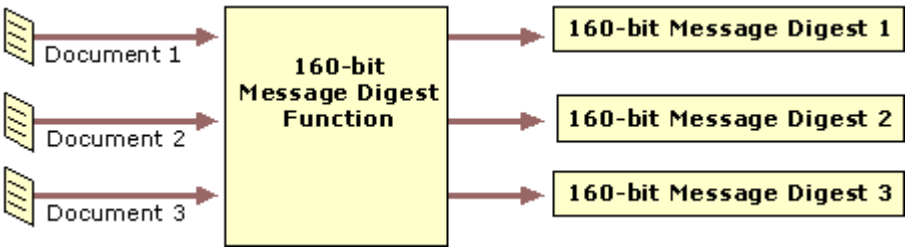
Message digest functions also called hash functions, are used to produce digital summaries of information called message digests.

Message digests (also called hashes) are commonly 128 bits to 160 bits in length and provide a digital identifier for each digital file or document.

Message digest functions are mathematical functions that process information to produce a different message digest for each unique document.



The basic message digest process

For example, to provide data integrity for e-mail messages, message digests can be generated from the completed mail message, digitally signed with the originator's private key.

The recipient of the message can then do the following to check the integrity of the message:

- Use the same message digest function to compute a digest for the message.
- Use the originator's public key to verify the signed message digest.
- Compare the new message digest to the original digest.

Uses of Message Digest Functions:

Message digest functions are widely used today for a number of reasons:

- Message digest functions are much faster to calculate than traditional symmetric key cryptographic functions but appear to share many of their strong cryptographic properties.
- There are no patent restrictions on any message digest functions that are currently in use.
- There are no exports or import restrictions on message digest functions.

Attacks of message difgest functions:

There are two kinds of attacks on message digest functions.

1. The first is finding two messages, any two message, that have the same message digest.
2. The second attack is significantly harder. Given a particular message, the attacker finds a second message that has the same message digest code.

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. Digital signature
17. Authentication Functions
18. One way hash function
19. Hash function in network web security
20. Digital signature standard
21. SSL Secure socket layer