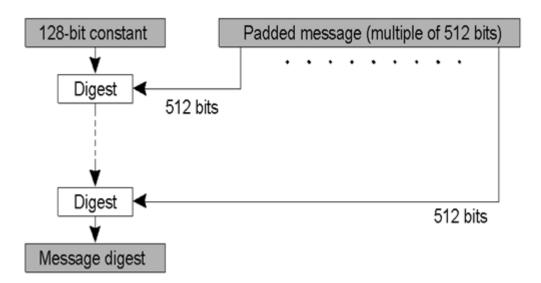
MD5 algorithm was developed by Professor Ronald L. Rivest in 1991. According to RFC 1321, "MD5 message-digest algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input.

The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA."



MD5 algorithm structure

General steps:

- 1. Input message must be < 264 bits
- 2. Not really a problem.
- 3. Message is processed in 512-bit blocks sequentially
- 4. Message digest is 160 bits

MD5 Algorithms steps:

Step1: Padding

Step2: Appending length as 64 bit unsigned

Step3: Initialize MD buffer 5 32-bit words

Store in big endian format, most significant bit in low address

A|B|C|D|E

A = 67452301

B = efcdab89

C = 98badcfe

D = 10325476

E = c3d2e1f0

Step 4: the 80-step processing of 512-bit blocks - 4 rounds, 20 steps each.

Each step t (0 \leq t \leq 79):

Input:

Wt. - a 32-bit word from the message

Kt - a constant.

ABCDE: current MD.

Output:

ABCDE: new MD.

Only 4 per-round distinctive additive constants

$$0 <= t <= 19 \text{ Kt} = 5A827999$$

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. Message digest functions
- 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