

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.

Substitution S-box (hexadecimal values)

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

select value from element number hex c1 of S-box

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

T	e	d	d	...	m	o	t	o
---	---	---	---	-----	---	---	---	---

text > UTF hexadecimal

54	65	64	64	...	6d	6f	74	6f
----	----	----	----	-----	----	----	----	----

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
---	---	---	---	---	---	---	---

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

The hash being computed

		a5	ec	...				
--	--	----	----	-----	--	--	--	--

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