CRYPTOGRAPHY & NETWORK SECURITY

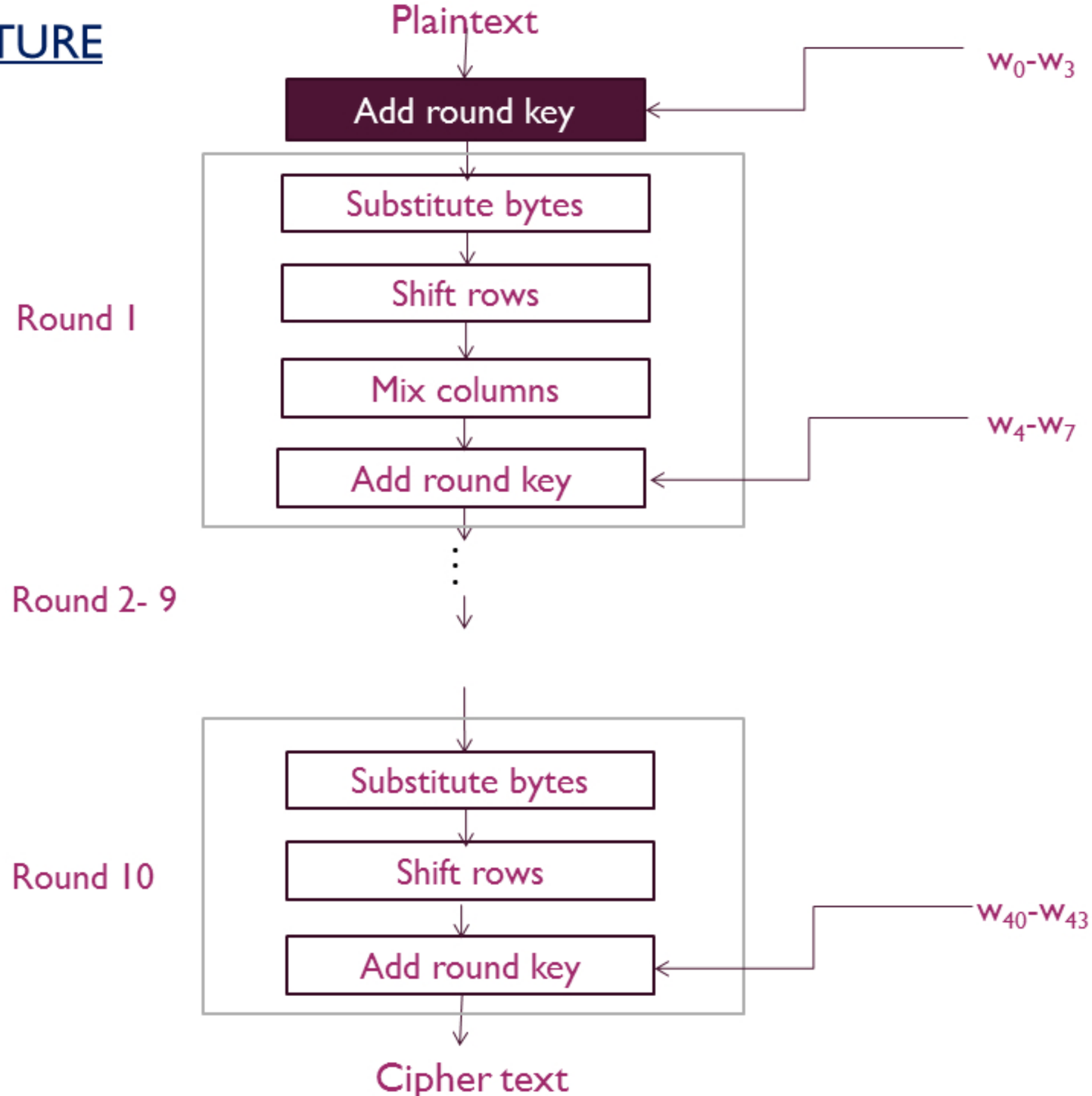
ADVANCED ENCRYPTION STANDARD (AES)

Vijesh Nair

ADVANCED ENCRYPTION STANDARD (AES)

- One of the best & popular algorithm used today.
- Is a symmetric block cipher.
- Block size = 128 bits.
- No . of rounds depends on key size.
- 128-bit key- 10 rounds
- 192-bit key - 12 rounds
- 256-bit key - 14 rounds

(AES) - STRUCTURE



Vijesh Nair

ADVANCED ENCRYPTION STANDARD (AES)

- It process data as bytes and not as bits.
- So we have 128 bit key & data
- So 128 / 8 = 16
- So 128 bits = 16 bytes.
- And 4 bytes = 1 word
- Input arranged in 4 x 4 matrix.

in_0	in_4	in_8	in_{12}
in_1	in_5	in_9	in_{13}
in_2	in_6	in_{10}	in_{14}
in_3	in_7	in_{11}	in_{15}

ADVANCED ENCRYPTION STANDARD (AES)

- Intermediate results are stored in another 4 x 4 matrix -- State array.

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

ADVANCED ENCRYPTION STANDARD (AES)

- Output is stored in another 4 x 4 matrix.

out_0	out_4	out_8	out_{12}
out_1	out_5	out_9	out_{13}
out_2	out_6	out_{10}	out_{14}
out_3	out_7	out_{11}	out_{15}

ADVANCED ENCRYPTION STANDARD (AES)

- Key is stored in another 4 x 4 matrix.

k_0	k_4	k_8	k_{12}
k_1	k_5	k_9	k_{13}
k_2	k_6	k_{10}	k_{14}
k_3	k_7	k_{11}	k_{15}

ADVANCED ENCRYPTION STANDARD (AES)

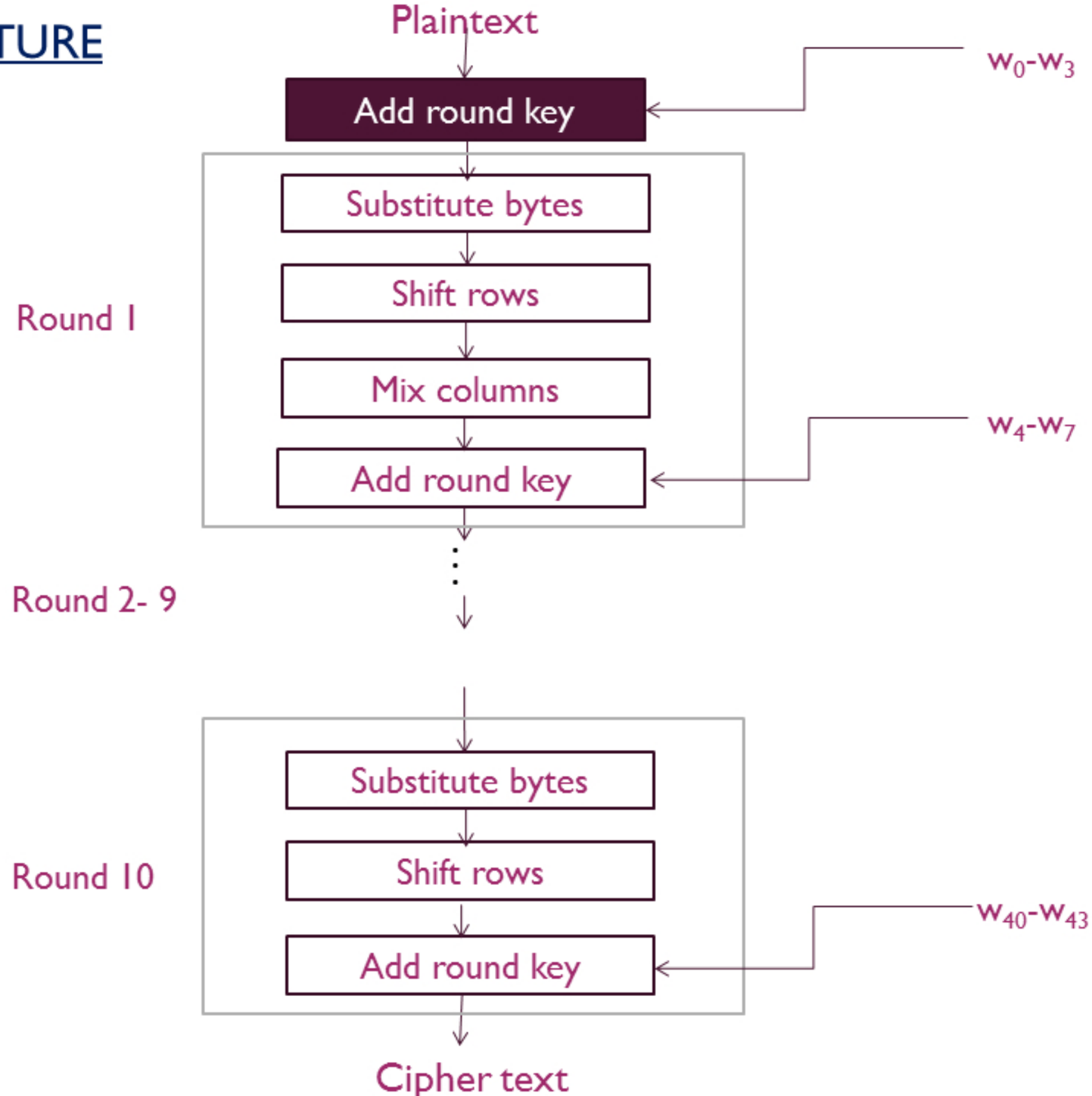
- Key is stored in another 4 x 4 matrix.

k_0	k_4	k_8	k_{12}
k_1	k_5	k_9	k_{13}
k_2	k_6	k_{10}	k_{14}
k_3	k_7	k_{11}	k_{15}

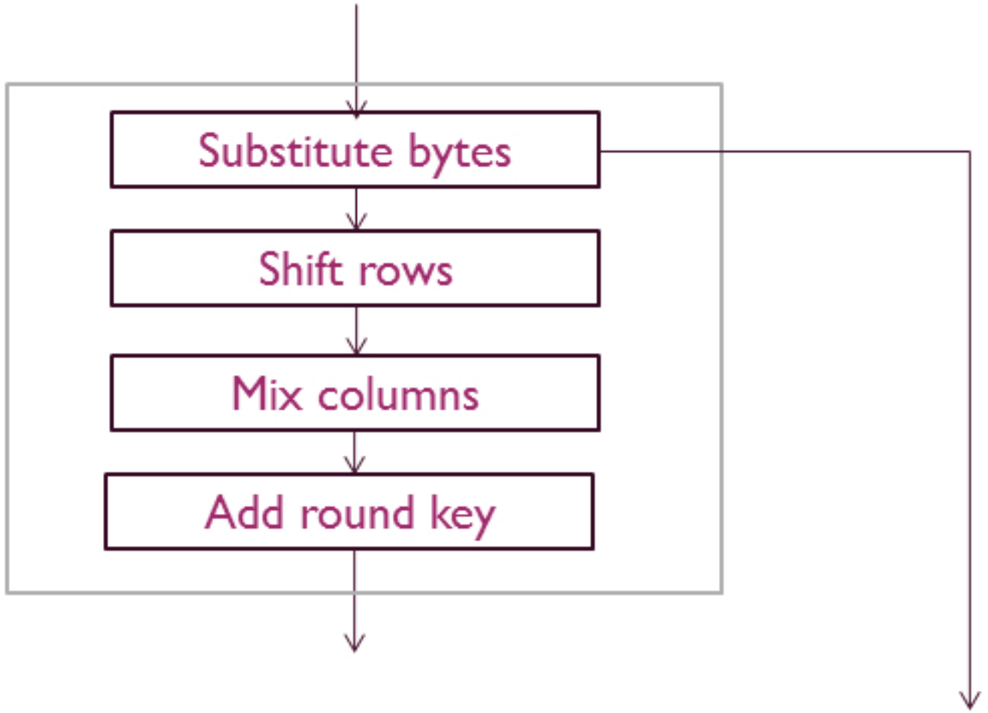
$$w_1 = k_0k_1k_2k_3$$
$$w_2 = k_4k_5k_6k_7$$
$$w_3 = k_8k_9k_{10}k_{11}$$
$$w_4 = k_{12}k_{13}k_{14}k_{15}$$

This key will be expanded to 44 words ($w_0, w_1, \ldots.w_{43}$)

(AES) - STRUCTURE



Round 1

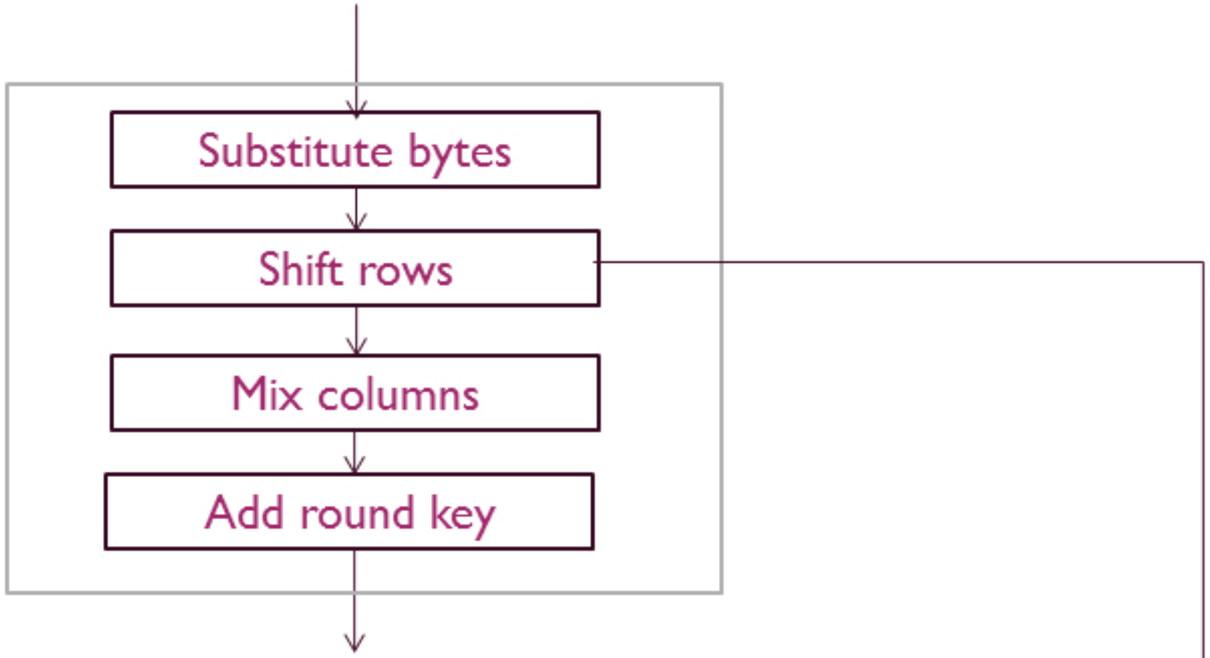


- Uses an S-box to perform a byte-by-byte substitution of the block
- Take in_0 i.e, 8 bits.
- Split it into two halves.
- First half represents row and second half represents column.
- 16 x 16 s box.
- Result will be sent to state array.

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0001																
0010																
0011																
0100																
0101					11100101											
0110																
0111																
1000																
1001																
1010																
1011																
1100																
1101																
1110																
1111																

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Round 1



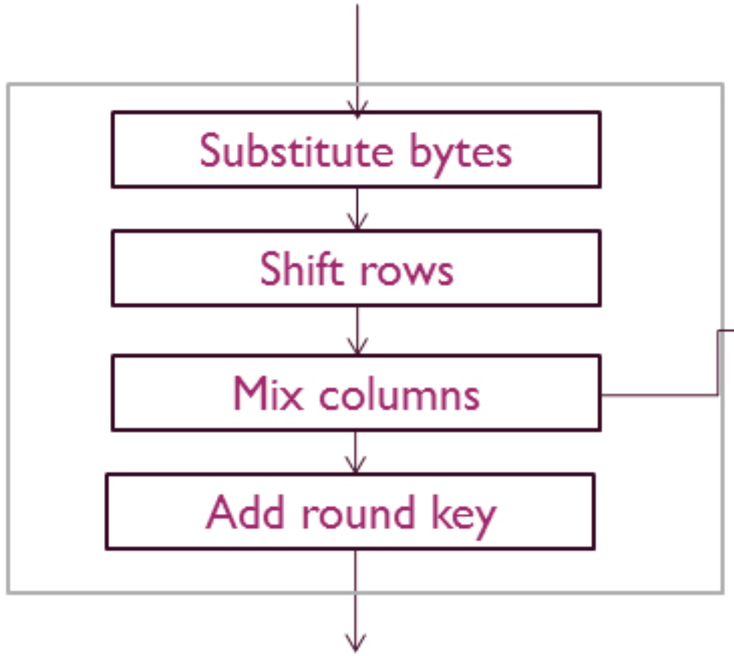
- Output matrix from Substitution stage will be the input to this round.
- For first row no shift is made.
- For second row - 1 byte circular left shift.
- For third - 2 byte circular left shift.
- For forth row - 3 byte circular left shift.

- For first row no shift is made.
- For second row - 1 byte circular left shift.
- For third row - 2 byte circular left shift.
- For forth row - 3 byte circular left shift.

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

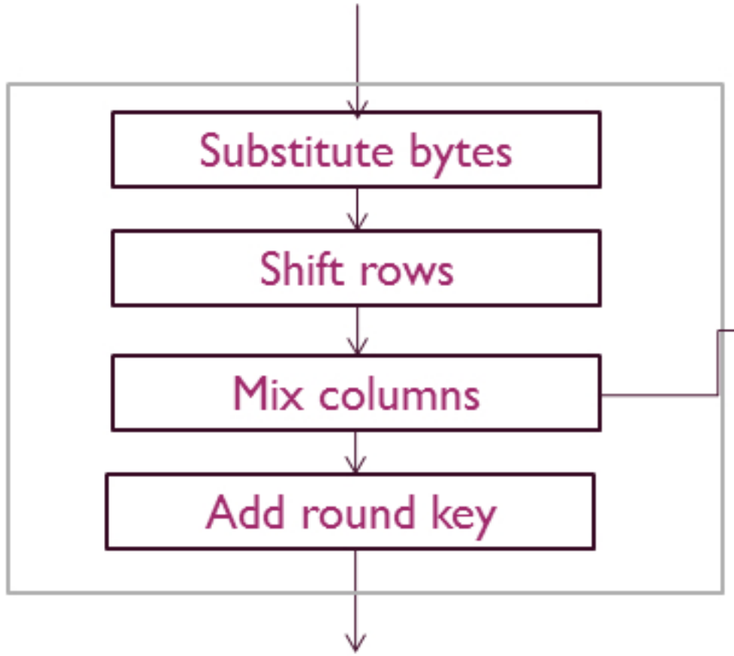
A	B	C	D
F	G	H	E
K	L	I	J
P	M	N	O

Round 1



- Output matrix from Shift rows will be the input to this round.
- Take each column (word) and multiply with a predifined 4 x 4 matrix.

Round 1



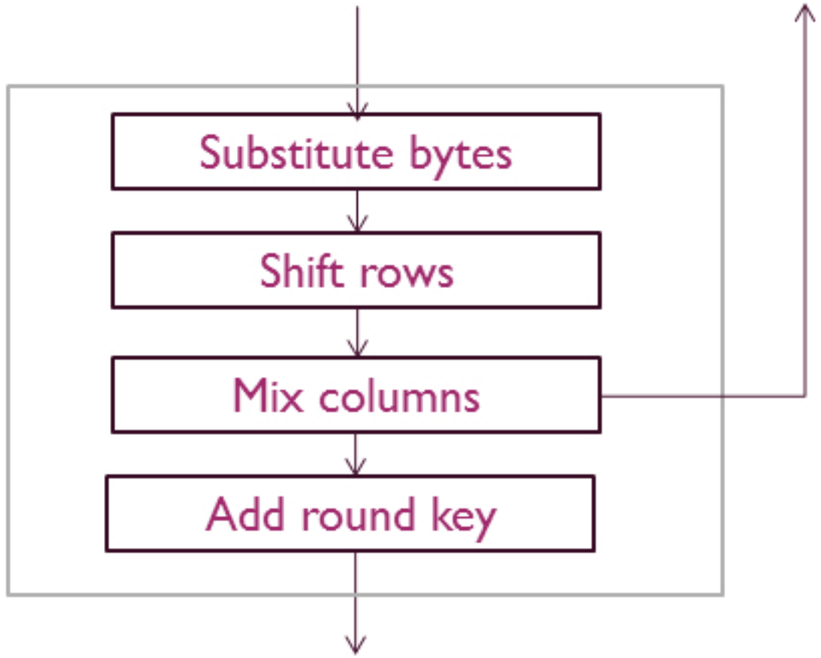
- Output matrix from Shift rows will be the input to this round.
- Take each column (word) and multiply with a predifined 4 x 4 matrix.

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

X

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

Round 1



- Output matrix from Shift rows will be the input to this round.
- Take each column (word) and multiply with a predifined 4 x 4 matrix.

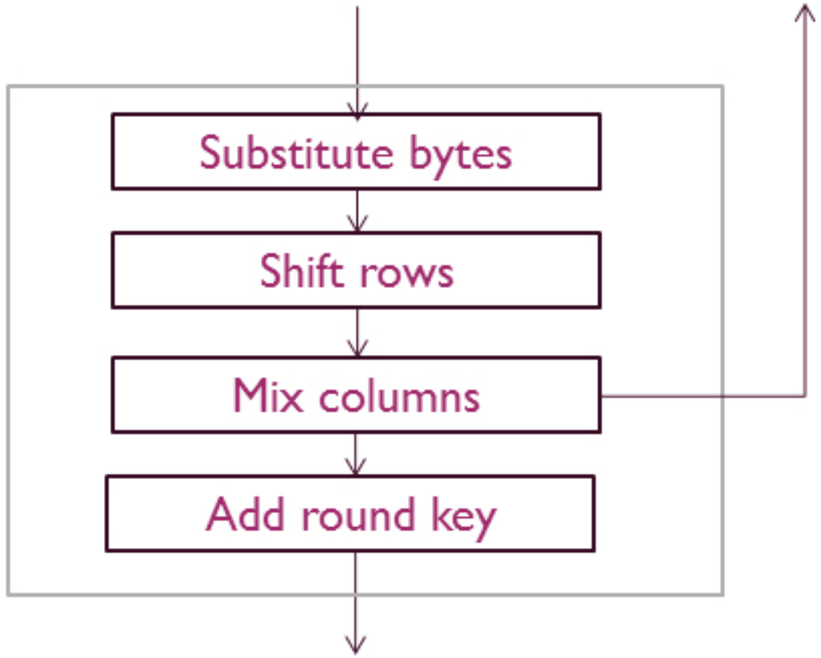
A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

X

A
E
I
M

Round 1



- Output matrix from Shift rows will be the input to this round.
- Take each column (word) and multiply with a predifined 4 x 4 matrix.

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

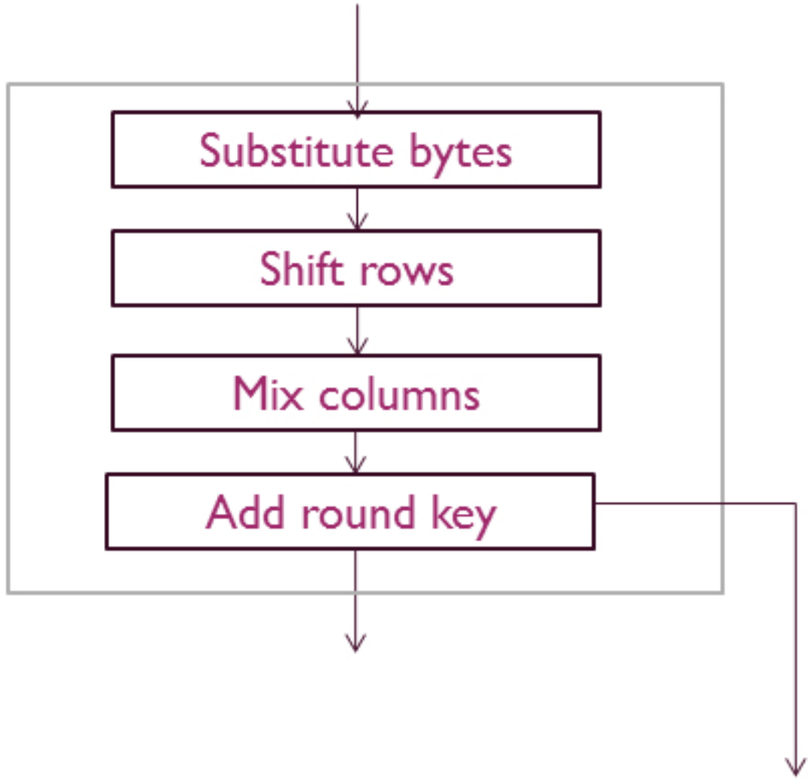
2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

X

A
E
I
M

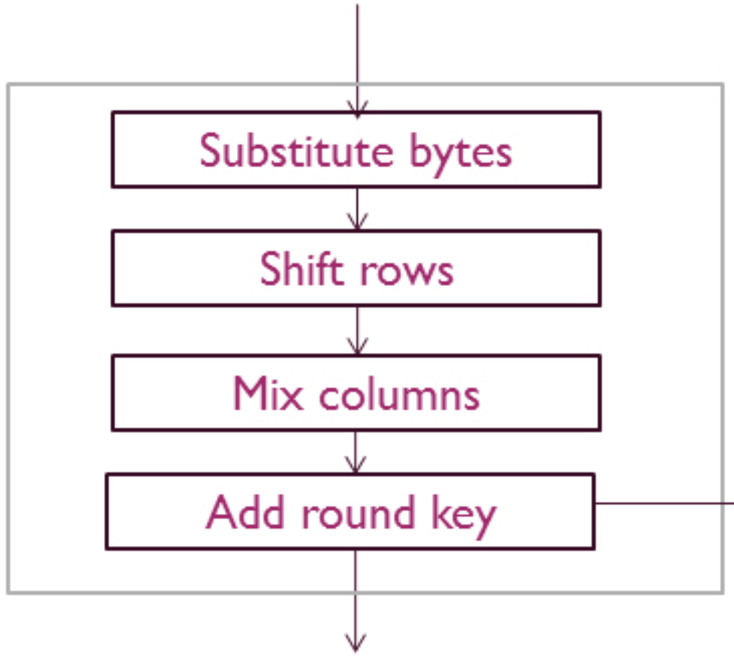
$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

Round 1



- Do XOR operation on state array with the first 4 words of the key.
- i.e, a 4 x 4 matrix XOR a 4 x 4 matrix

Round 1



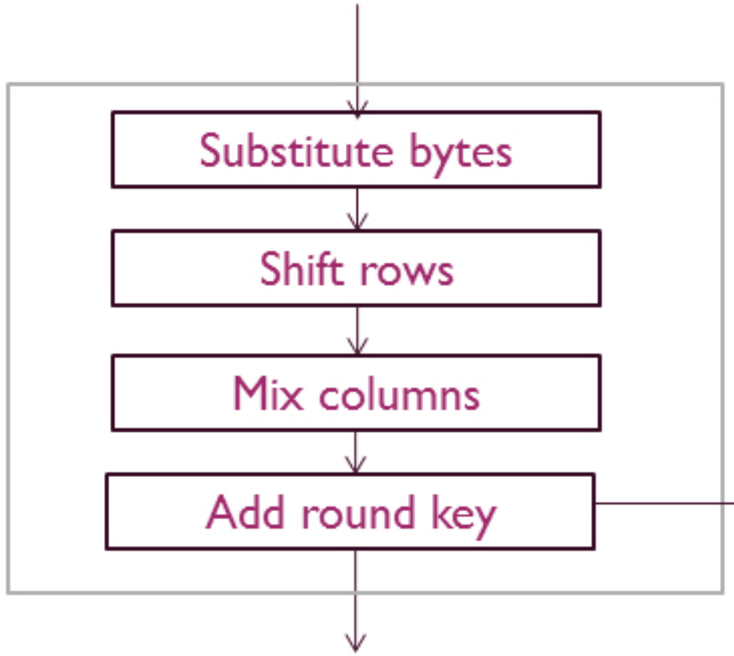
- Do XOR operation on state array with the first 4 words of the key.
- i.e, a 4 x 4 matrix XOR a 4 x 4 matrix

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

⊕

Q	R	S	T
U	V	W	X
Y	Z	I	2
3	4	5	6

Round I



- Do XOR operation on state array with the first 4 words of the key.
- i.e, a 4 x 4 matrix XOR a 4 x 4 matrix

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

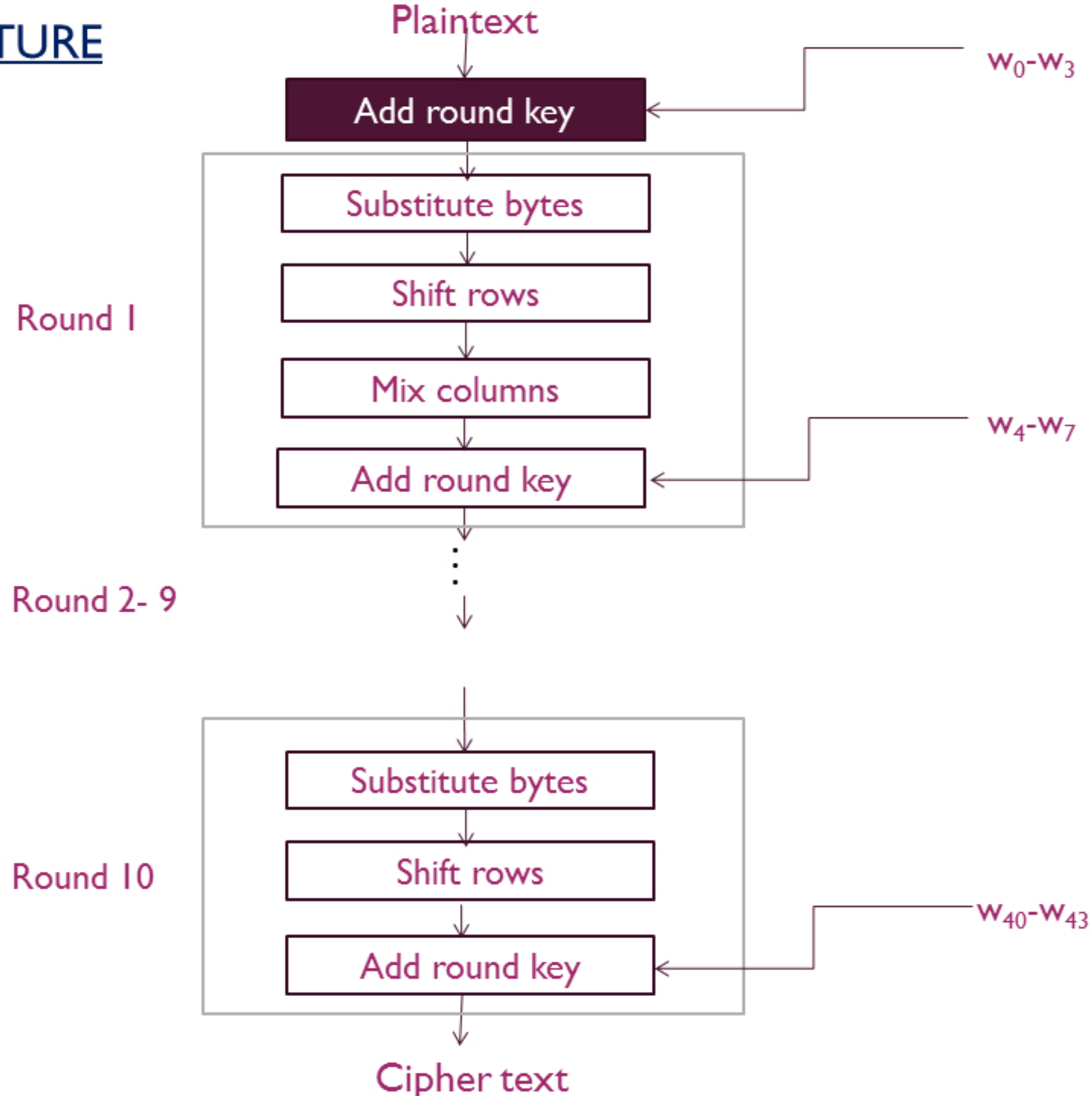
⊕

Q	R	S	T
U	V	W	X
Y	Z	I	2
3	4	5	6

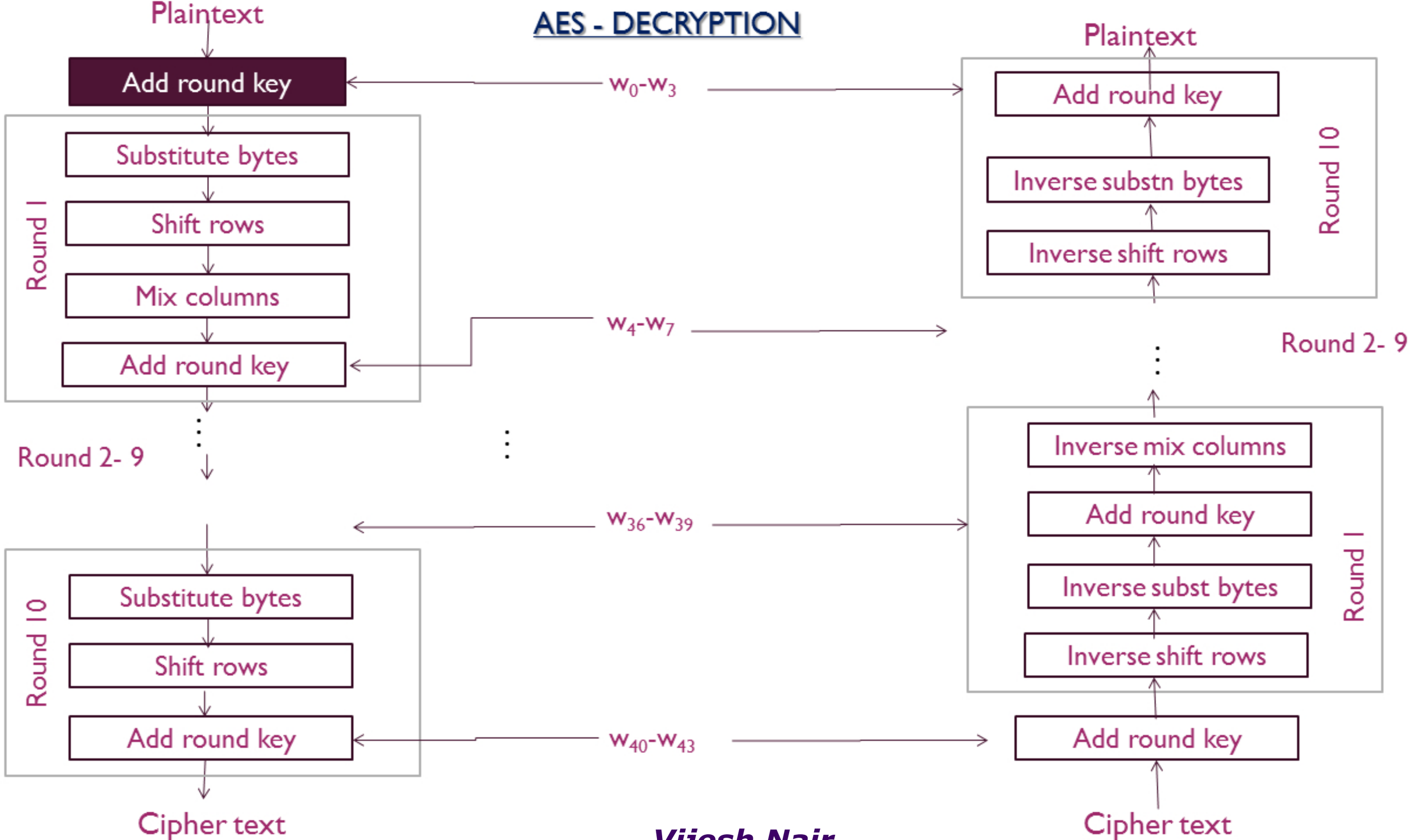
=

State array

(AES) - STRUCTURE



AES - DECRYPTION



Inverse S- box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Inverse shift operations :

- For first row no shift is made.
- For second row - 1 byte circular right shift.
- For third row - 2 byte circular right shift.
- For forth row - 3 byte circular right shift.

A	B	C	D
F	G	H	E
K	L	I	J
P	M	N	O

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

Inverse mix columns operations :

- Take each column (word) and multiply with a predifined 4 x 4 matrix.

0E	0B	0D	09
09	0E	0B	0D
0D	09	0E	0B
0B	0D	09	0E

X

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

THANK YOU

Vijesh Nair