Funciones Hash e Integridad de datos

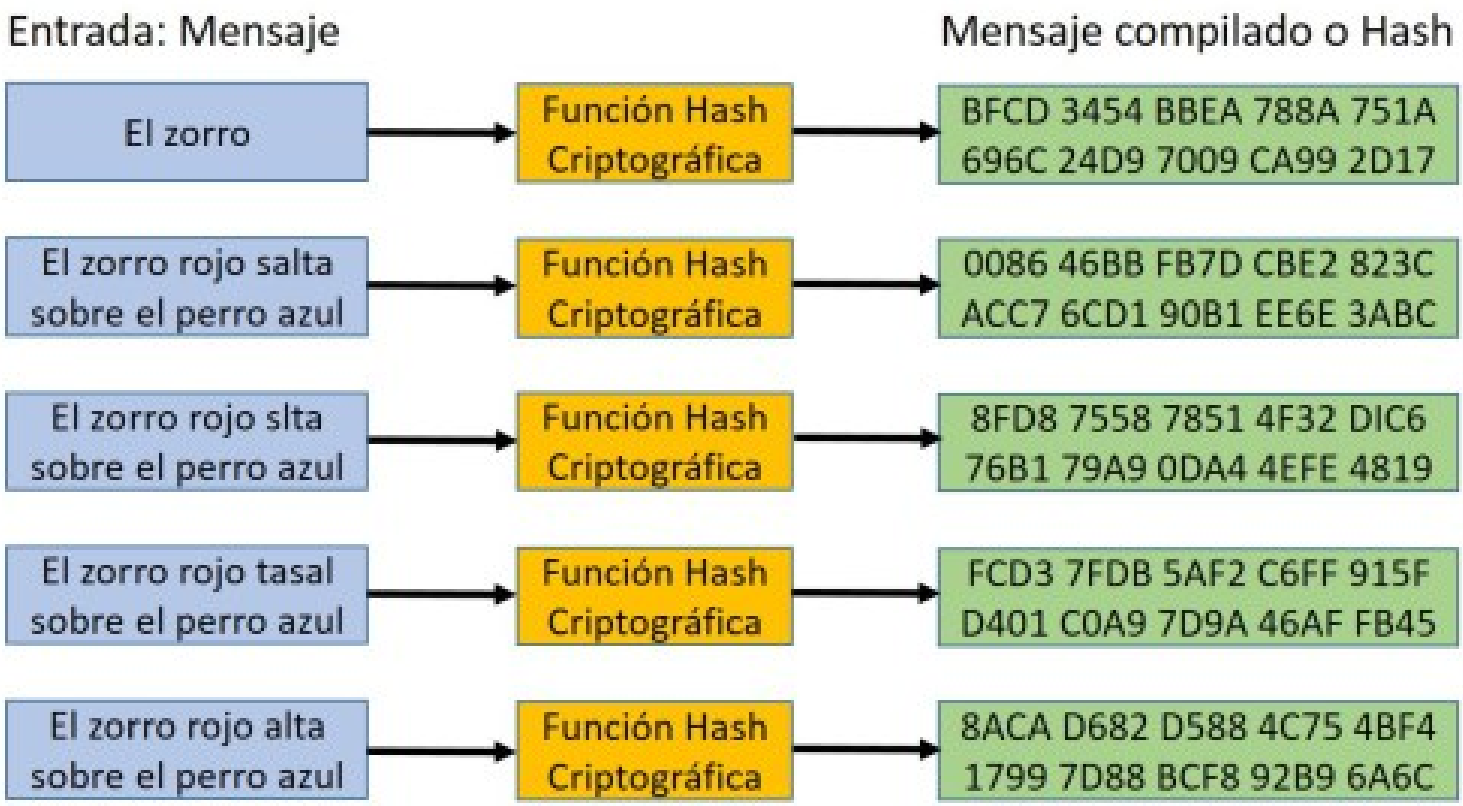
Aarón Arias Pérez

Universidad de Cádiz

27 de diciembre de 2017

Funciones Hash

1. ¿Qué son las funciones hash?
2. ¿Para qué se utilizan?



Clasificación

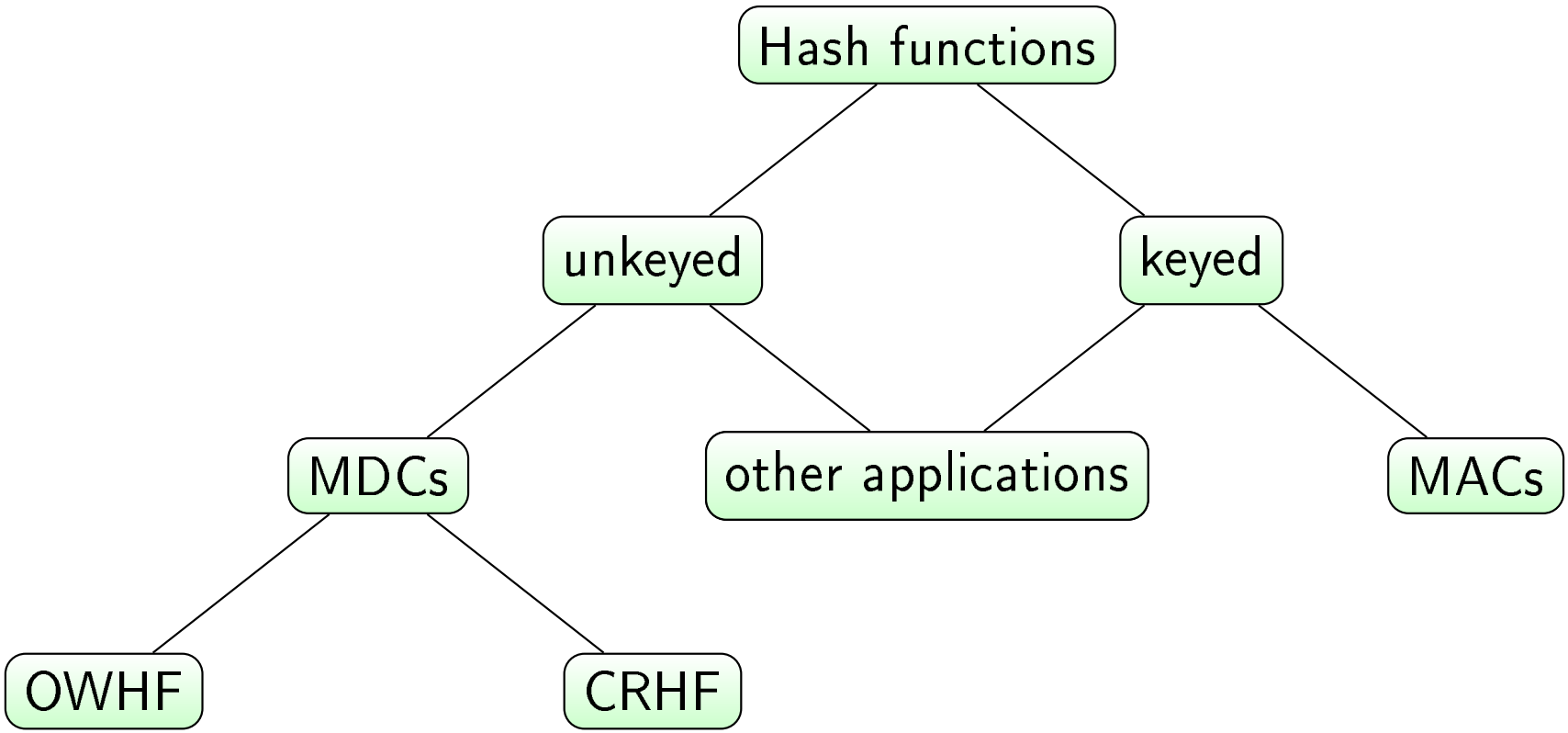
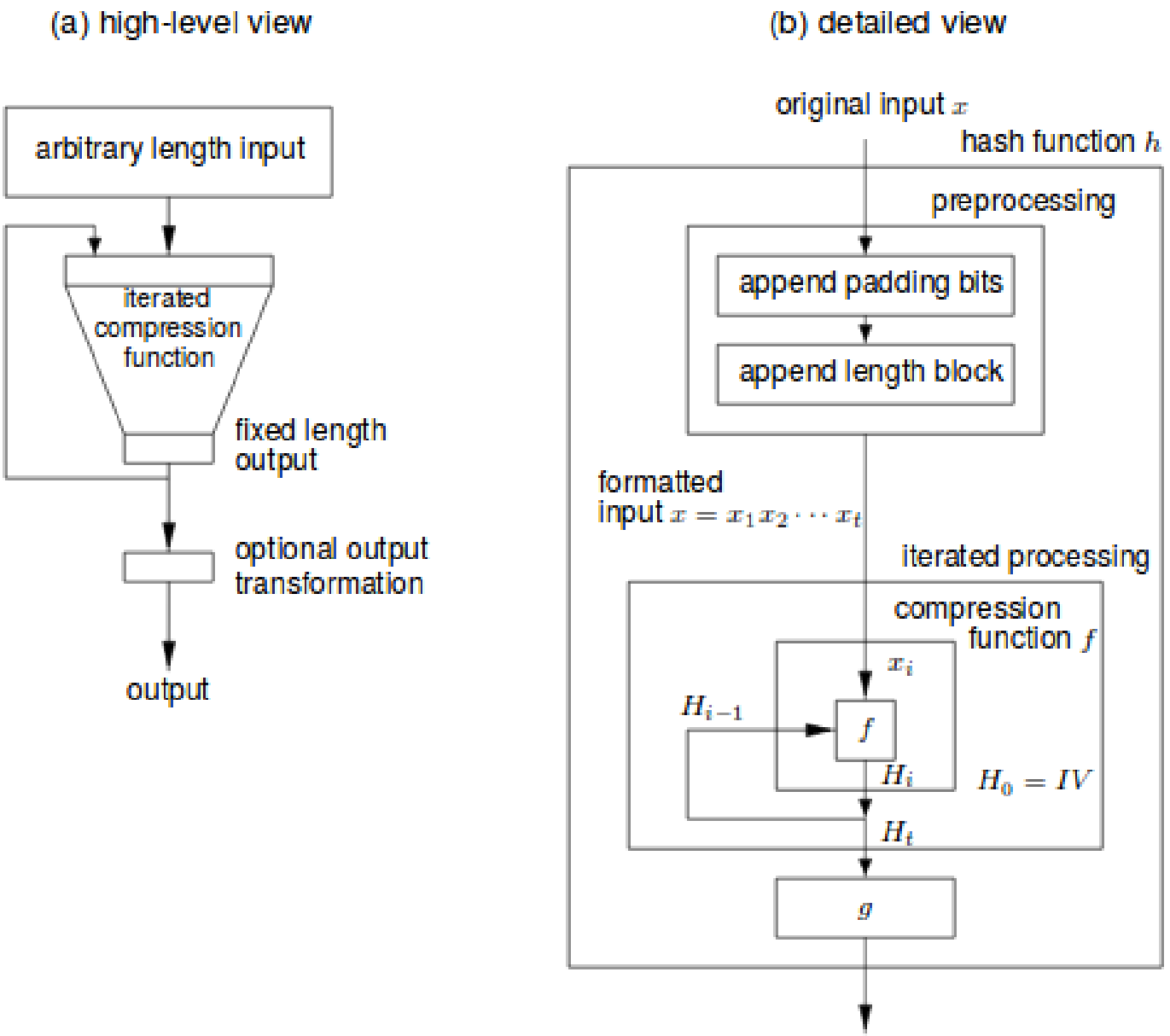


Figura: Esquema de la clasificación de funciones hash.

Propiedades

1. Resistencia a la preimagen
2. Resistencia a la 2ª preimagen
3. Resistencia a la colisión

Proceso iterativo



Integridad de datos

Definición

La integridad de datos es la propiedad por la cual los datos no han sido alterados de manera no autorizada desde el momento en el que fueron creados, transmitidos o almacenados por una fuente autorizada.

Operaciones que invalidan la integridad

- Inserción de bits (incluyendo las que provienen de fuentes fraudulentas)
- Eliminación de bits
- Reordenamiento de bits o grupos de bits
- Inversión o sustitución de bits
- Cualquier combinación de las anteriores

Importancia del Hashing

- Comunicaciones (protección contra intrusos y integridad de datos)
- Bases de datos (contra accesos indeseados)
- Estructuras de datos mas eficientes en búsqueda (tablas resumen, árboles Merkle)

Referencias


Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone (1996)
Handbook of Applied Cryptography