4.4 HASH FUNCTION

- A hash function maps a variable-length message into a fixed-length hash value, or message digest.
- Virtually all cryptographic hash functions involve the iterative use of a compression function.
- The compression function used in secure hash algorithms falls into one of two categories: a function specifically designed for the hash function or an algorithm based on a symmetric block cipher. SHA and Whirlpool are examples of these two approaches, respectively.
- A hash function H accepts a variable-length block of data as input and produces a fixed- size hash value .
- A "good" hash function has the property that the results of applying the function to a large set of inputs will produce outputs that are evenly distributed and apparently random. In general terms, the principal object of a hash function is data integrity.
- A change to any bit or bits in results, with high probability, in a change to the hash code. The kind of hash function needed for security applications is referred to as a cryptographic hash function.
- A cryptographic hash function is an algorithm for which it is computationally infeasible (because no attack is significantly more efficient than brute force) to find either (a) a data object that maps to a pre-specified hash result (the one-way property) or (b) two data objects that map to the same hash result (the collision-free property).
- Because of these characteristics, hash functions are often used to determine whether or not data has changed

BLACK DIAGRAM OF CRYPTOGRAPHIC HASH FUNCTION

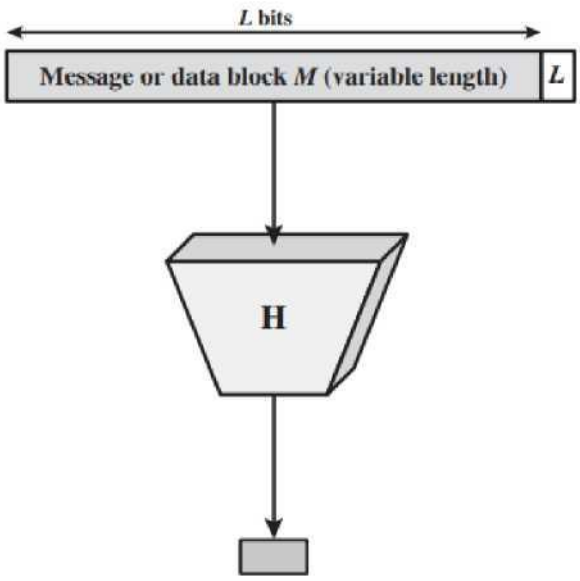


Figure 11.1 Black Diagram of Cryptographic Hash Function; $h = H(M)$

Reference :William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006

APPLICATIONS OF CRYPTOGRAPHIC HASH FUNCTIONS

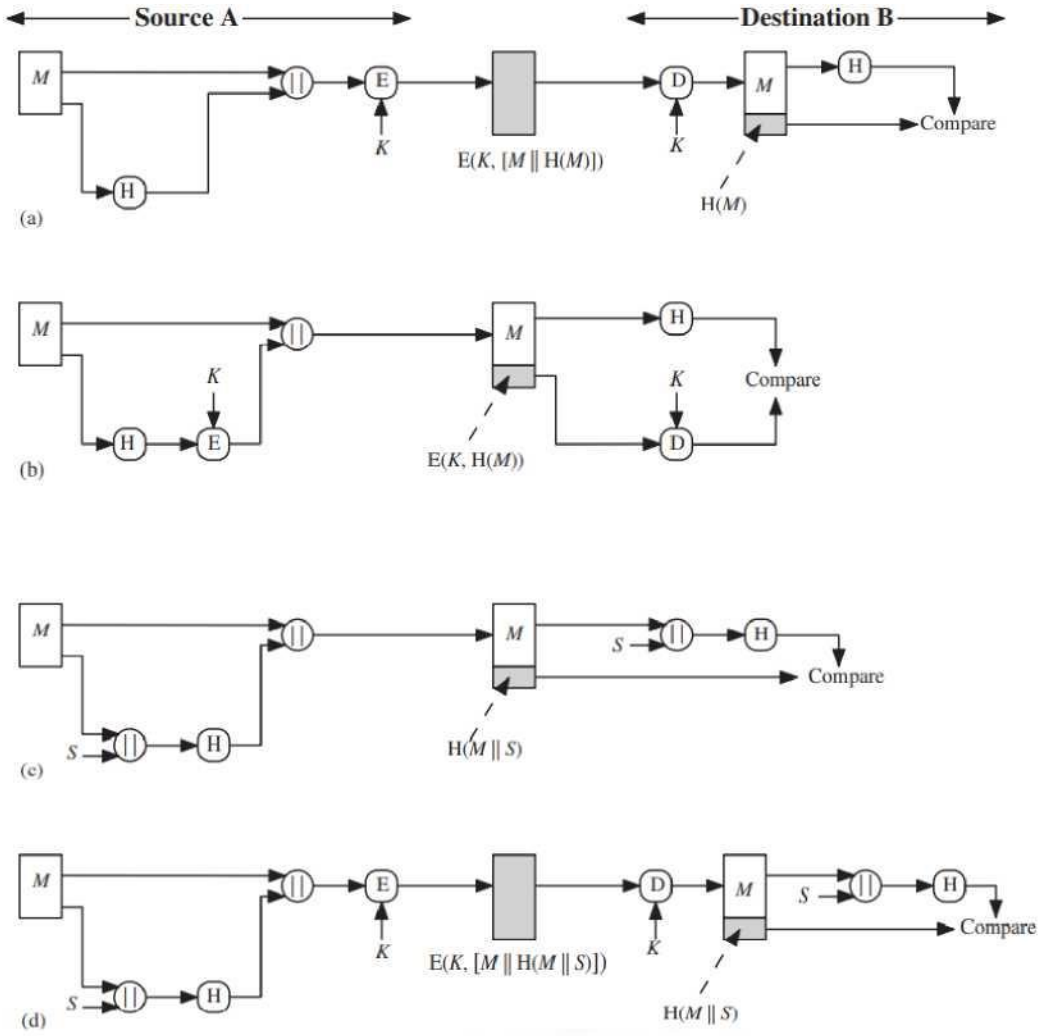
- Message Authentication
- Digital Signatures
- Other Applications
    - to create a one-way password file
    - intrusion detection and virus detection

to construct a pseudorandom function (PRF) or a pseudorandom number generator (PRNG)

MESSAGE AUTHENTICATION

- Message authentication is a mechanism or service used to verify the integrity of a message. Message authentication assures that data received are exactly as sent (i.e., contain no modification, insertion, deletion, or replay).
- When a hash function is used to provide message authentication, the hash function value is often referred to as a message digest

SIMPLIFIED EXAMPLES OF THE USE OF A HASH FUNCTION FOR MESSAGE AUTHENTICATION



Reference :William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006