1. A one-way hash function, also known as a message digest, fingerprint or compression function, is a mathematical function which takes a variable-length input string and converts it into a fixed-length binary sequence.
2. Furthermore, a one-way hash function is designed in such a way that it is hard to reverse the process, that is, to find a string that hashes to a given value (hence the name one-way.) A good hash function also makes it hard to find two strings that would produce the same hash value.
3. All modern hash algorithms produce hash values of 128 bits and higher.
4. Even a slight change in an input string should cause the hash value to change drastically. Even if 1 bit is flipped in the input string, at least half of the bits in the hash value will flip as a result. This is called an avalanche effect.
5. Since it is computationally infeasible to produce a document that would hash to a given value or find two documents that hash to the same value, a document's hash can serve as a cryptographic equivalent of the document.
6. This makes a one-way hash function a central notion in public-key cryptography. When producing a digital signature for a document, we no longer need to encrypt the entire document with a sender's private key (which can be extremely slow).
7. It is sufficient to encrypt the document's hash value instead.
8. Although a one-way hash function is used mostly for generating digital signatures, it can have other practical applications as well, such as secure password storage, file identification and message authentication code (MAC).

One-way cryptographic hash function

The ideal cryptographic hash function has four main properties

- It is easy to compute the hash value for any given message.
- It is infeasible to generate a message that has a given hash.

- It is infeasible to modify a message without changing the hash.
- It is infeasible to find two different messages with the same hash

Ex: MD5, SHA-1, etc.

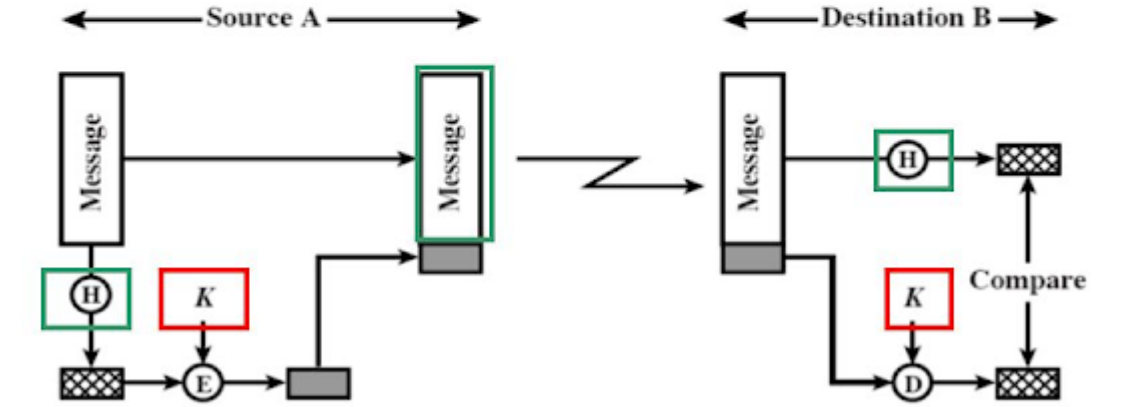
One-Way Hash Functions

Given a message, M, of arbitrary length a hash function produces a short, fixed-length block that is unique to M ("fingerprint")

A hash function is a component of a MAC system.

It is not the complete system because a hash itself does not involve any secret information.

Figure 3.2 shows three ways to use hash functions in producing a MAC.



(a) Using conventional encryption

8

Hash Algorithms:

Some examples of hash algorithms: MD4, MD5, SHA and SHA256.

MD4 & M5

Both MD4 andMD5 were invented by Ron Rivest. MD stands for Message Digest. Both algorithms produce 128-bit hash values. MD5 is an improved version of MD4.

SHA

SHA stands for Secure Hash Algorithm. It was designed by NIST and NSA. SHA produces 160-bit hash values, longer than MD4 and MD5. SHA is generally considered more secure that other algorithms and is the recommended hash algorithm.

SHA256

SHA256 is a 256-bit modern version of SHA and is only supported by the Microsoft Enhanced RSA and AES Cryptographic Provider.

Applications of One Way Hash Functions

1. Message authentication: used to check if a message has been modified.
2. Digital signatures: encrypt digest with private key.
3. Password storage: digest of password is compared with that in the storage; hackers cannot get password from storage.
4. Key generation: key can be generated from digest of pass-phrase; can be made computationally expensive to prevent brute-force attacks.
5. Pseudorandom number generation: iterated hashing of a seed value.
6. Intrusion detection and virus detection: keep and check hash of files on system

Related posts:

1. Types of Attack
2. Security threats
3. Computer and cyber security
4. Introduction to network security
5. Intrusion detection tool
6. Categories of security assessments
7. Security terminologies and principals
8. Intoduction to intrusion
9. Intrusion detection tool
10. Categories of security assessments
11. Intrusion terminology
12. Cryptography attacks
13. Cryptography
14. SSH
15. MD5
16. Message digest functions
17. Digital signature
18. Authentication Functions
19. Hash function in network web security
20. Digital signature standard
21. SSL Secure socket layer