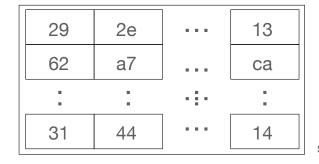
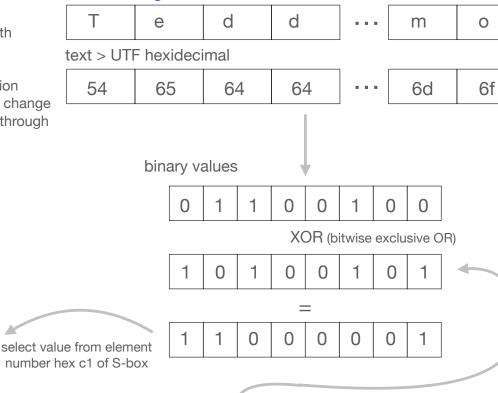


- "Confusion" by mixing message information with random numbers from the S-box
- "Diffusion" by value in current position in hash selecting S-box number for next message position such that confused information cascades and a change anywhere in message affects all hash locations through repeated passes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

## Substitution S-box (hexadecimal values)



## The message



this message value is mixed with **random** value from S-box in hash from previous iteration, selected by operation with previous message value

t

74

0

6f

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

a5 ec

The hash being computed

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

MD2 hash length is 32 hex char = 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