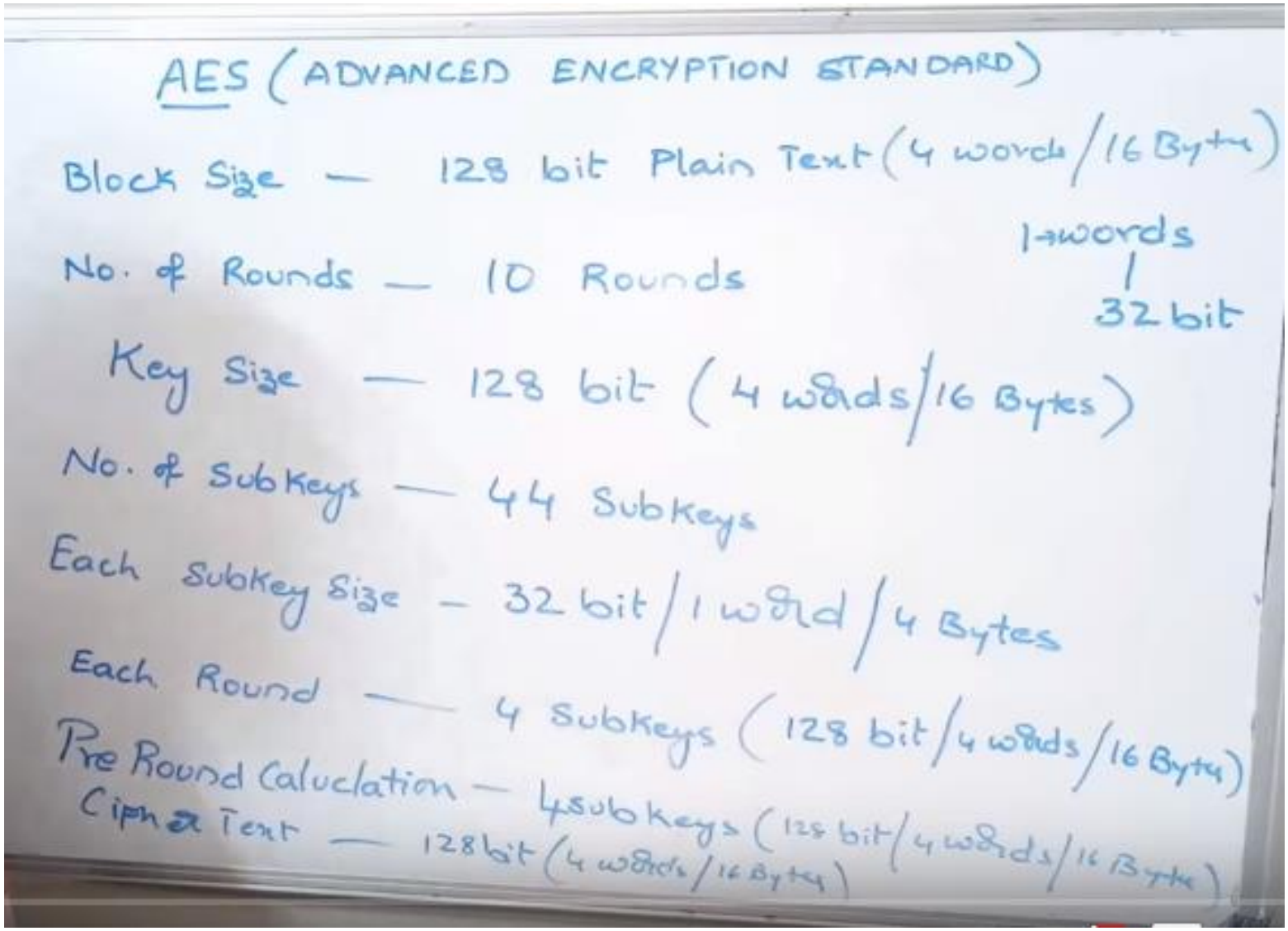
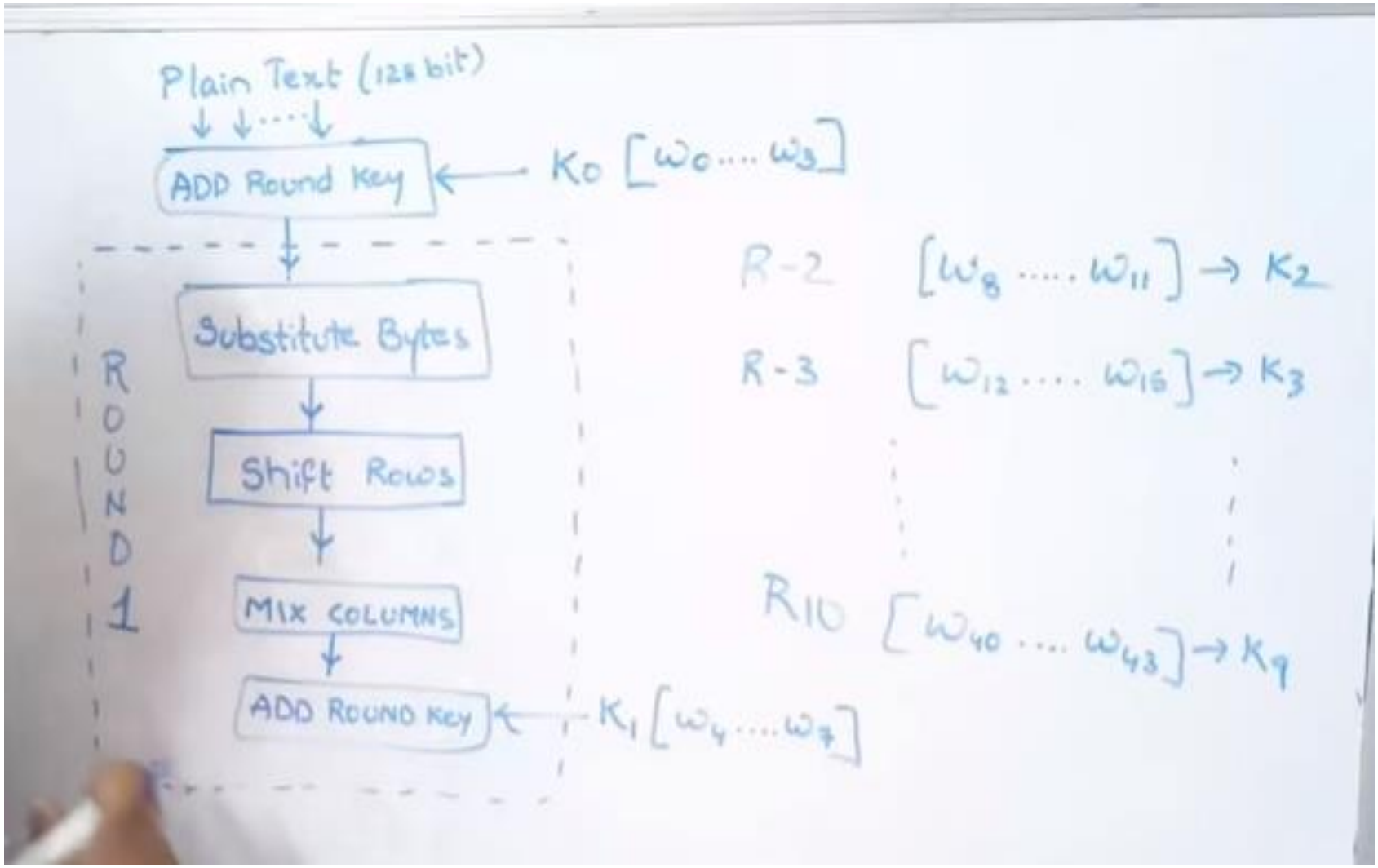
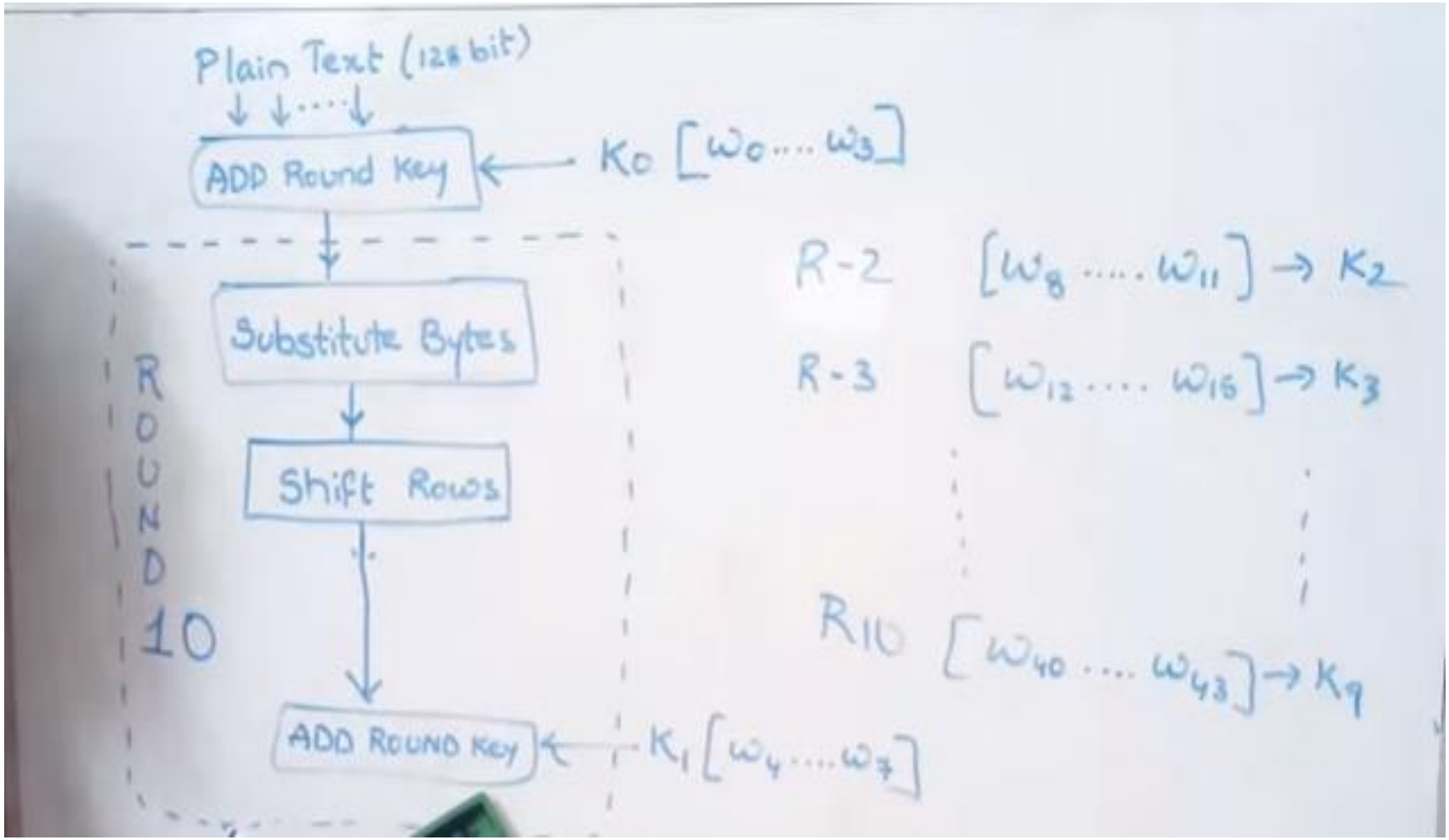
AES:


AES (ADVANCED ENCRYPTION STANDARD)
Block Size — 128 bit Plain Text (4 words / 16 Bytes)
No. of Rounds — 10 Rounds
1 word = 32 bit
Key Size — 128 bit (4 words / 16 Bytes)
No. of SubKeys — 44 SubKeys
Each SubKey Size — 32 bit / 1 word / 4 Bytes
Each Round — 4 SubKeys (128 bit / 4 words / 16 Bytes)
Pre Round Caluclation — 4 subkeys (128 bit / 4 words / 16 Bytes)
Cipher Text — 128 bit (4 words / 16 Bytes)

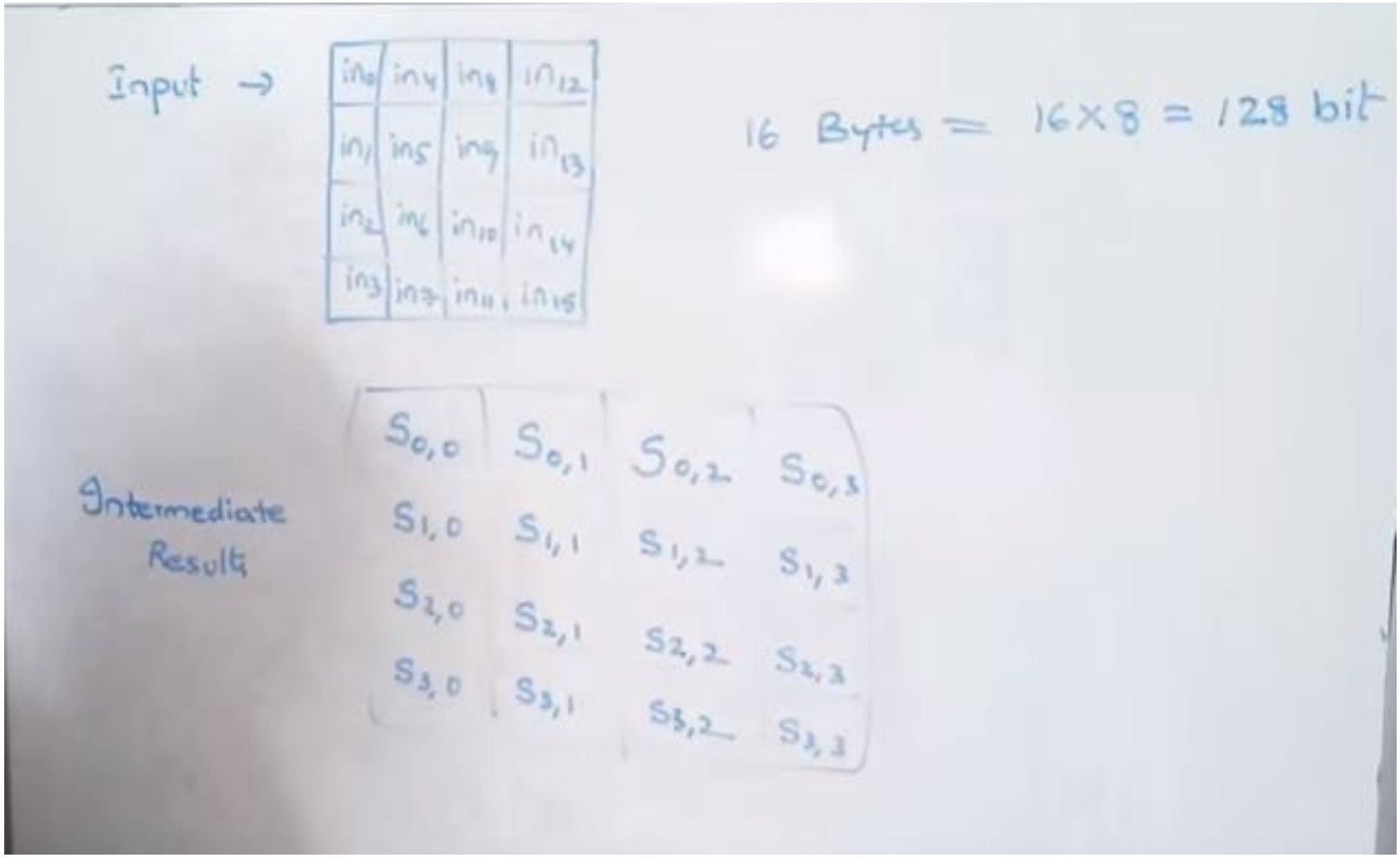
Single Round Function in AES:



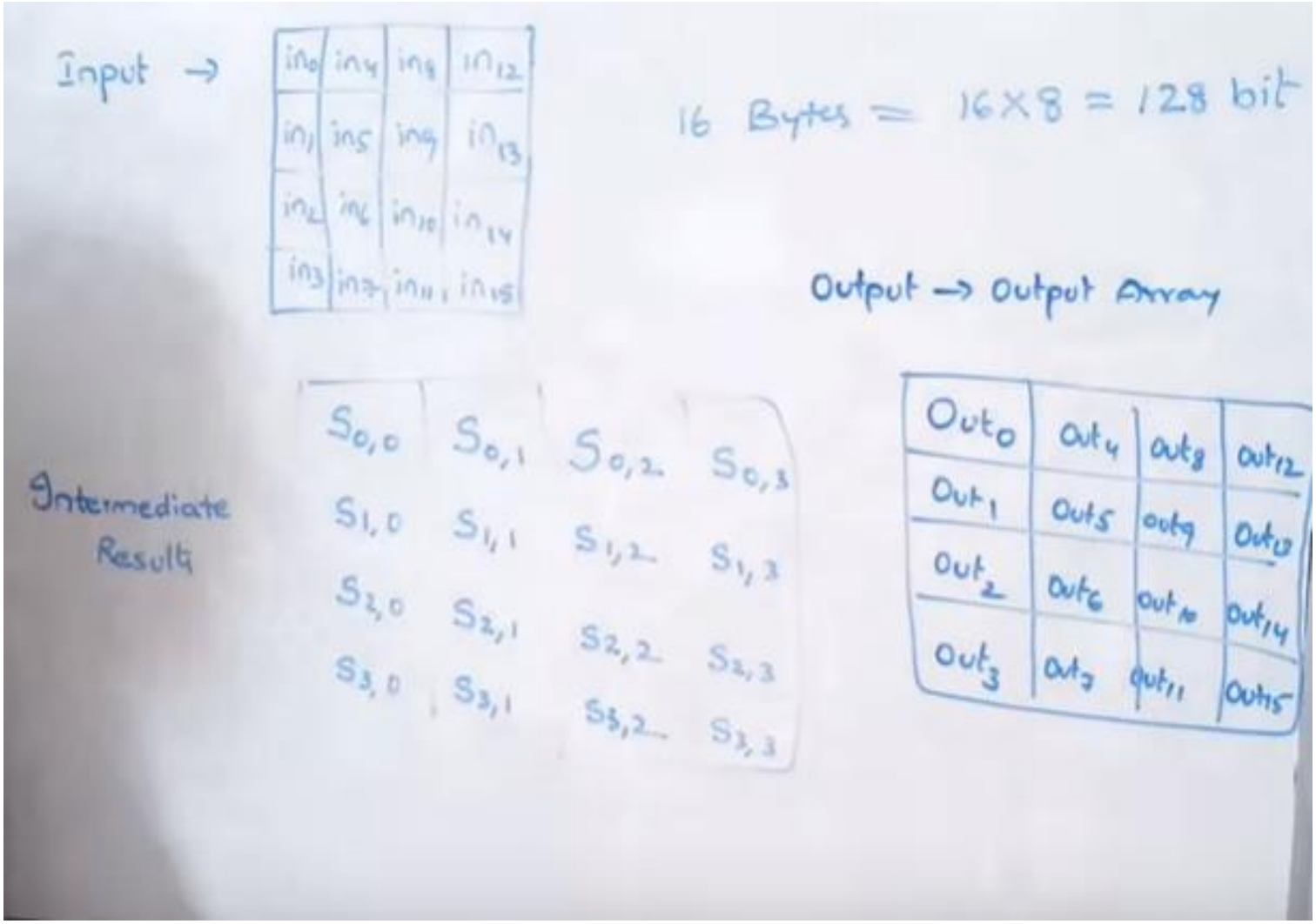
In Round 10, Need not Apply mix column



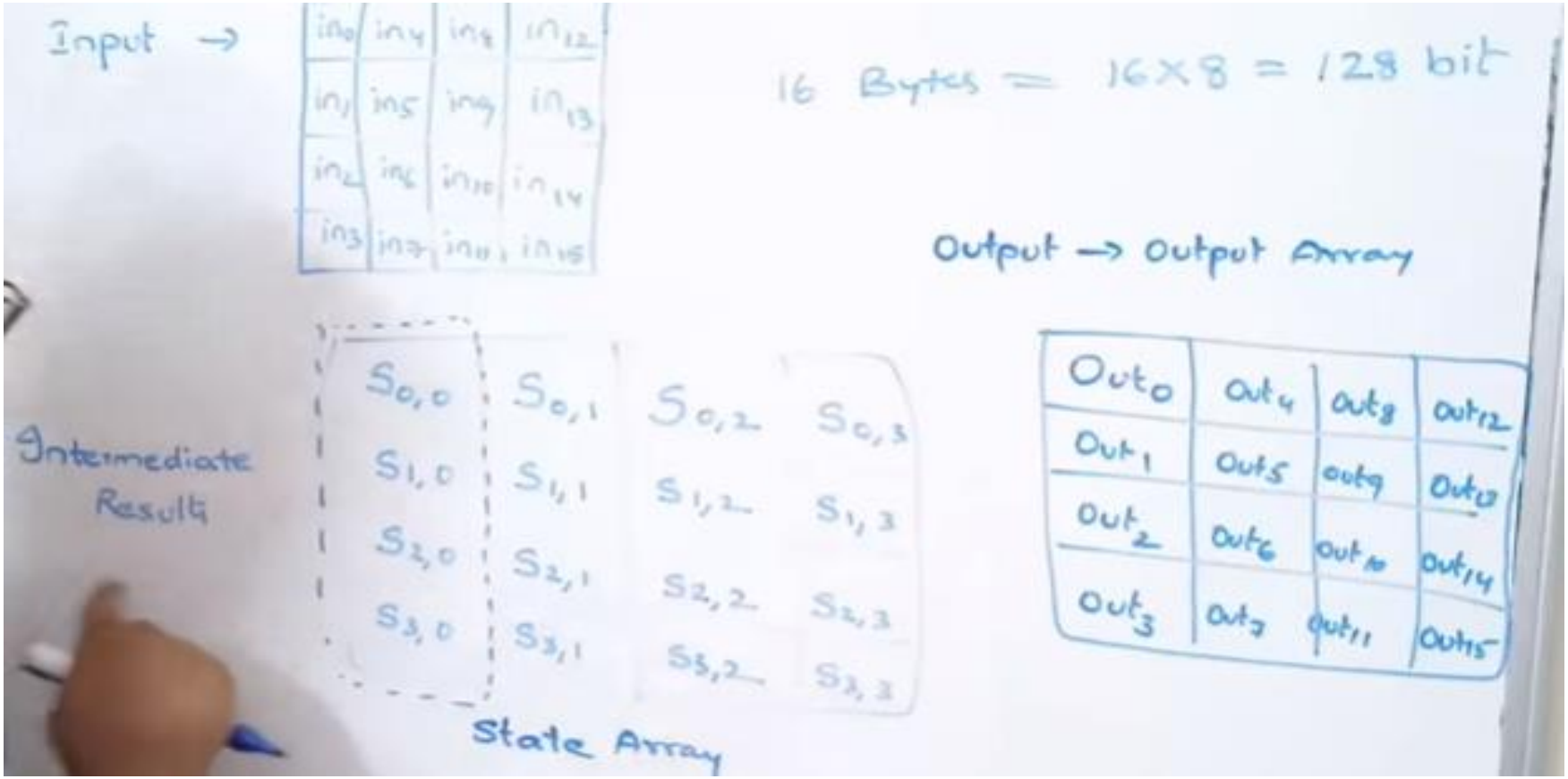
128 PT is represented in input array
4X4 matrix and intermediate results are stored in state array.



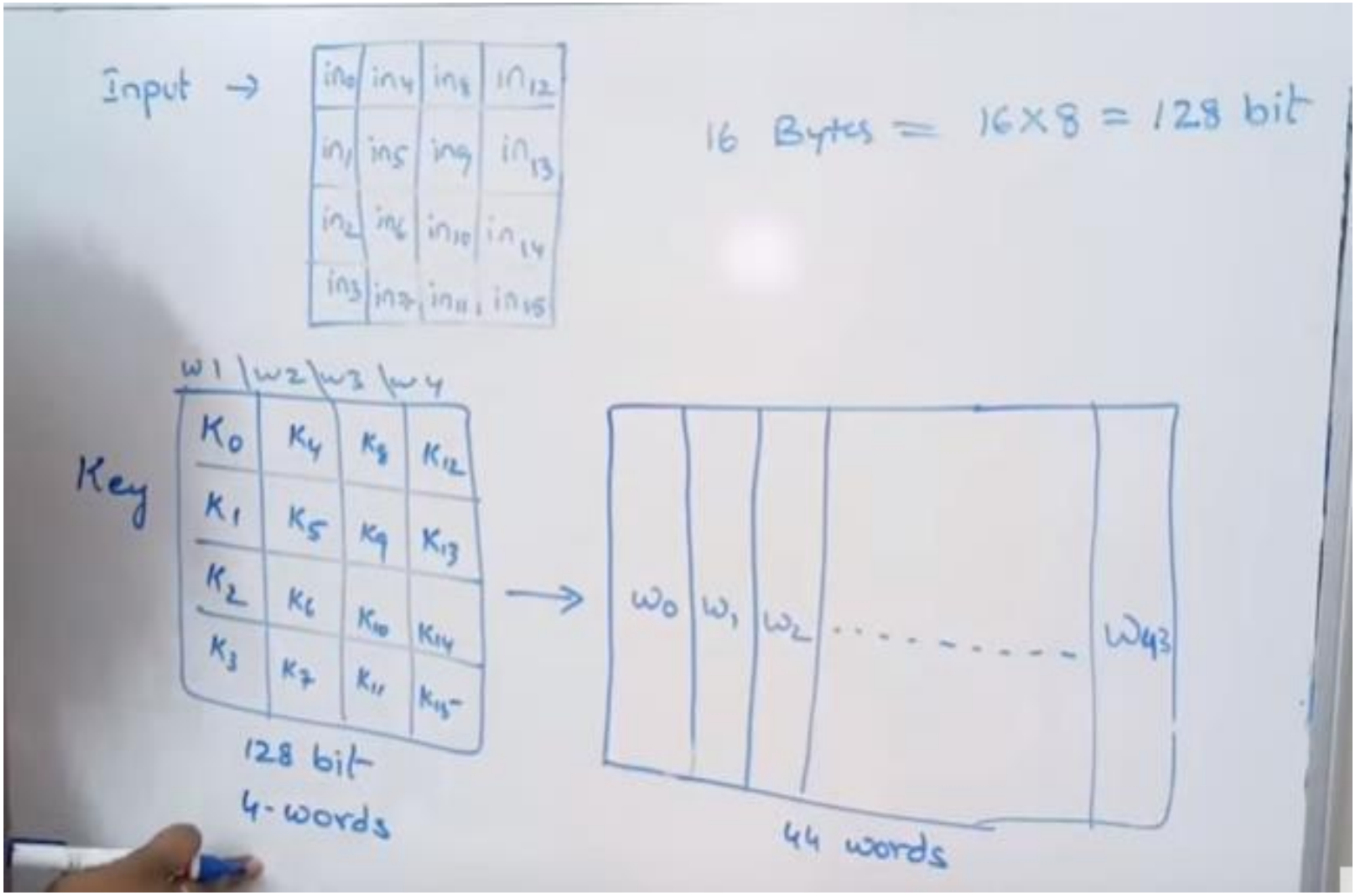
O/P is stored in O/P Array: 4x4

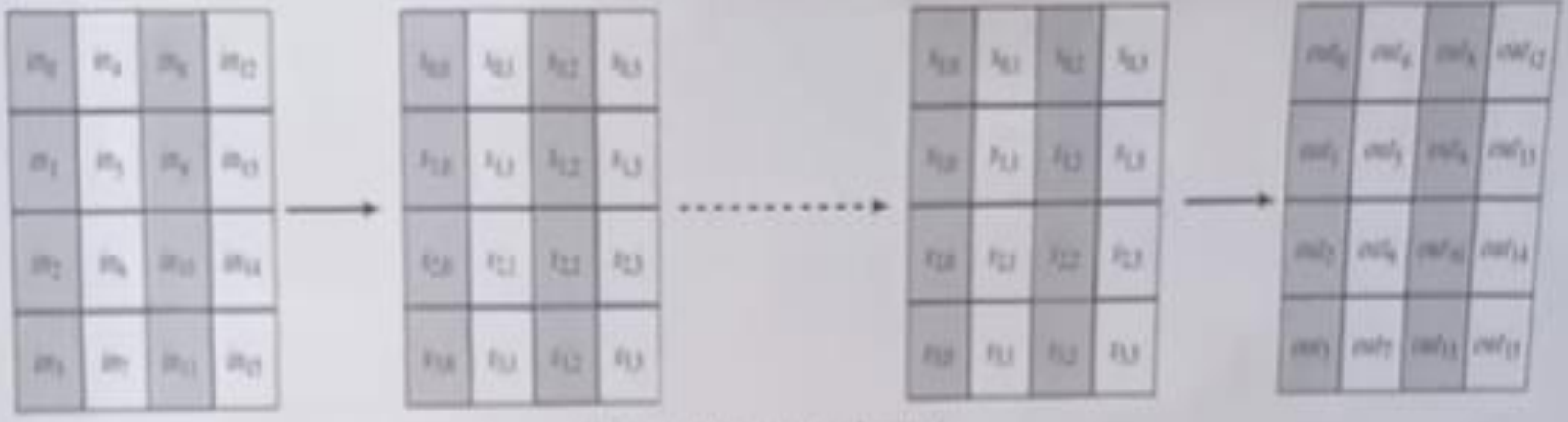


First column in state array is first word.
$S_{1,0}$ first Byte of zeroth **word (BxW)**

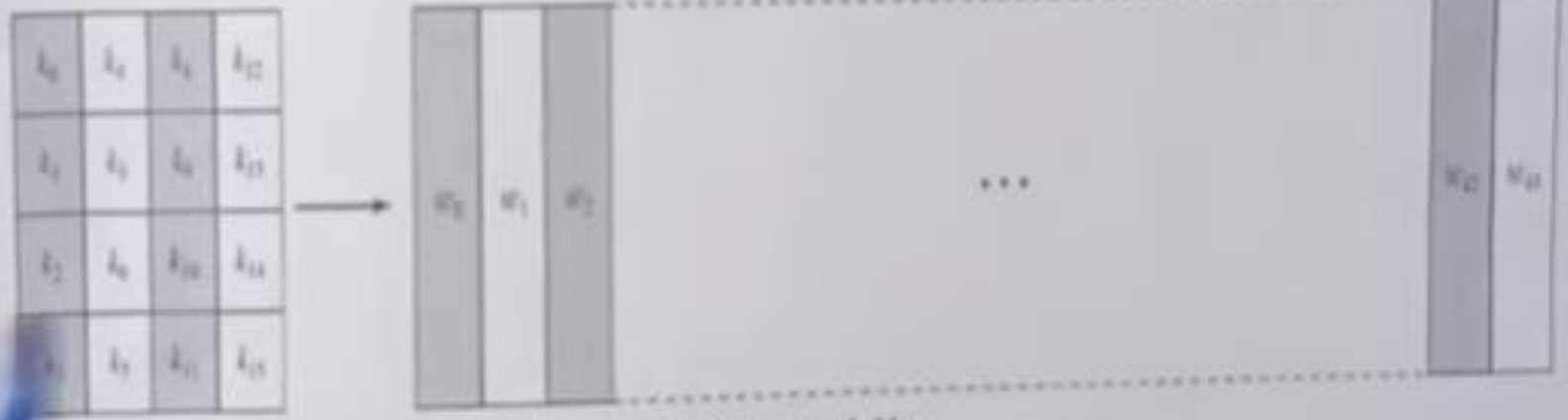


Key: 4 words expanded 44 words.

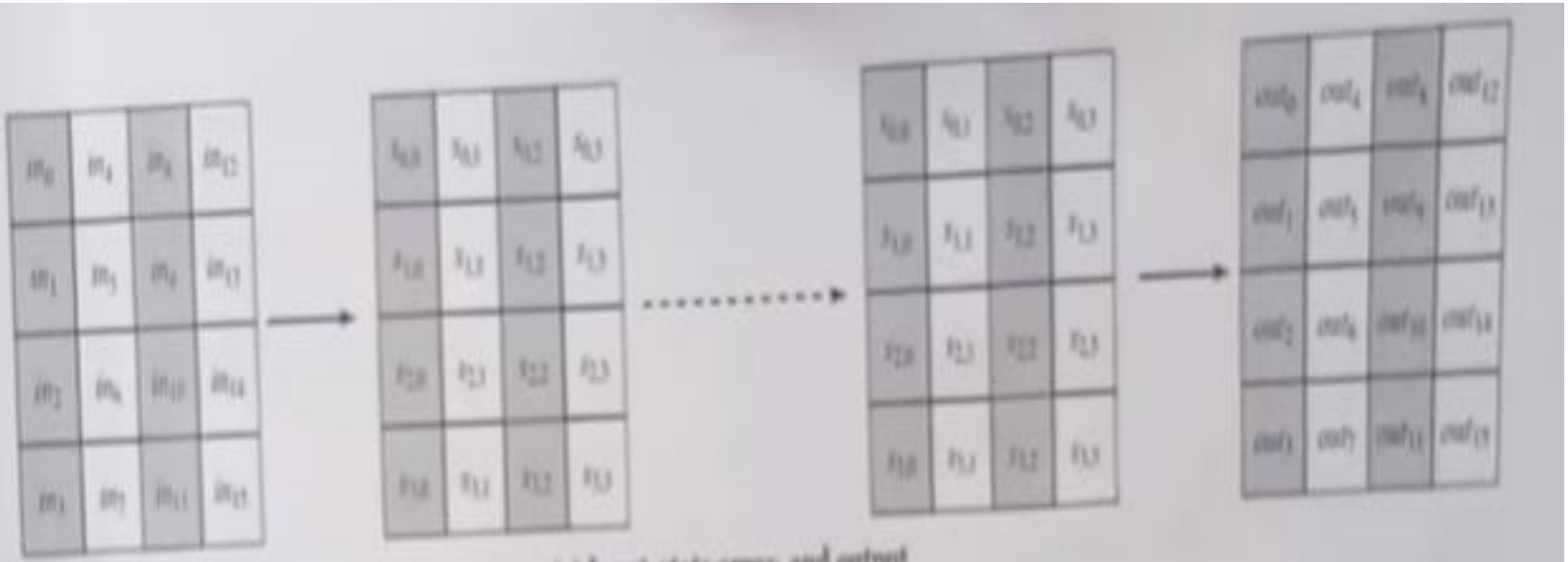




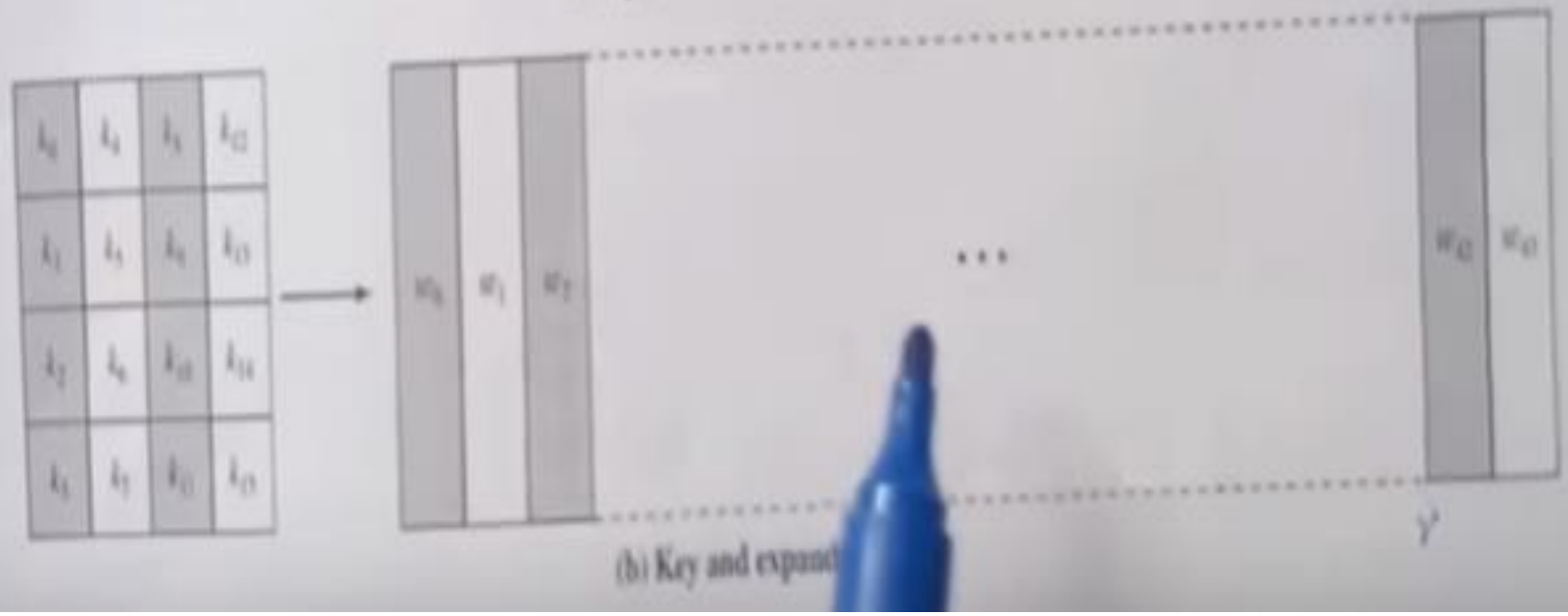
(a) Input, state array, and output



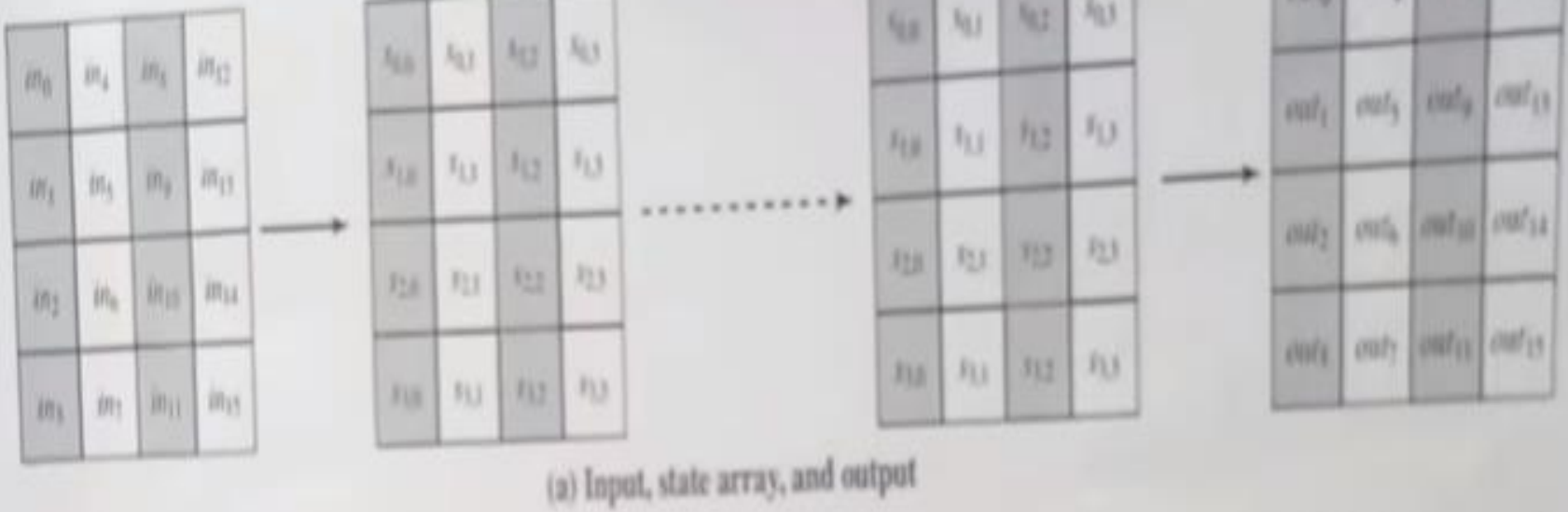
(b) Key and expanded key



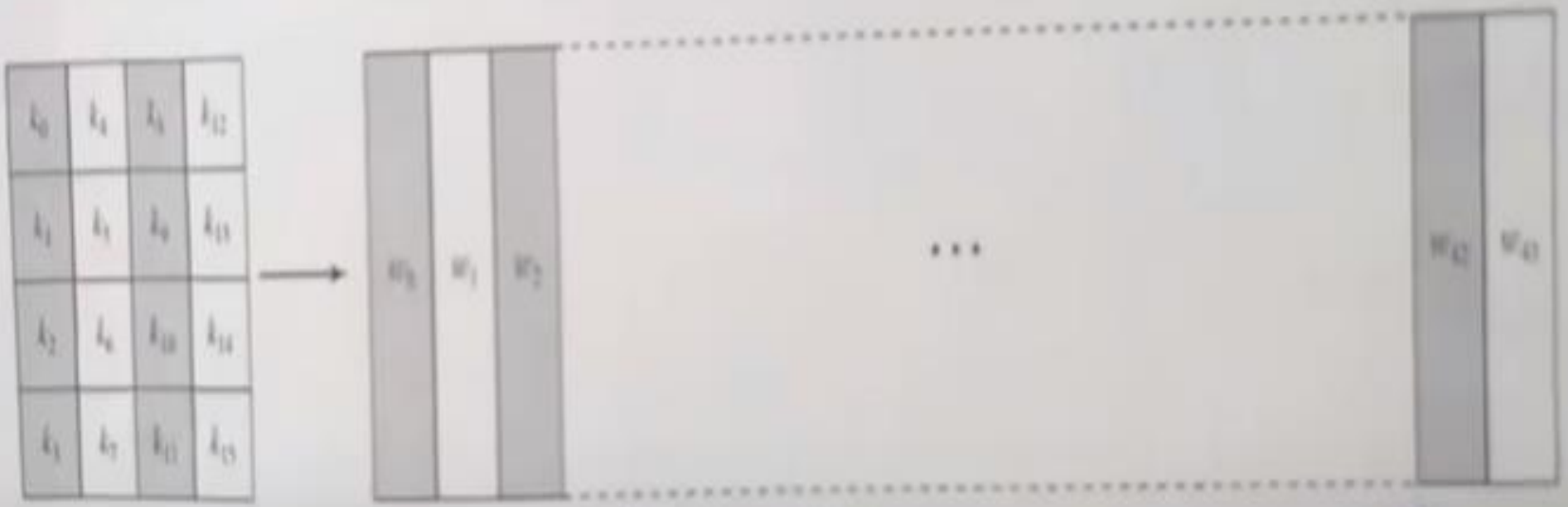
(a) Input, state array, and output



(b) Key and expans

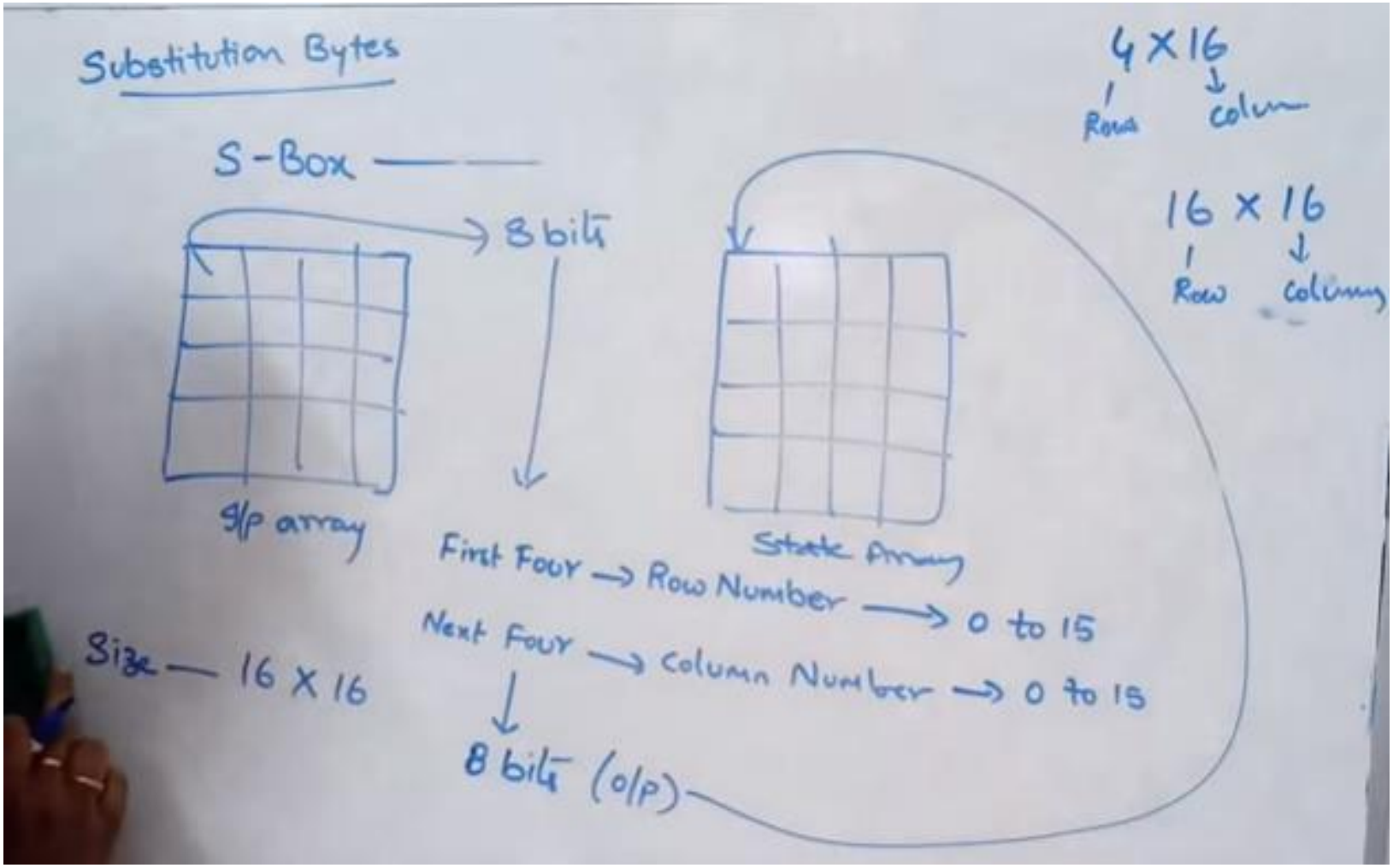


(a) Input, state array, and output

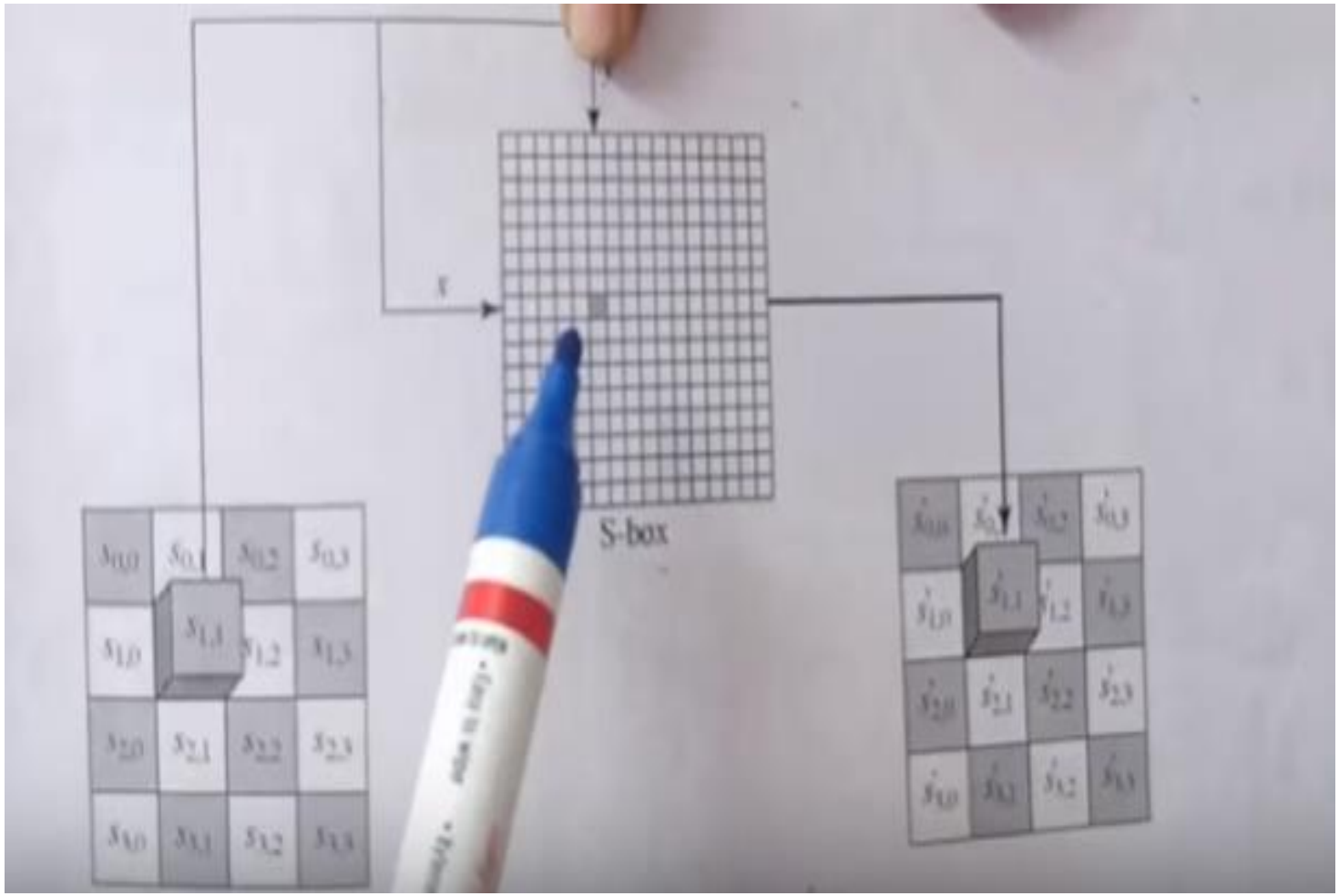


(b) Key and expanded key

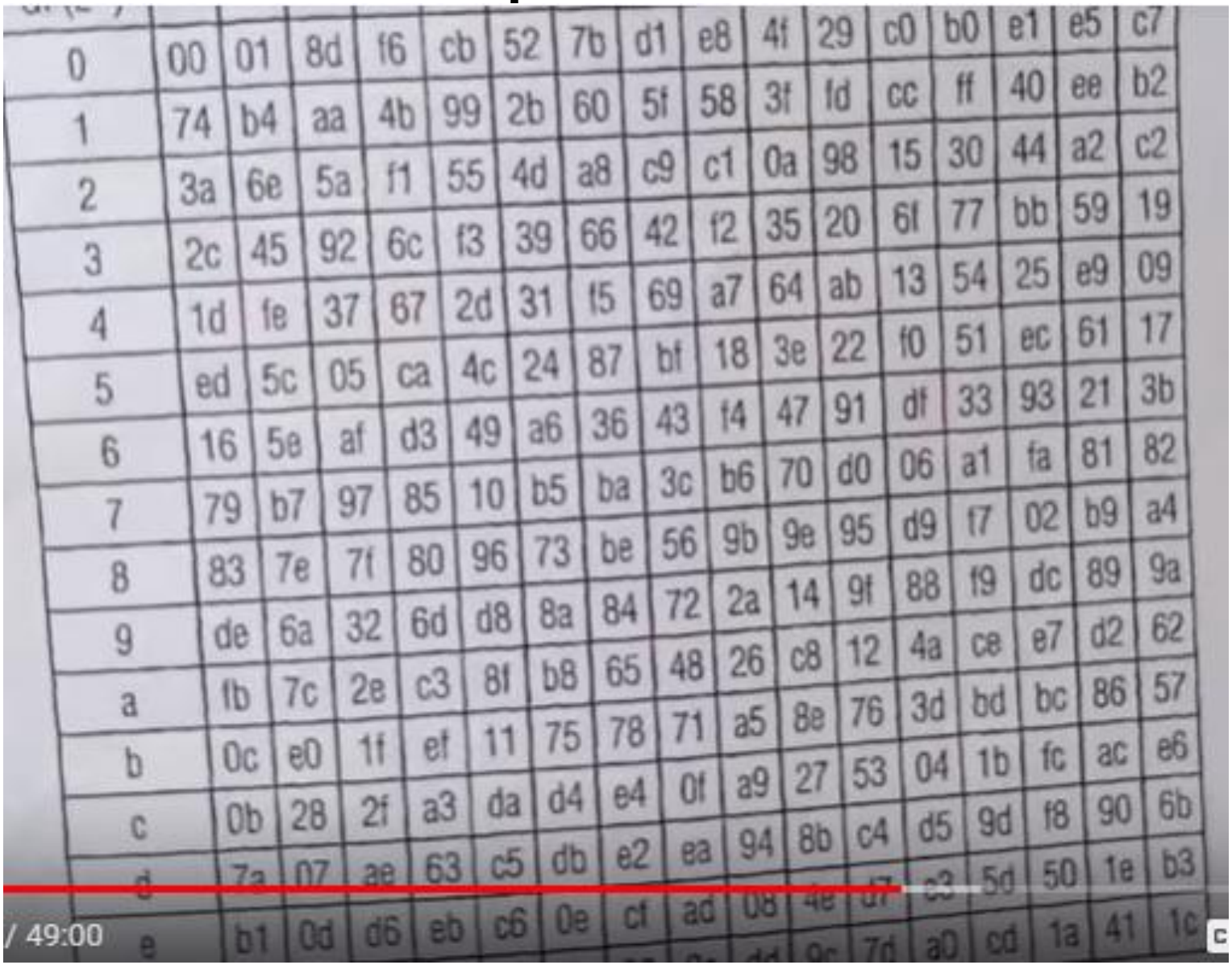
S-Box:


Substitution Bytes
4 X 16
Row
colum
S-Box
8 bits
16 X 16
Row
colum
I/P array
State Array
First Four → Row Number → 0 to 15
Next Four → Column Number → 0 to 15
Size — 16 X 16
8 bits (o/p)

S-box

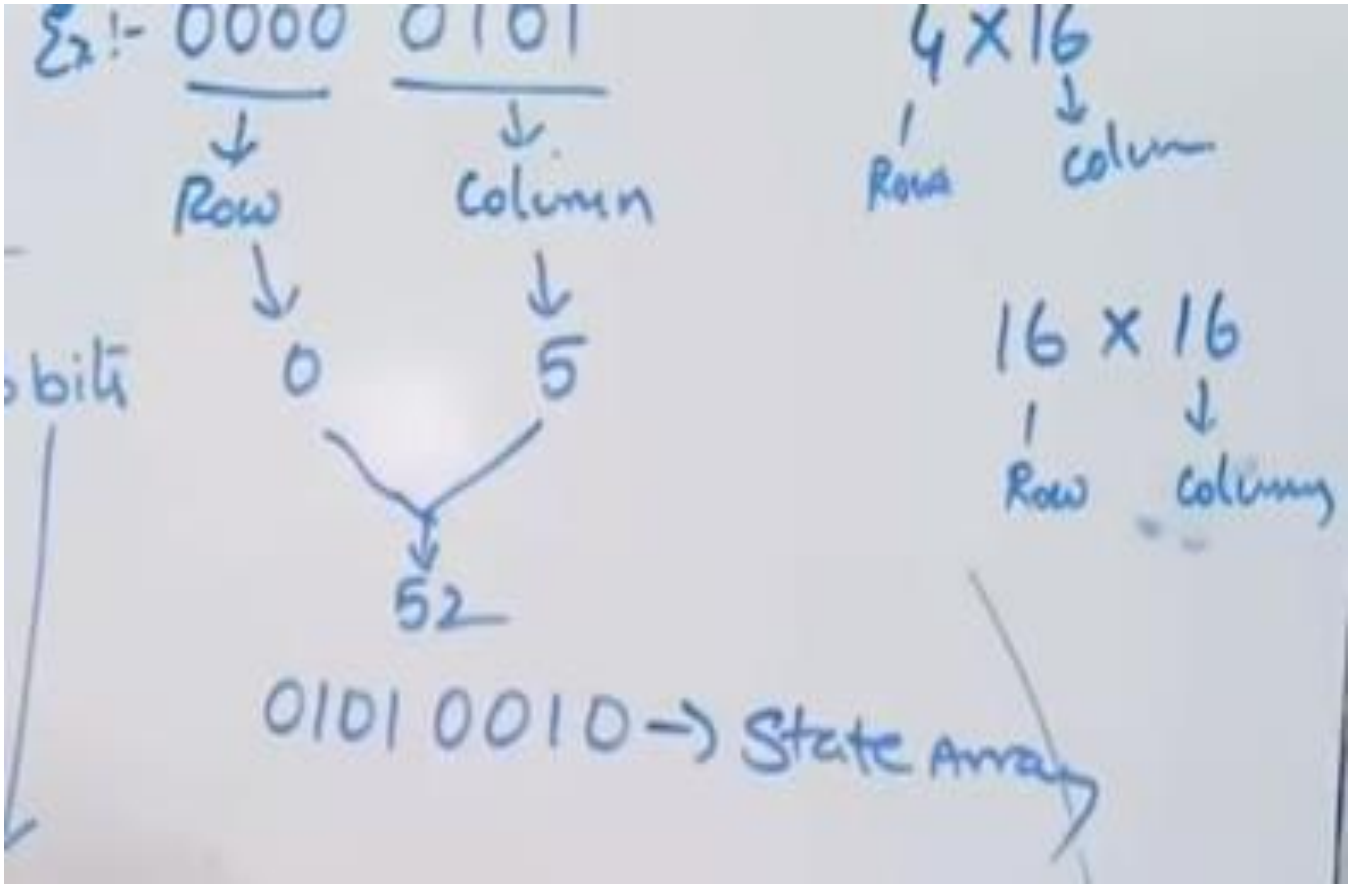


Sample S-box

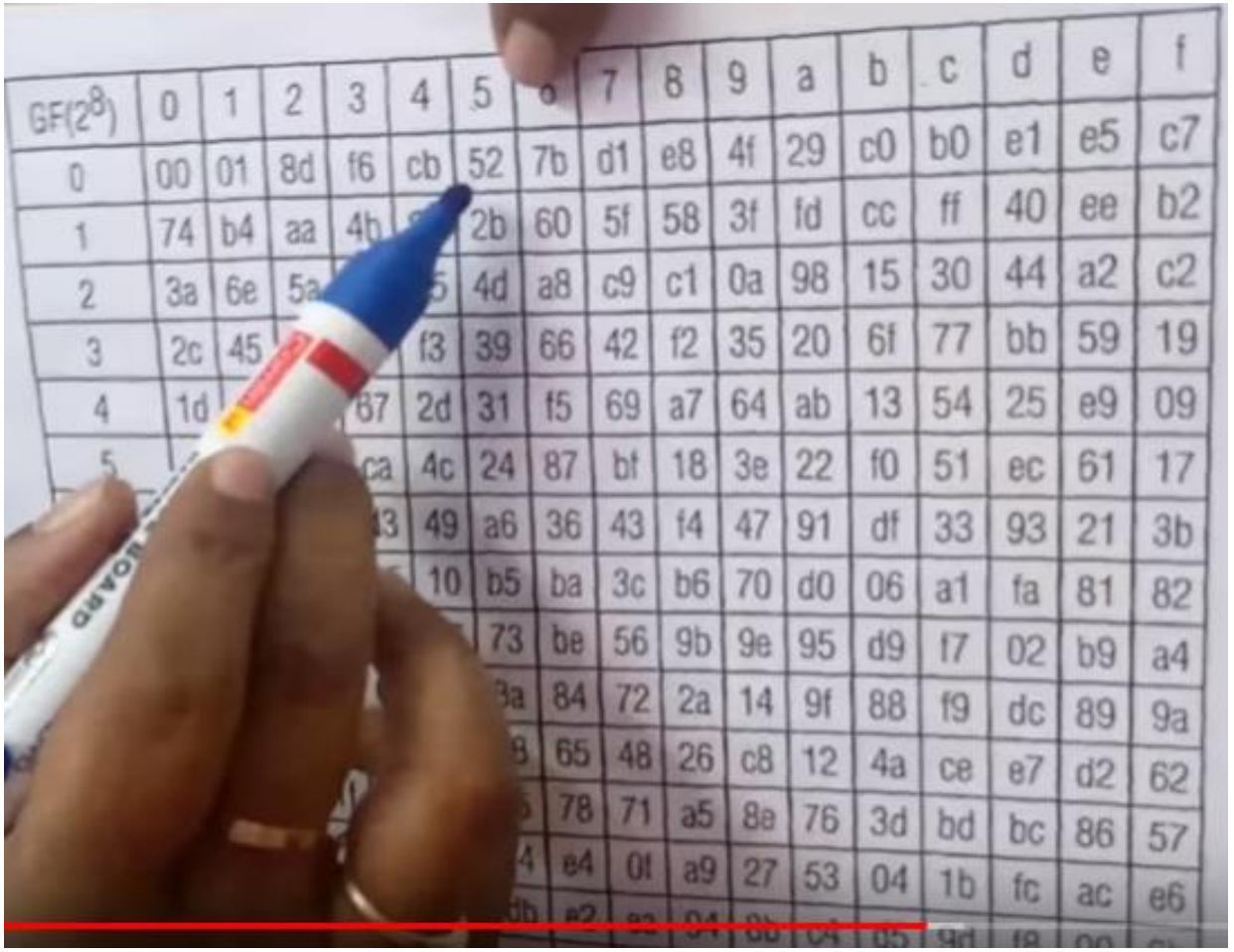


	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	00	01	8d	f6	cb	52	7b	d1	e8	4f	29	c0	b0	e1	e5	c7
1	74	b4	aa	4b	99	2b	60	5f	58	3f	fd	cc	ff	40	ee	b2
2	3a	6e	5a	f1	55	4d	a8	c9	c1	0a	98	15	30	44	a2	c2
3	2c	45	92	6c	f3	39	66	42	f2	35	20	6f	77	bb	59	19
4	1d	fe	37	67	2d	31	f5	69	a7	64	ab	13	54	25	e9	09
5	ed	5c	05	ca	4c	24	87	bf	18	3e	22	f0	51	ec	61	17
6	16	5e	af	d3	49	a6	36	43	f4	47	91	df	33	93	21	3b
7	79	b7	97	85	10	b5	ba	3c	b6	70	d0	06	a1	fa	81	82
8	83	7e	7f	80	96	73	be	56	9b	9e	95	d9	f7	02	b9	a4
9	de	6a	32	6d	d8	8a	84	72	2a	14	9f	88	f9	dc	89	9a
a	fb	7c	2e	c3	8f	b8	65	48	26	c8	12	4a	ce	e7	d2	62
b	0c	e0	1f	ef	11	75	78	71	a5	8e	76	3d	bd	bc	86	57
c	0b	28	2f	a3	da	d4	e4	0f	a9	27	53	04	1b	fc	ac	e6
d	7a	07	ae	63	c5	db	e2	ea	94	8b	c4	d5	9d	f8	90	6b
e	b1	0d	d6	eb	c6	0e	cf	ad	08	4e	d7	c3	5d	50	1e	b3
f																

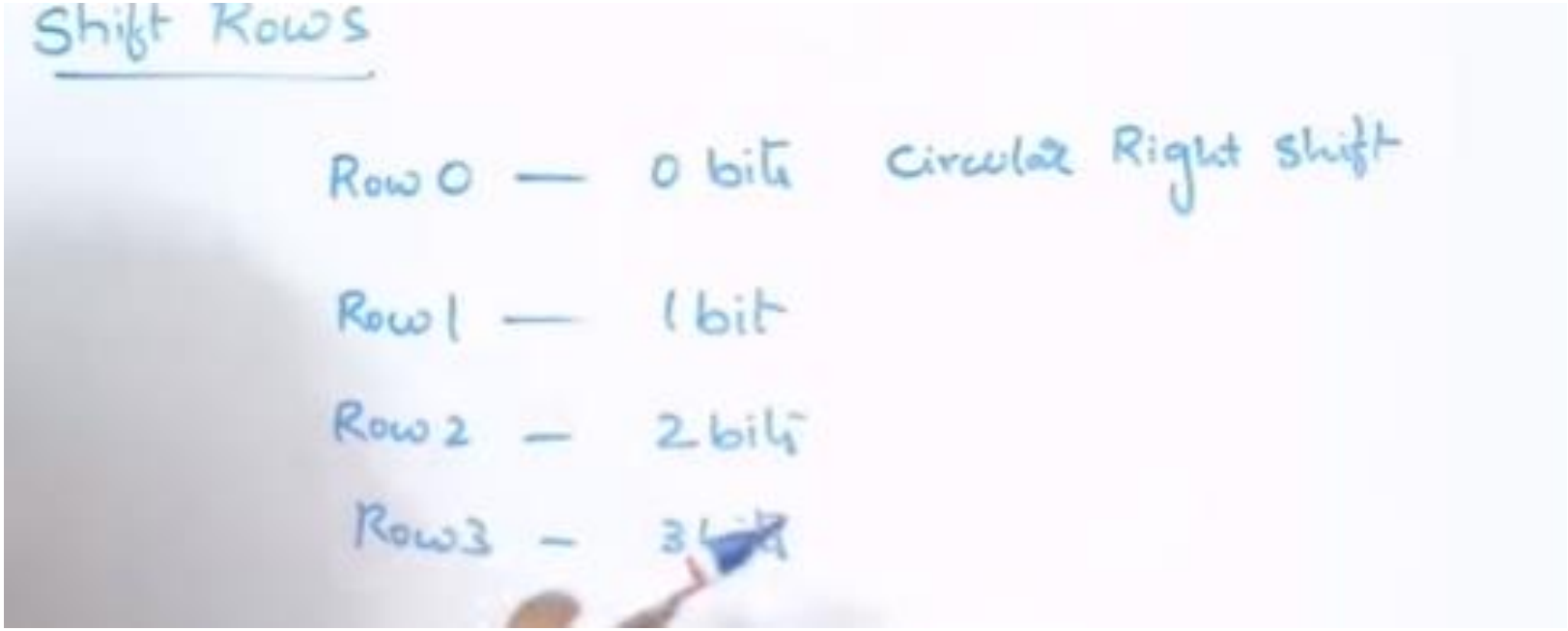
S –box ex:



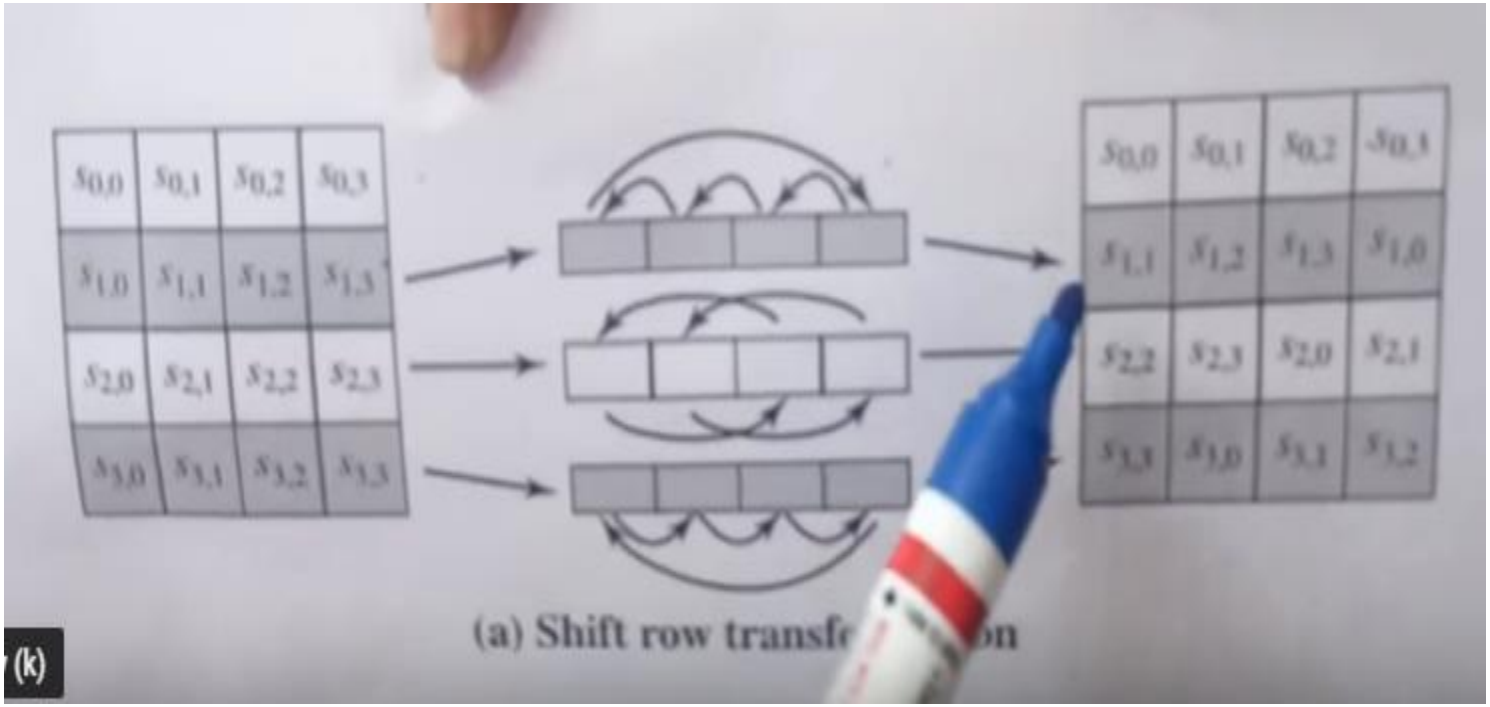
0^{th} row 5^{th} column

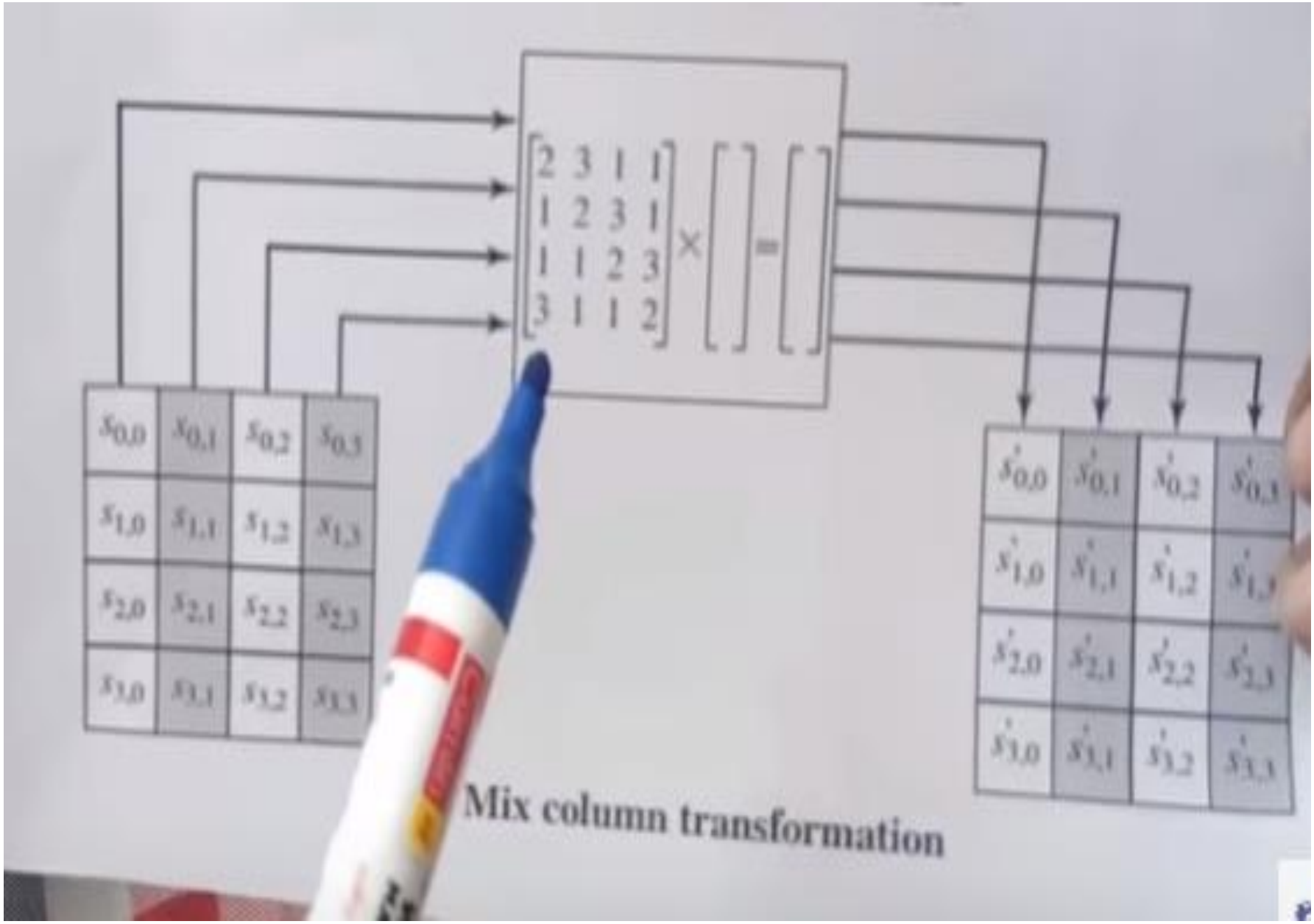


GF(2^8)	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	00	01	8d	f6	cb	52	7b	d1	e8	4f	29	c0	b0	e1	e5	c7
1	74	b4	aa	4b	[illegible]	2b	60	5f	58	3f	fd	cc	ff	40	ee	b2
2	3a	6e	5a	[illegible]	[illegible]	4d	a8	c9	c1	0a	98	15	30	44	a2	c2
3	2c	45	[illegible]	[illegible]	f3	39	66	42	f2	35	20	6f	77	bb	59	19
4	1d	[illegible]	[illegible]	87	2d	31	f5	69	a7	64	ab	13	54	25	e9	09
5	[illegible]	[illegible]	[illegible]	ca	4c	24	87	bf	18	3e	22	f0	51	ec	61	17
[illegible]	[illegible]	[illegible]	[illegible]	43	49	a6	36	43	f4	47	91	df	33	93	21	3b
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	10	b5	ba	3c	b6	70	d0	06	a1	fa	81	82
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	73	be	56	9b	9e	95	d9	f7	02	b9	a4
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	84	72	2a	14	9f	88	f9	dc	89	9a
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	65	48	26	c8	12	4a	ce	e7	d2	62
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	78	71	a5	8e	76	3d	bd	bc	86	57
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	e4	0f	a9	27	53	04	1b	fc	ac	e6
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

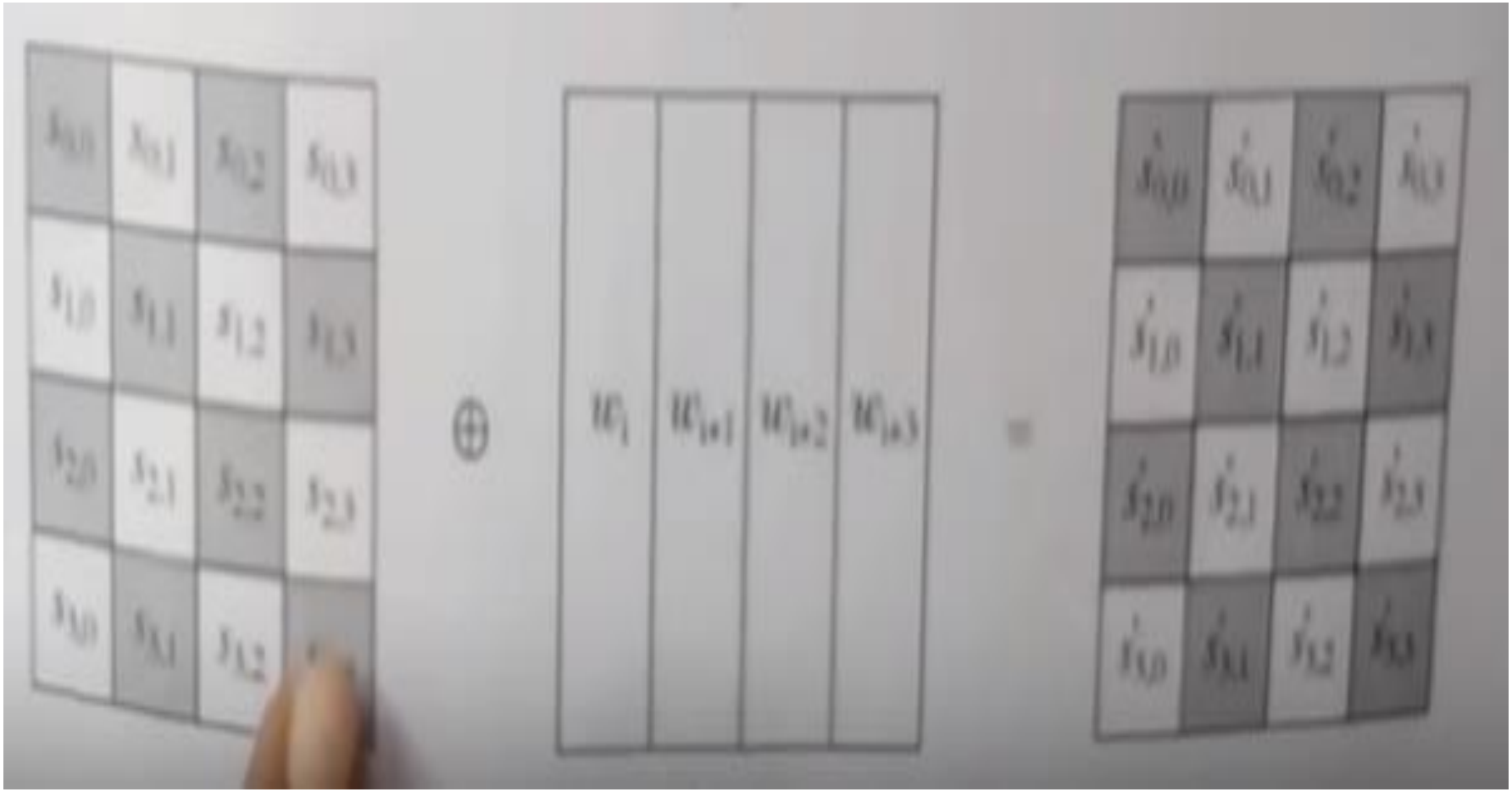

Shift Rows
Row 0 — 0 bits Circular Right shift
Row 1 — 1 bit
Row 2 — 2 bits
Row 3 —

Shift rows Transformation:

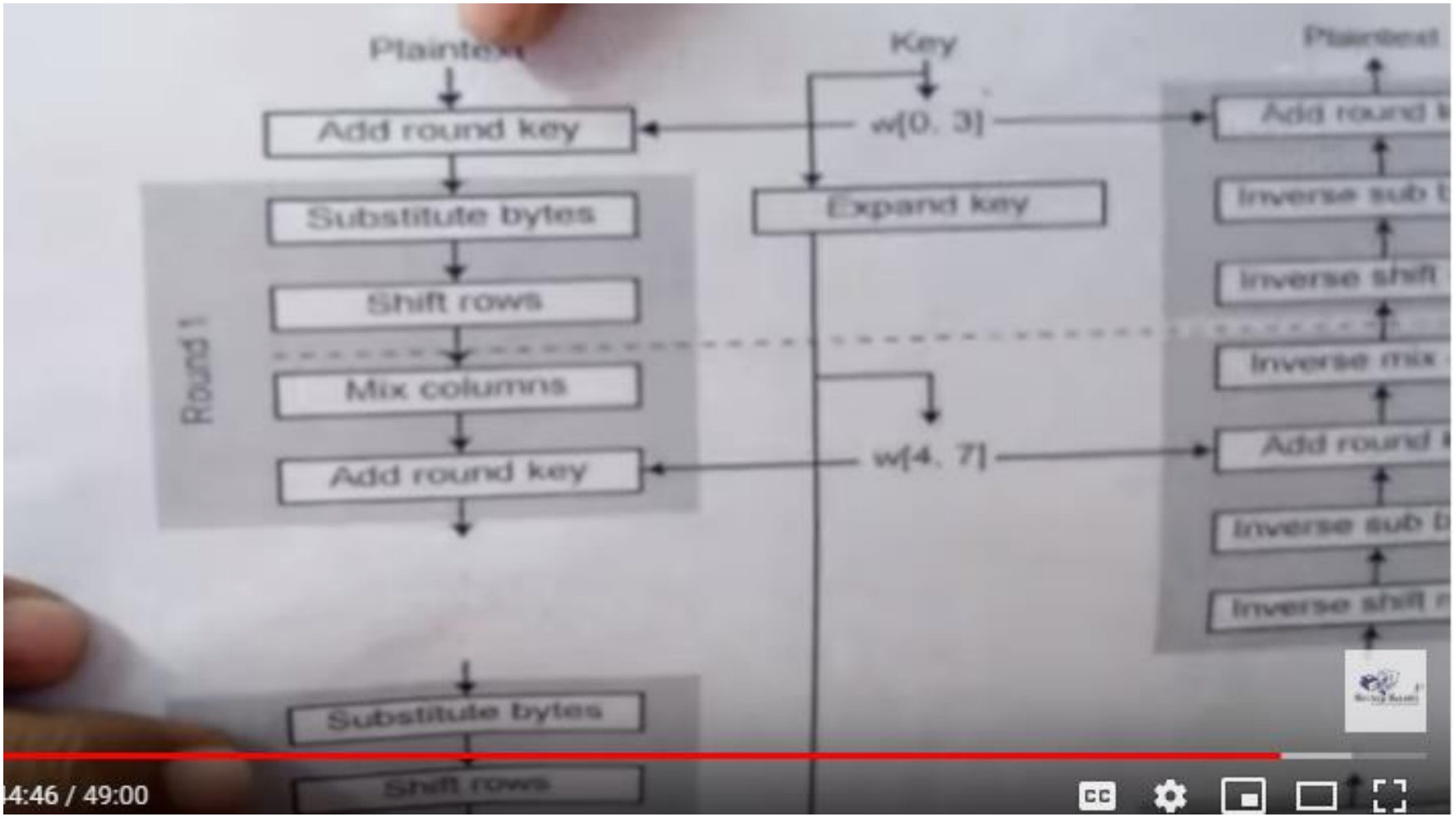



2 3 1 1
1 2 3 1
1 1 2 3
3 1 1 2
Mix column transformation

Add Round key Transformation: 1st col(1 word) Ex-Or with 1st word



Block Diagram AES:



AES	DES
AES stands for Advanced Encryption Standard	DES stands for Data Encryption Standard
Key length can be of 128-bits, 192-bits and 256-bits.	Key length is 56 bits in DES.
Number of rounds depends on key length : 10(128-bits), 12(192-bits) or 14(256-bits)	DES involves 16 rounds of identical operations
The structure is based on substitution-permutation network.	The structure is based in feistal network.
AES is more secure than the DES cipher and is the de facto world standard.	DES can be broken easily as it has known vulnerabilities. 3DES(Triple DES) is a variation of DES which is secure than the usual DES.
The rounds in AES are : Byte Substitution, Shift Row, Mix Column and Key Addition	The rounds in DES are : Expansion, XOR operation with round key, Substitution and Permutation
AES can encrypt 128 bits of plaintext.	DES can encrypt 64 bits of plaintext.
AES cipher is derived from square cipher.	DES cipher is derived from Lucifer cipher.
AES was designed by Vincent Rijmen and Joan Daemen.	DES was designed by IBM.
No known crypt-analytical attacks against AES but side channel attacks against AES implementations possible. Biclique attack have better complexity than brute-force but still ineffective.	Known attacks against DES include : Brute-force, Linear crypt-analysis and Differential crypt-analysis.