Academic City University College, Accra, Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

33rd ECOWAS iSTEAMS ETech Multidisciplinary Conference (ECOWAS-ETech)

An Illustration on Hash Functions

Michael Kodjo Agorsah
School of Technology
E-mail: mkagorsah@gmail.com

ABSTRACT

A **hash function** is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but the output is always of fixed length. Values returned by a hash function are called the **message digest** or simply **hash values.** This treatise illustrates Hash Functions.

Keywords: Hash, Functions, Message, Digest, Outputs

Proceedings Citation Format
Michael Kodjo Agorsah (2022): An Illustration on Hash Functions. Proceedings of the 33rd ECOWAS iSTEAMS Emerging Technologies, Scientific, Business, Social Innovations & Cyber Space Ecosystem Multidisciplinary Conference. University of Ghana/Academic City University College, Ghana. 29th Sept – 1st Oct, 2022. Pp 131-132. www.isteams.net/ghanabespoke2022. dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P25

INTRODUCTION

Hash function converts data of arbitrary length to a fixed length. This process is often referred to as **hashing the data.** In general, the hash is much smaller than the input data, hence hash functions are sometimes called **compression functions.** Since a hash is a smaller representation of larger data, it is also referred to as a **digest.** Hash function with n bit output is referred to as an **n-bit hash function.** Popular hash functions generate values between 160 and 512 bits. Fig 1 illustrates hash functions.

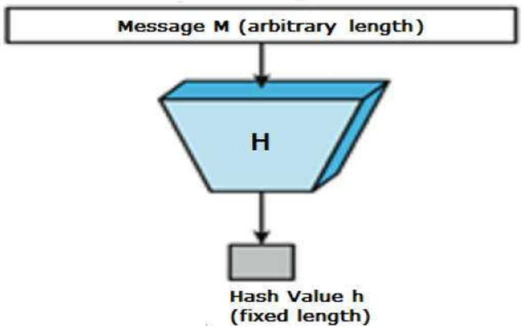

Fig 1: The typical features of hash functions: Fixed Length Output (Hash Value)

2. EFFICIENCY OF OPERATION

Generally, for any hash function h with input x, computation of h(x) is a fast operation. Computationally hash functions are much faster than symmetric encryption.

3. DESIGN OF HASHING ALGORITHMS

At the heart of hashing is a mathematical function that operates on two fixed-size blocks of data to create a hash code. This hash function forms part of the hashing algorithm. The size of each data block varies depending on the algorithm. Typically, the block sizes are from 128 bits to 512 bits. The following illustration demonstrates the hash function –

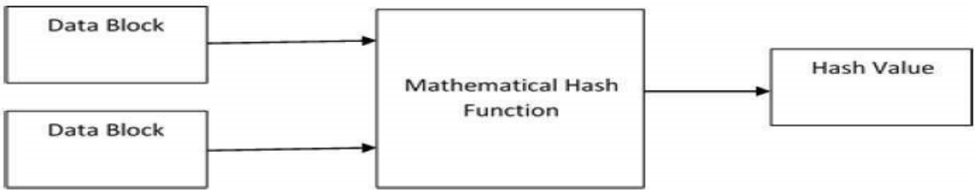

Fig 2: Mathematical Function That Operates On Two Fixed-Size Blocks

Hashing algorithm involves rounds of above hash function like a block cipher. Each round takes an input of a fixed size, typically a combination of the most recent message block and the output of the last round. This process is repeated for as many rounds as are required to hash the entire message. Schematic of hashing algorithm is depicted in the following illustration –

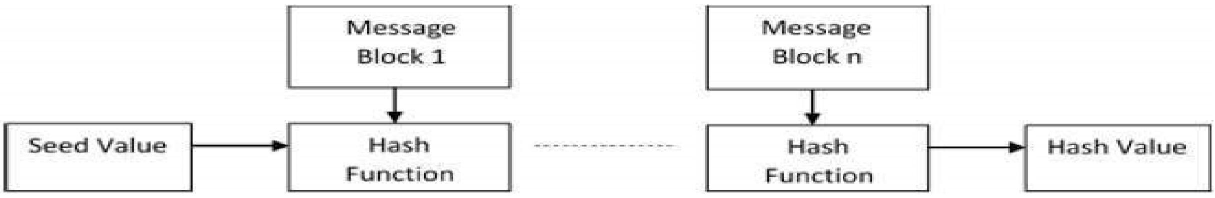

Fig 3: HASH Values

Since, the hash value of first message block becomes an input to the second hash operation, output of which alters the result of the third operation, and so on. This effect, known as an avalanche effect of hashing. Avalanche effect results in substantially different hash values for two messages that differ by even a single bit of data. Understand the difference between hash function and algorithm correctly. The hash function generates a hash code by operating on two blocks of fixed-length binary data. Hashing algorithm is a process for using the hash function, specifying how the message will be broken up and how the results from previous message blocks are chained together.

REFERENCE

1. Hash function - Wikipediahttps://en.wikipedia.org › wiki › Hash_function