Chapter 5
Hash Functions and Their Applications

Kannan Balasubramanian
Mepco Schlenk Engineering College, India

ABSTRACT

Cryptographic Hash Functions are used to achieve a number of Security goals like Message Authentication, Message Integrity, and are also used to implement Digital Signatures (Non-repudiation), and Entity Authentication. This chapter discusses the construction of hash functions and the various attacks on the Hash functions. The Message Authentication Codes are similar to the Hash functions except that they require a key for producing the message digest or hash.Authenticated Encryption is a scheme that combines hashing and Encryption. The Various types of hash functions like one-way hash function, Collision Resistant hash function and Universal hash functions are also discussed in this chapter.

INTRODUCTION

Cryptographic Hash functions are used to achieve a number of security objectives. In this chapter, we bring out the importance of hash functions and their variations, the design techniques and the attacks on them. Throughout the development of Cryptography and Cryptanalysis, confidentiality has taken the primary position and it was believed that if privacy is maintained (using symmetric encryption and secret key) then the authentication will automatically be achieved. Cryptographic Hash Functions are used to achieve a number of Security Goals like Message Authentication, Message Integrity, and are also used to implement Digital Signatures (Non-repudiation), Entity Authentication and steganography. Considerable research has undergone in the field of Cryptographic Hash Functions. Hash Functions can be generated from existing primitives like the Block ciphers (Baretto et al., 2003), as well as being explicitly and specially constructed from scratch as in the MD-4 and MD-5 hash functions (Rivest, 1992a, 1992b) and the family of SHA hash functions. (FIPS 180, FIPS 180-1, FIPS 180-2 and FIPS 180-3 standard of NIST).
CRYPTOGRAPHIC HASH FUNCTIONS

Cryptographic Hash functions are one of the most important tools in the field of cryptography and are used to achieve a number of security goals like authenticity, digital signatures, pseudo number generation, digital steganography, digital time stamping and other security goals. The following definition of hash functions is due to Rompay (2004).

- **Hash Function**: A hash function is a function $h: D \rightarrow R$, where the domain $D = \{0,1\}^*$ and $R = \{0,1\}^n$ for some $n \geq 1$.

Cryptographic Hash Functions are broadly of two types i.e. Keyed Hash functions; the ones that use a secret key, and Unkeyed Hash Functions; the other ones which do not use a secret key. The keyed Hash functions are referred to as Message Authentication codes (MAC). Generally, the term hash functions refer to unkeyed hash functions only. Unkeyed or simply Hash functions (some time also known as MDC – Manipulation Detection Codes) can further be classified into OWHF (One Way Hash Functions), CRHF (Collision Resistant Hash Functions) and UOWHF (Universal One Way Hash Functions) depending on the additional properties they satisfy.

- **One Way Hash Functions (OWHF)**: One Way Hash Function as defined by Merkle (1979) is a hash function $H$ that satisfies the following requirements:
  1. $H$ can be applied to block of data of any length. (In practice, ‘any length’ may be actually be bounded by some huge constant, larger than any message we ever would want to hash).
  2. $H$ produces a fixed-length output.
  3. Given $H$ and $x$ (any given input), it is easy to computer message digest $H(x)$.
  4. Given $H$ and $H(x)$, it is computationally infeasible to find $x$.
  5. Given $H$ and $H(x)$, it is computationally infeasible to find $x$ and $x'$ such that $H(x) = H(x')$.

The first three requirements are a must for practical applications of a hash function to message authentication and digital signatures. The fourth requirement also known as pre-image resistance or one way property, states that it is easy generate a message code given a message but hard (virtually impossible) to generate a message given a code (Sobti et al., 2012). The fifth requirement also known as Second pre-image resistance guarantees that an alternative message hashing to the same code as a given message cannot be found.

- **Collision Resistant Hash Functions (CRHF)**: A Collision Resistant Hash Function (Merkle, 1979), may be defined as a Hash function $H$, that satisfies all the requirements 1 through 5 of OWHF and in addition satisfy the following collision resistance property:

  Given $H$, it is computationally infeasible to find a pair $(x, y)$ such that $H(x) = H(y)$

- **Universal One Way Hash Functions (UOWHF)**: The Security property of a Universal One Way Hash Functions as described in Naor et al (1989) is defined as follows: