

Diagram illustrating the A2 operation on a 64-bit input C . The input C is divided into four 16-bit segments. The output $A2(C)$ is shown as a 64-bit result, with specific bytes highlighted in green, red, and blue to show the mapping from the input segments.

Input C (64 bits):

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

Output $A2(C)$ (64 bits):

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

Mapping (Green lines):

- Input segment 1 (bits 0-15) maps to output bytes 0-5.
- Input segment 2 (bits 16-31) maps to output bytes 16-21.
- Input segment 3 (bits 32-47) maps to output bytes 32-37.
- Input segment 4 (bits 48-63) maps to output bytes 48-53.

Highlighted output bytes (Green, Red, Blue):

- Green: 5, 16, 22, 32, 48, 53
- Red: 6, 19, 23, 33, 49
- Blue: 7, 20, 24, 34, 50