NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Shamik Sural
Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 04: Basic Cryptographic Primitives - II

CONCEPTS COVERED

- Cryptographic Hash Functions
- SHA-256
- Types of Hashing

KEYWORDS

- Hash Function
- Secure Hash Algorithm
- Patterns of Hashing Data

Hash Function – SHA256

- SHA256 is used in Bitcoin mining – to construct the Bitcoin blockchain
- Secure Hash Algorithm (SHA) that generates 256 bit message digest
- A part of SHA-2, a set of cryptographic hash functions designed by United States National Security Agency (NSA)

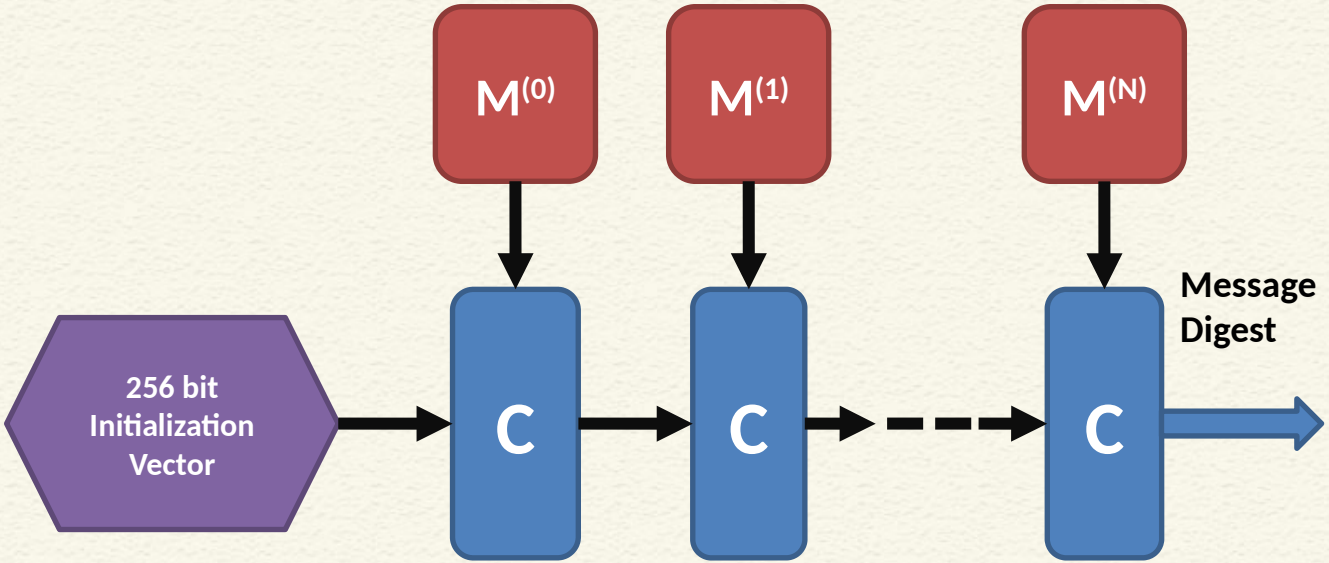
SHA256 Algorithm - Preprocessing

- Pad the message such that the message size is a multiple of 512
  - Suppose that the length of the message M is l; and $l \ mod$ 512≠0
  - Append the bit “1” at the end of the message
  - Append k zero bits, where k is the smallest non-negative solution to the equation l+1+k≡448 mod 512
  - Append the 64-bit block which is equal to the number l written in binary
  - **The total length gets divisible by 512**
- Partition the message into N 512-bit blocks , ,...,
- Every 512 bit block is further divided into 32 bit sub-blocks , ,...,

SHA-256 Algorithm

- The message blocks are processed one at a time
- Start with a fix initial hash value
- Sequentially compute ; is the SHA-256 *compression function* and + means mod addition. is the hash of .

SHA-256 Algorithm

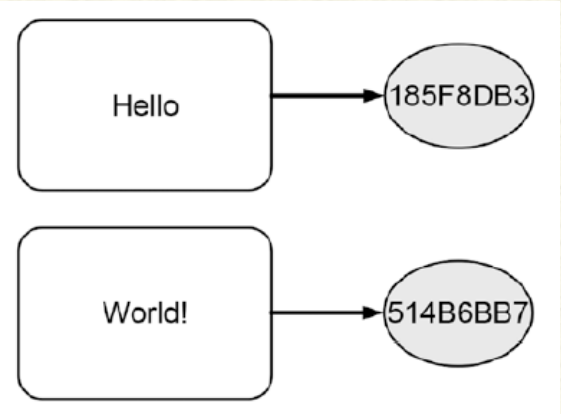


Patterns of Hashing Data

- Independent hashing
- Repeated hashing
- Combined hashing
- Sequential hashing
- Hierarchical hashing

Types of Hashing

- Independent hashing

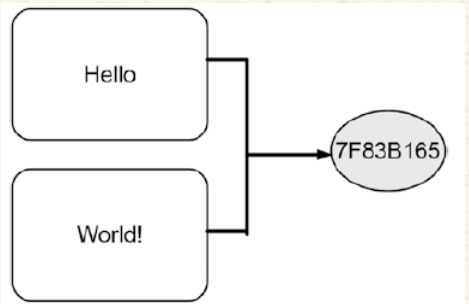


- Repeated hashing

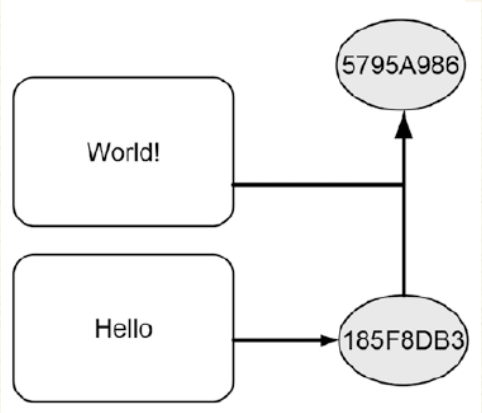
Courtesy: Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher

Types of Hashing

Combined hashing



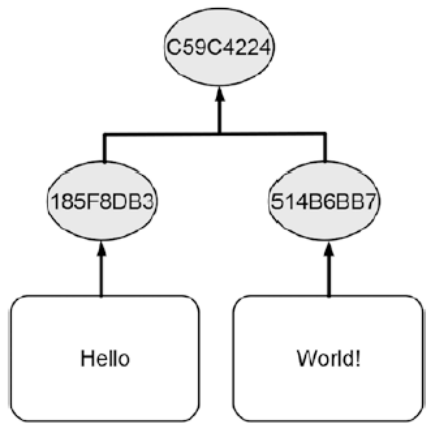
Sequential hashing



Courtesy: Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher

Types of Hashing

Hierarchical hashing



Illustration

http://www.blockchain-basics.com/HashFunctions.html

Courtesy: Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher

CONCLUSIONS

- Discussed implementation of hash functions
- Types of hashing

REFERENCES

- Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher, Apress (2017)
- Cryptography and Network Security – Principles and Practice by William Stallings, Pearson (2017)


Thank
you