Hash Functions

Keith Bogart

CCIE #4923

- kbogart@ine.com
- @keithbogart1
- linkedin.com/in/keith-bogart-2a75042

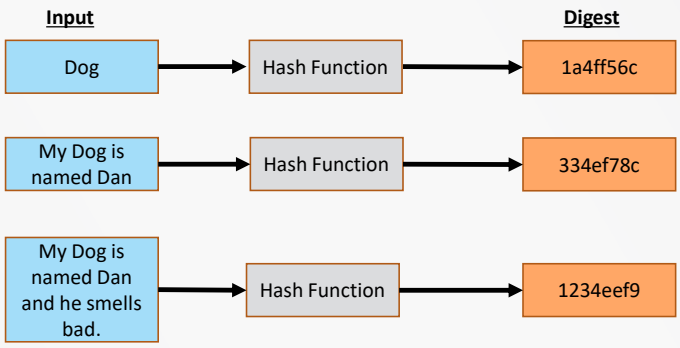
CCIE Routing & Switching

Topic Overview

- What Are Hash Functions
- Properties Of Cryptographic Hash Functions
- How Hashing Provides Data Integrity
- Variety Of Hash Algorithms

Hash Functions

- "Any function that can be used to map data of arbitrary size to data of a fixed size."
- The result of a hash function is called:
  - Hash values
  - Hash codes
  - Digests
  - Hashes



Hashing For Integrity

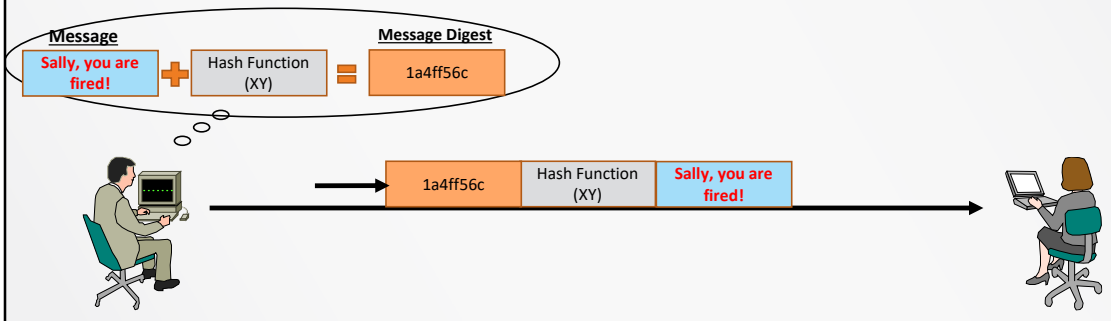
- A “Hash” received along with data provides verification of data integrity.
- A “Hash” (aka “Digest” or “Fingerprint”) is derived as a result of a “Hash Function”.
- A secure Hash is also paired with a password, or “key”.
- Can also be used with authentication.

Cryptographic Hash Function Properties

- Cryptographic Hash Functions have five properties:
  - Deterministic: the same message always results in the same hash
  - Quick to compute the hash value for any given message
  - Infeasible to determine the original message from its hash value except by trying all possible messages
  - A small change to a message should change the hash value **so extensively** that the new hash value appears uncorrelated with the old hash value
  - Infeasible to find two different messages with the same hash value (this would be called a “hash collision”

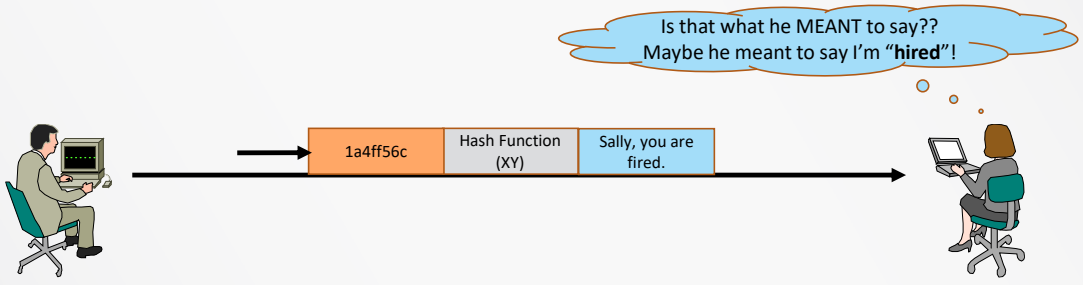
Hashes And Data Integrity

- So how does a cryptographic hash function provide data integrity?

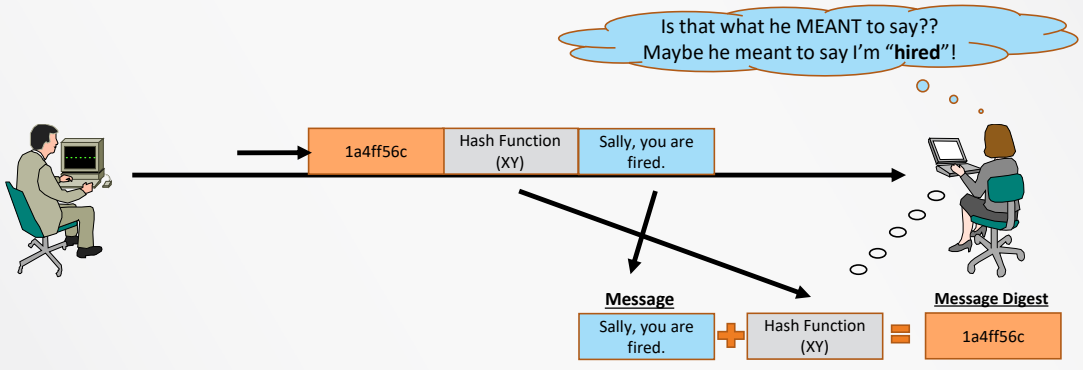


You have to tell the receiver what Hash algorithm you used so they can perform the same hash to check for validity.

Hashes And Data Integrity



Hashes And Data Integrity



Choices, Choices, Choices

- There are many different Hash Functions to choose from.
- Point to remember: The longer the Digest, the more secure the function.
- The following list denotes the most common cryptographic hash functions:
  - MD5 (Message Digest 5): **128-bit Digest**
  - SHA-1 (Secure Hash Algorithm 1): **160-bit Digest**
  - RIPEND-160 (RACE Integrity Primitives Evaluation Message Digest): **160-bit Digest**
  - **SHA-2 (Secure Hash Algorithm 2): 224 through 512-bit Digest**
  - SHA-3 (Secure Hash Algorithm 2): **224 through 512-bit Digest**
  - WHIRLPOOL: **512-bit Digest**
  - BLAKE2: **8 through 512-bit Digest**

MD5 was designed by Ronald Rivest in 1991 (the same Rivest as in RSA Signature), Creates digest of 128-bits. Proven to be insecure.

-

SHA1: Developed by US Governments Capstone project in 1993. Produces digest of 160-bits but proven insecure and susceptible to collisions so is considered “broken”.

-

RIPEND used in the Bitcoin standard (more secure than MD5, similar security to SHA-1)

-

SHA-2 is the current standard used in SSL Certificates. Has many variants capable of creating Hash Digests from 224 to 512-bits. Currently SSL Certificates are standardized on the SHA-256 function.

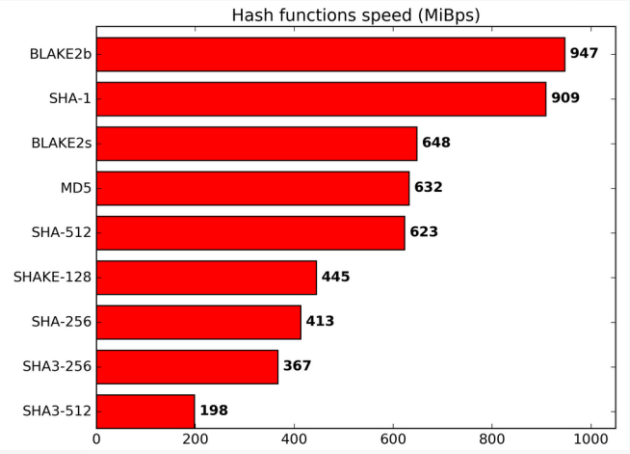
-

WHIRLPOOL – no known weaknesses, creates a 512-bit digest, but slower than other algorithms.

-

BLAKE2 is a cryptographic hash function **faster than MD5, SHA-1, SHA-2, and SHA-3**, yet is at least as secure as the latest standard SHA-3.

Hash Function Speeds



https://blake2.net/

Statistics gathered from tests performed on a Skylake Intel CPU (speeds are for hashing using a single core).

Secure Hash Algorithms

- To aid in Authentication and Data Integrity Validation, Hash algorithms sometimes incorporate a shared password into the formula in addition to the digital message.
- This prevents spoofing, because a Malicious Actor cannot create an acceptable Hash Digest without knowing the shared password.