AC_1 \gg$  y  $AC_3 \ll AC_2 \gg$ , entonces A y B pueden comunicarse de manera segura usando cifrado asimétrico

27. (V) El protocolo IPsec permite que las aplicaciones usen canales seguros sin necesidad de ser modificadas o recompiladas
28. (V) El servicio de autenticación (AH) de IPsec en modo transporte protege contra alteraciones de direcciones IP del paquete original
29. (V) El protocolo ISAKMP (*Internet Security Association and Key Management Protocol*) permite establecer claves de cifrado en IPsec
30. (F) TLS (*Transporte Layer Security*) permite que las aplicaciones usen canales seguros sin necesidad de ser modificadas o recompiladas
31. (F) El protocolo *Record* de SSL permite, entre otros, negociar los parámetros de cifrado y de autenticación
32. (V) PGP comprime antes de cifrar
33. (V) El sistema de llaveros de PGP permite que un usuario tenga varias claves secretas
34. (F) Actualmente, en sistemas UNIX las claves de acceso (*passwords*) se guardan cifradas usando una clave secreta en un archivo del sistema en el directorio `/etc/shadow`
35. (F) Los virus informáticos se replican sin necesidad de un programa anfitrión

## II. Desarrollo (10 puntos)

### Instrucciones:

- Los estudiantes de Ingeniería de Computación (pre-grado) deben contestar sólo la primera pregunta, que vale 10 puntos para ellos, y 5 para los estudiantes de post-grado.
  - Los estudiantes de post-grado deben contestar todas las preguntas.
1. (**PRE-GRADO: 10 puntos. POST-GRADO: 5 puntos**) Dé un esquema de cortafuegos con bastión y encaminadores con filtro de paquetes para proteger la red interna de una organización. Explique las bondades de su esquema
  2. (**SOLO POST-GRADO: 3 puntos**) Justifique por qué se usa Triple DES (Cifrado-Decifrado-Cifrado) y no doble DES (EE)
  3. (**SOLO POST-GRADO: 2 puntos**) Compare la complejidad de los algoritmos Lempel-Ziv (compresión) y de AES (cifrado).