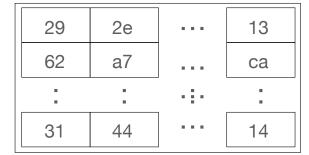
One step in the MD2 cryptographic hash (C array)

- "Confusion" by mixing message information with random numbers from the S-box
- "Diffusion" by value in current position in hash selecting S-box number for next message position such that confused information cascades and a change anywhere in message affects all locations by repeated passes through the message.

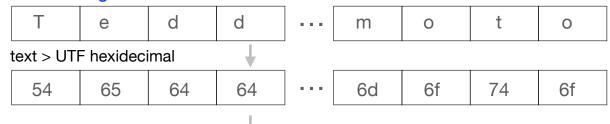
Substitution S-box (hexadecimal values)



value from element number hex c1 of S-box is hex ec

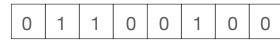
S-box is array of 256 elements, each containing a **randomly** placed, non-repeating value in decimal range 0-255

The message



info for step 4

binary values



XOR (bitwise exclusive OR)

0

0



0

0

select value from element number hex c1 of S-box same concepts in more secure ways: random "round constants" in SHA-256, mixing by XOR & other operations, diffusion by bit shift.

Modern algorithms use the

info from step 3 for step 4

The hash being computed

a5 ec

0

info from step 4 for step 5

MD2 hash length is 32 hex = 16 each, 8-bit bytes = 128 bits, regardless of length of message, and maintained at this length by **MODULAR ARITHMETIC**

github.com/RichardHerz

Page 3 of 9

www.ReactorLab.net