Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

"Funciones resumen"

Test de autoevaluación

Seleccione la respuesta correcta.

1. ¿Qué es una función resumen o *hash*?
   - Un proceso que, dado un mensaje, produce una salida que es siempre más pequeña.
   - Un proceso que, dados dos mensajes, produce dos salidas que siempre son distintas.
   - Un proceso que, ante cualquier mensaje de entrada, produce una salida siempre del mismo tamaño.
   - Un proceso que cifra un mensaje de forma irrecuperable.

2. ¿Qué relación tienen las colisiones con las funciones resumen?
   - Sólo las "malas" funciones resumen tienen colisiones.
   - Todas las funciones resumen tienen colisiones.
   - Sólo las funciones resumen que producen una salida corta tienen colisiones.
   - Las funciones resumen, al ser irreversibles, tienen colisiones, pero es computacionalmente imposible encontrarlas.

3. Una función resumen criptográficamente segura…
   - Sólo se puede aplicar a mensajes cuyo tamaño sea más grande que el de la salida.
   - Debe producir una salida pseudoaleatoria.
   - No puede tener colisiones.
   - Es típicamente un proceso lento en comparación con el cifrado.

4. Si se modifica un bit del mensaje, y se aplica una función resumen de 56 bits, el resumen (al aplicar una función resumen criptográfica) se modificará en una media de:
   - 1 bit, en la misma posición que donde se alteró el mensaje.
   - 1 bit, en cualquier parte del resumen.
   - 56 bits.
   - 26 bits.

5. Una buena función *hash*…
   - Aplicada sobre un mismo mensaje, debe producir siempre el mismo resultado.
   - Aplicada sobre un mismo mensaje, puede producir resultados diferentes.
   - Debe disponer de una implementación en hardware.
   - Debe basarse en un diseño que permanezca en secreto.

6. Dado un mensaje M, ¿cómo de difícil debe ser encontrar otro mensaje de forma que los resúmenes coincidan, si la función resumen es criptográficamente segura?
   - Matemáticamente imposible.
   - Computacionalmente imposible.
   - Probabilísticamente imposible.
   - Técnicamente improbable.

7. La propiedad de una sola vía establece que…
   - No es técnicamente factible encontrar un mensaje que resulte en un valor concreto de resumen.
   - No es fácil encontrar dos mensajes cualesquiera que den un resumen concreto.
   - Es imposible obtener el mensaje a partir del resumen.
   - No se puede aplicar la función resumen sobre dos mensajes a la vez.

8. ¿Cuándo se puede decir que una función resumen está "rota"?
   - Cuando se puede encontrar una colisión de un mensaje.
   - Cuando existe una forma de encontrar colisiones más sencilla que la fuerza bruta.
   - Cuando existe un procedimiento (algoritmo) técnicamente viable en un corto espacio de tiempo.
   - Cuando el ataque de colisión involucra menos de 2^{121} operaciones.

9. El ataque de cumpleaños refleja la probabilidad de un ataque de colisión, modelando…
   - Las personas (identidades) como mensajes, la fecha (día y mes) de cumpleaños como resumen.
   - La fecha de cumpleaños (día y mes) como mensaje, la persona (identidad) como resumen.
   - Las personas (identidades) como mensajes, la fecha (día, mes y año) de cumpleaños como resumen.
   - El día de cumpleaños como mensaje, la persona (identidad) como resumen.

10. ¿Cuál de las siguientes afirmaciones es cierta sobre MD5?
    - Se considera técnicamente robusta.
    - Genera una salida de 256 bits.
    - No puede trabajar sobre mensajes menores de 512 bits.
    - Se basa en una función de compresión que se aplica iterativamente.

11. Acerca de la familia SHA-x,
    - Son refinamientos iterativos de un mismo diseño.
    - SHA-1 se considera insegura desde el año 2005.
    - SHA-256 no pertenece a la familia SHA-2.
    - SHA-2 fue comprometida, al igual que SHA-3.