Sexto Trabajo de Laboratorio

CUI:20153688 Alexander Apaza Torres

Seguridad en Computación
21 de junio de 2019

1. Cuestionario Previo

1. ¿A que se llama Little Endian? ¿Que funciones Hash la usan?

   Es un formato en el que se trataran los datos. A diferencia de *Big Endian* en el que los bytes más significativos van primero y luego van los bytes menos significativos, el *Little Endian* pondrá los bytes menos significativos al principio y los más significativos al final. Esto hace más intuitivo el acceso a los datos ya que las operaciones se darán desde los menos relevantes a los más relevantes. Sin embargo, el uso de estos formatos no afectan a la seguridad de un algoritmo, es solo para conveniencia de cada algoritmo. Entre las funciones que las usan están:

   a) Haval-3, Haval-4, Haval-5

   b) MD4, MD5

   c) La familia de RIPEMD

   d) GOST R 34.11-94 y GOST 34.311-95

2. Explique las funciones implementadas en cada ronda de MD5

   MD5 trabaja sobre un texto de 128 bits, que es dividido en 4 palabras de 32 bits cada una, denotadas por A, B, C, D. A estas 4 palabras se le aplicará cualquiera de estas funciones, dependiendo del número de ronda:

   a) $F(B, C, D) : (B \wedge C) \vee (\neg B \wedge D)$ Se ejecutará desde la iteración 0 a la 15.

   b) $G(B, C, D) : (B \wedge D) \vee (C \wedge \neg D)$ Se ejecutará desde la iteración 16 a la 31.

   c) $H(B, C, D) : B \oplus C \oplus D$ Se ejecutará de la iteración 32 a la 47.

   d) $I(B, C, D) : C \oplus (B \vee \neg D)$ Se ejecutará de la iteración a la 63.

3. ¿Como se implementa el ataque de cumpleaños del MD5?

   Haciendo colisionar el hash para encontrar un par de valores que produzcan la misma firma. Esto se hace por el método de fuerza bruta, siendo H el número de resultados distintos de igual probabilidad, se evalua $1{,}2\sqrt{H}$ elementos distintos y se espera encontrar un par que tenga el mismo resultado.

4. Muestre un ejemplo de colisión en MD5 Los siguientes bloques producen una colisión en MD5:

   d131dd02c5e6eec4693d9a0698aff95c
   2fcab58712467eab4004583eb8fb7f89
   55ad340609f4b30283e488832571415a
   085125e8f7cdc99fd91dbdf280373c5b
   d8823e3156348f5bae6dacd436c919c6
   dd53e2b487da03fd02396306d248cda0
   e99f33420f577ee8ce54b67080a80d1e
   c69821bcb6a8839396f9652b6ff72a70

   2fcab50712467eab4004583eb8fb7f89
   55ad340609f4b30283e4888325f1415a
   085125e8f7cdc99fd91dbd7280373c5b
   d8823e3156348f5bae6dacd436c919c6
   dd53e23487da03fd02396306d248cda0
   e99f33420f577ee8ce54b67080280d1e
   c69821bcb6a8839396f965ab6ff72a70

5. Explique la función de compresión en SHA1, ¿porque se dice que cada bloque pasa por 80 vueltas? ¿Cuáles son las operaciones sobre cada bloque de entrada?

   SHA-1 trabaja sobre un bloque de 512 bits, dividiéndolos en 16 palabras de 32 bits. Tendremos también 5 palabras que se inicializarán, a estas palabras se les aplicará, las siguientes funciones:

$$F(B,C,D) = (B \wedge C) \vee (\neg B) \wedge D$$
$$G(B,C,D) = (B \oplus C \oplus D)$$
$$H(B,C,D) = (B \wedge C) \vee (B \wedge D) \vee (C \wedge D)$$
$$I(B,C,D) = (B \oplus C \oplus D)$$

Referencias

[1] Why do all hash functions use big-endian data?. https://crypto.stackexchange.com/questions/2099/why-do-all-hash-functions-use-big-endian-data.

[2] Bert den Boer; Antoon Bosselaers (1993). Collisions for the Compression Function of MD5. Berlin; London: Springer. pp. 293–304.