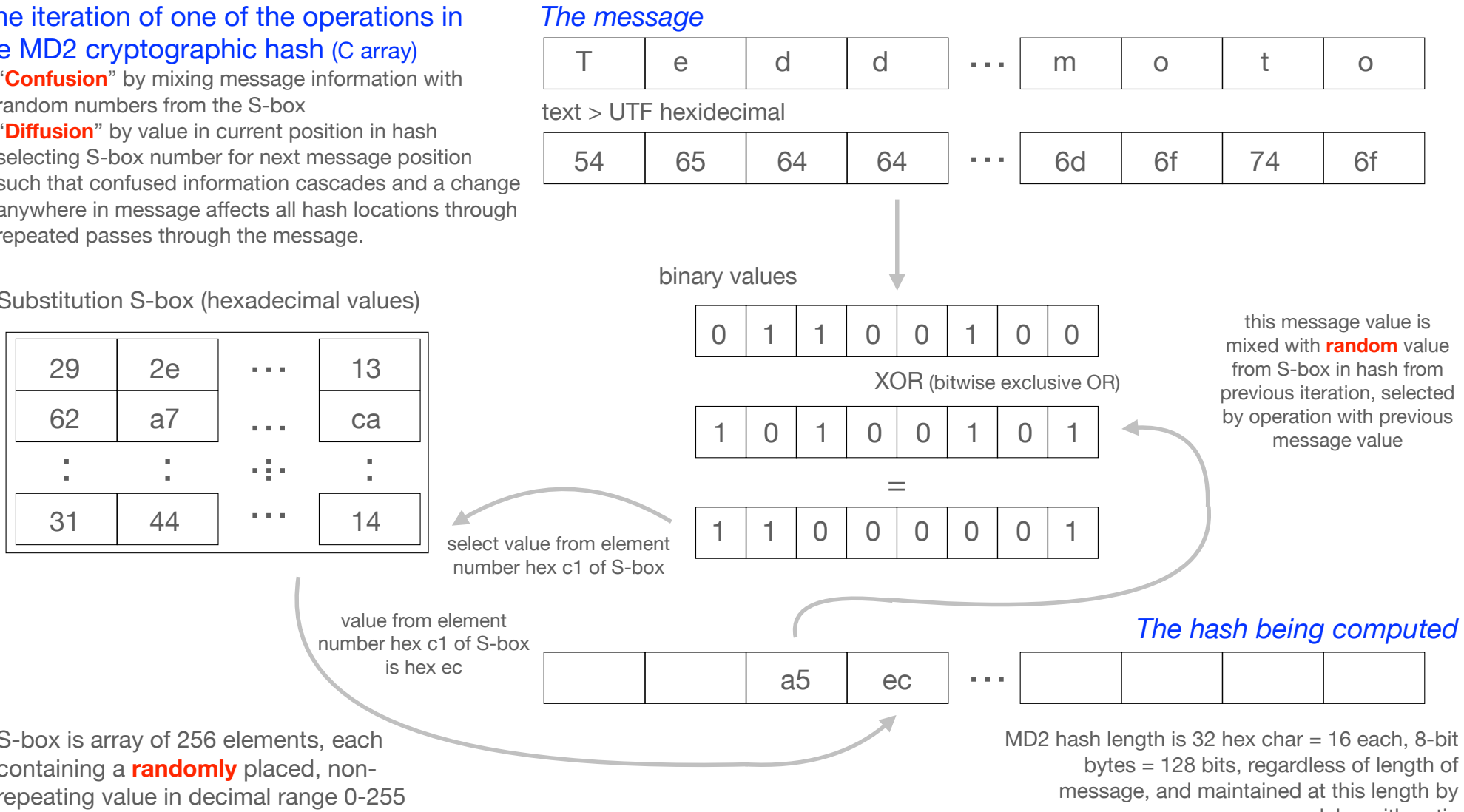
One iteration of one of the operations in the MD2 cryptographic hash (C array)

- "**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 hash locations through repeated passes through the message.



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