Criptografía

Profesor: Melvin Fernández Ch.

Video 10

fidélitas

Virtual

fidélitas Virtual

Funciones de Hash y protocolos de seguridad

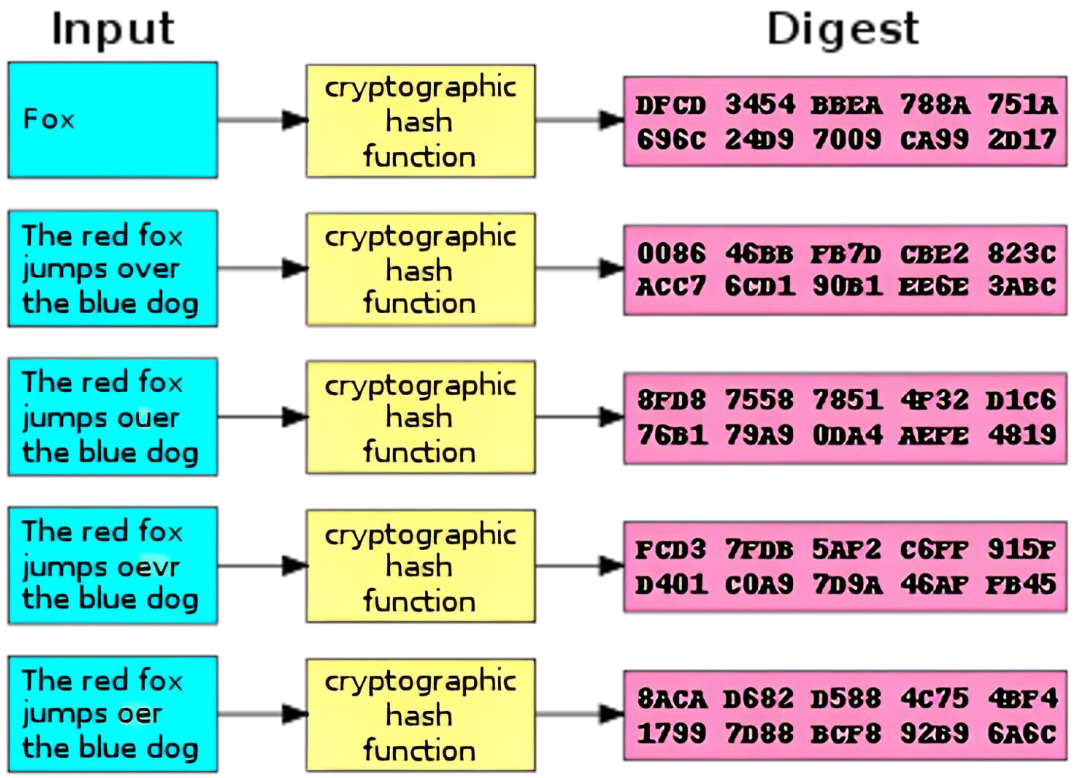
Módulo: 4

Definición de una función de Hash

fidélitas Virtual

- Una función criptográfica hash- usualmente conocida como “hash”- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija.

- Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.



Características de las funciones Hash

fidélitas Virtual

- Tiene un mensaje M de tamaño variable como entrada y producen un resumen (digest) del mensaje H(M) de tamaño fijo como salida.

- No tiene una clave secreta como entrada.

- Se usan para la autenticación de mensajes, el almacenamiento de contraseñas y la firma digital.
  - Produce una huella (fingerprint) de un fichero, mensaje o cualquier otro bloque de datos.

Características de las funciones Hash

- Para ser útil para autenticación de mensajes, una función resumen H debe tener las siguientes propiedades:
  1. Tiene entrada de cualquier tamaño y salida de tamaño fijo.
  2. Es relativamente fácil calcular H(x) para cualquier x dado, permitiendo implementaciones hardware y software.
  3. Dado h, es computacionalmente inviable encontrar un x tal que H(x) = h (de un sentido o resistencia a pre-imagen).
  4. Dado x, es computacionalmente inviable encontrar un y con H(y) = H(x) (resistencia débil a colisiones o a 2ª pre-imagen).
  5. Es computacionalmente inviable encontrar un par (x, y) tal que H(x) = H(y) (resistencia fuerte a colisiones).

Características de las funciones Hash

- Existen dos formas de atacar una función resumen:
  - Criptoanálisis.
  - Consisten en explotar debilidades lógicas del algoritmo.

- Fuerza bruta
  - La fortaleza de la función resumen depende únicamente del tamaño del código hash producido por el algoritmo.

Cronología de algoritmos Hash

- **N-Hash:** Nippon Telephone and Telegraph, 1990. Resumen de 128 bits.
- **Snefru:** Ralph Merkle, 1990. Resúmenes entre 128 y 256 bits. Ha sido criptoanalizado y es lento.
- **MD4:** Ronald L. Rivest, 1990. Resumen de 128 bits.
- **Haval:** Yuliang Zheng, Josef Pieprzyk y Jennifer Seberry, 1992. Resúmenes hasta 256 bits. Admite 15 configuraciones diferentes.
- **RIPEMD:** Comunidad Europea, RACE, 1992. Resumen de 160 bits.
- **MD5:** Ronald L. Rivest, 1991. Resumen de 128 bits. Mejoras sobre MD2 y MD4 (1990), más lento pero con mayor nivel de seguridad.
- **SHA-0 (o SHA):** National Security Agency (NSA), 1993. Resumen de 160 bits. Vulnerable y reemplazado por SHA-1.

Cronología de algoritmos Hash

- **SHA-1:** National Security Agency (NSA), 1994. Similar a MD5 pero con resumen de 160 bits.
- **Tiger:** Ross Anderson, Eli Biham, 1996. Resúmenes hasta 192 bits. Optimizado para máquinas de 64 bits (Alpha).
- **Panama:** John Daemen, Craig Clapp, 1998. Resúmenes de 256 bits. Trabaja en modo función hash o como cifrador de flujo.
- **SHA-2:** National Security Agency (NSA), 2001-2004. Resúmenes entre 224 y 512 bits (224, 256, 384, o 512). Mejoras sobre SHA-1.
- **SHA-3 (Keccak):** Guido Bertoni, Joan Daemen, MichaÎl Peeters y Gilles Van Assche, 2015. Resúmenes arbitrarios estándar (224, 256, 384, o 512). Más robusto que SHA-2.

Gracias

fidélitas Virtual