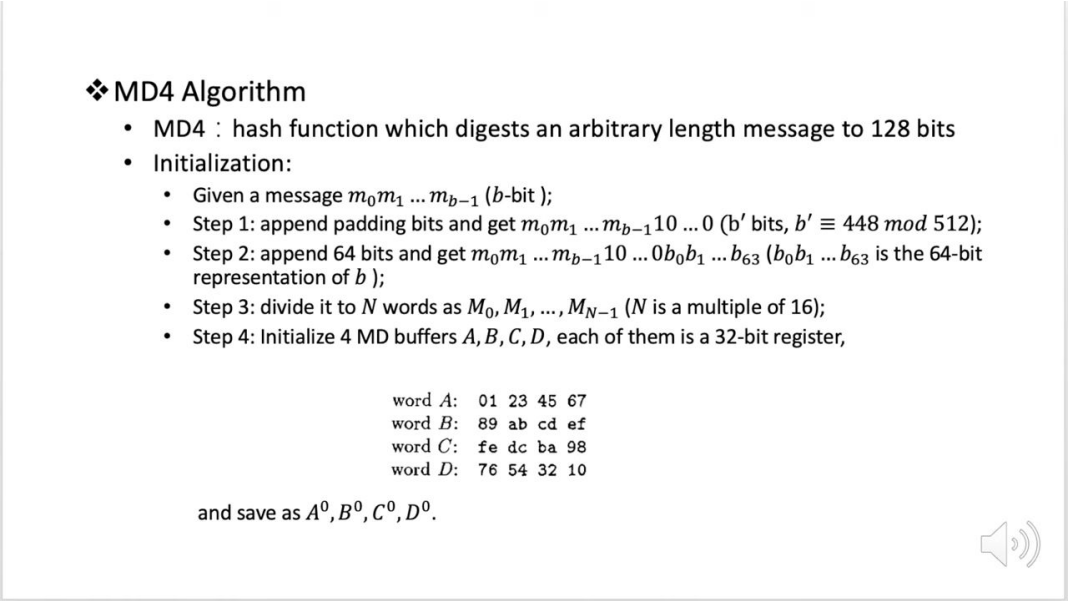
View, add and edit your notes in the app

Hash Function: MD4

Generated on December 19, 2023

Summary

Notes	Screenshots	Bookmarks
0	2	0

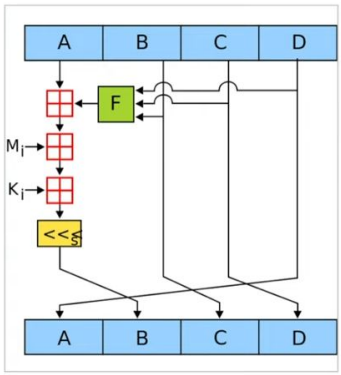


MD4 algorithm, developed by Renault drivers in 1990, is a hash function that digests arbitrary length messages into fixed length bit values.

0:05

- Processing 48 rounds
  - 16 rounds
    - $F(B, C, D) = BC \vee (\neg B)D$
    - $i = 0, 1, \ldots, 15$
    - $K_i = 0$
    - $s = 3, 7, 11, 19, 3, 7, 11, 19, 3, 7, 11, 19$
  - 16 rounds
    - $F(B, C, D) = BC \vee BD \vee CD$
    - $i = 0, 4, 8, 12, 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 15$
    - $K_i = 5A827999$
    - $s = 3, 5, 9, 13, 3, 5, 9, 13, 3, 5, 9, 13, 3, 5, 9, 13$
  - 16 rounds
    - $F(B, C, D) = B \oplus C \oplus D$
    - $i = 0, 8, 4, 12, 2, 10, 6, 14, 1, 9, 5, 13, 3, 11, 7, 15$
    - $K_i = 6ED9EBA1$
    - $s = 3, 9, 11, 15, 3, 9, 11, 15, 3, 9, 11, 15, 3, 9, 11, 15$
- Compute
  - $A = A + A^0$
  - $B = B + B^0$
  - $C = C + C^0$
  - $D = D + D^0$

and output $A\ B\ C\ D$ as the result



A new method using buffers for message processing will require 48 rounds of processing, consisting of 16 runs of 3.

3:13