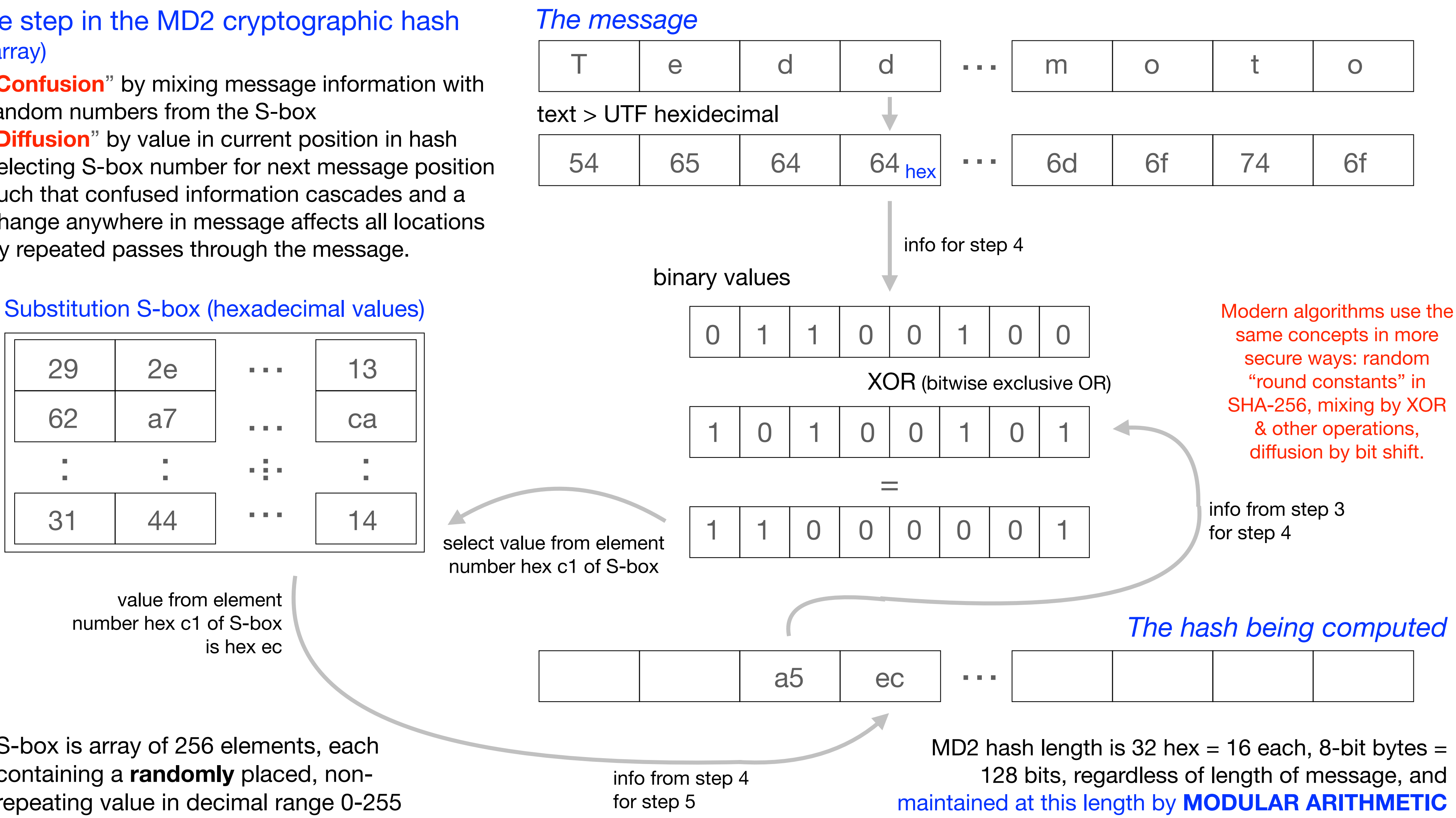
One step in the MD2 cryptographic hash
(C array)

- “**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.



The message

T	e	d	d	···	m	o	t	o

text > UTF hexidecimal

54	65	64	64 hex	···	6d	6f	74	6f

info for step 4

binary values

0	1	1	0	0	1	0	0

XOR (bitwise exclusive OR)

1	0	1	0	0	1	0	1

=

1	1	0	0	0	0	0	1

Modern algorithms use the same concepts in more secure ways: random “round constants” in SHA-256, mixing by XOR & other operations, diffusion by bit shift.

Substitution S-box (hexadecimal values)

29	2e	···	13
62	a7	···	ca
:	:	⋮·⋮	:
31	44	···	14

select value from element number hex c1 of S-box

info from step 3 for step 4

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

The hash being computed

		a5	ec	···				

info from step 4 for step 5

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