Why Was the AES Encryption Algorithm necessary?

- When the Data Encryption Standard algorithm, also known as the DES algorithm, was formed and standardized, it made sense for that generation of computers.
- Going by today's computational standards, breaking into the DES algorithm became easier and faster with every year, as seen in the image below.

Chronology of DES Cracking	
Broken for the first time	1997
Broken in 56 hours	1998
Broken in 22 hours and 15 minutes	1999
Capable of broken in 5 minutes	2021

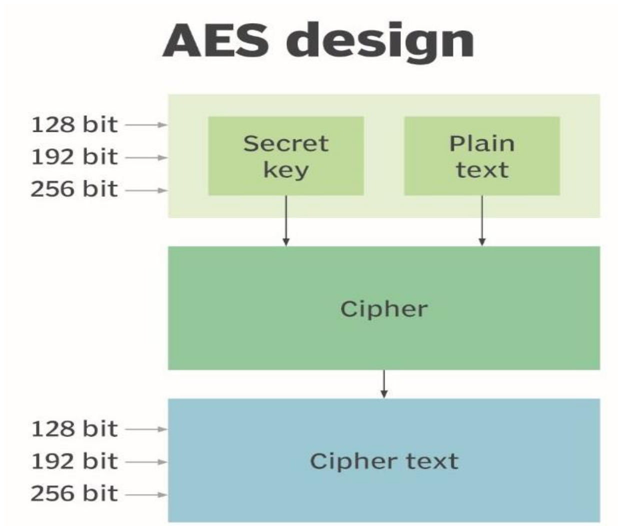
Source: Wikipedia

- A more robust algorithm was the need of the hour, with longer key sizes and stronger ciphers to break into.
- They created the triple DES to fix this problem, but it never became mainstream because of its relatively slower pace.
- Thus, the Advanced Encryption Standard came into existence to overcome this drawback.

❖ AES (Advanced Encryption Standard)

- The **AES** Encryption algorithm (also known as the Rijndael algorithm) is a symmetric block cipher algorithm with a block/chunk size of 128 bits.
- It is developed by the National Institute of Standards and Technology (NIST) in 2001.

- It is widely used today as it is much stronger than DES and triple DES despite being harder to implement.
- It converts these individual blocks using keys of 128, 192, and 256 bits.
- It is based on a substitution-permutation network, also known as an **SP network.**
- It consists of a series of linked operations, including replacing inputs with specific outputs (substitutions) and others involving bit shuffling (permutations).



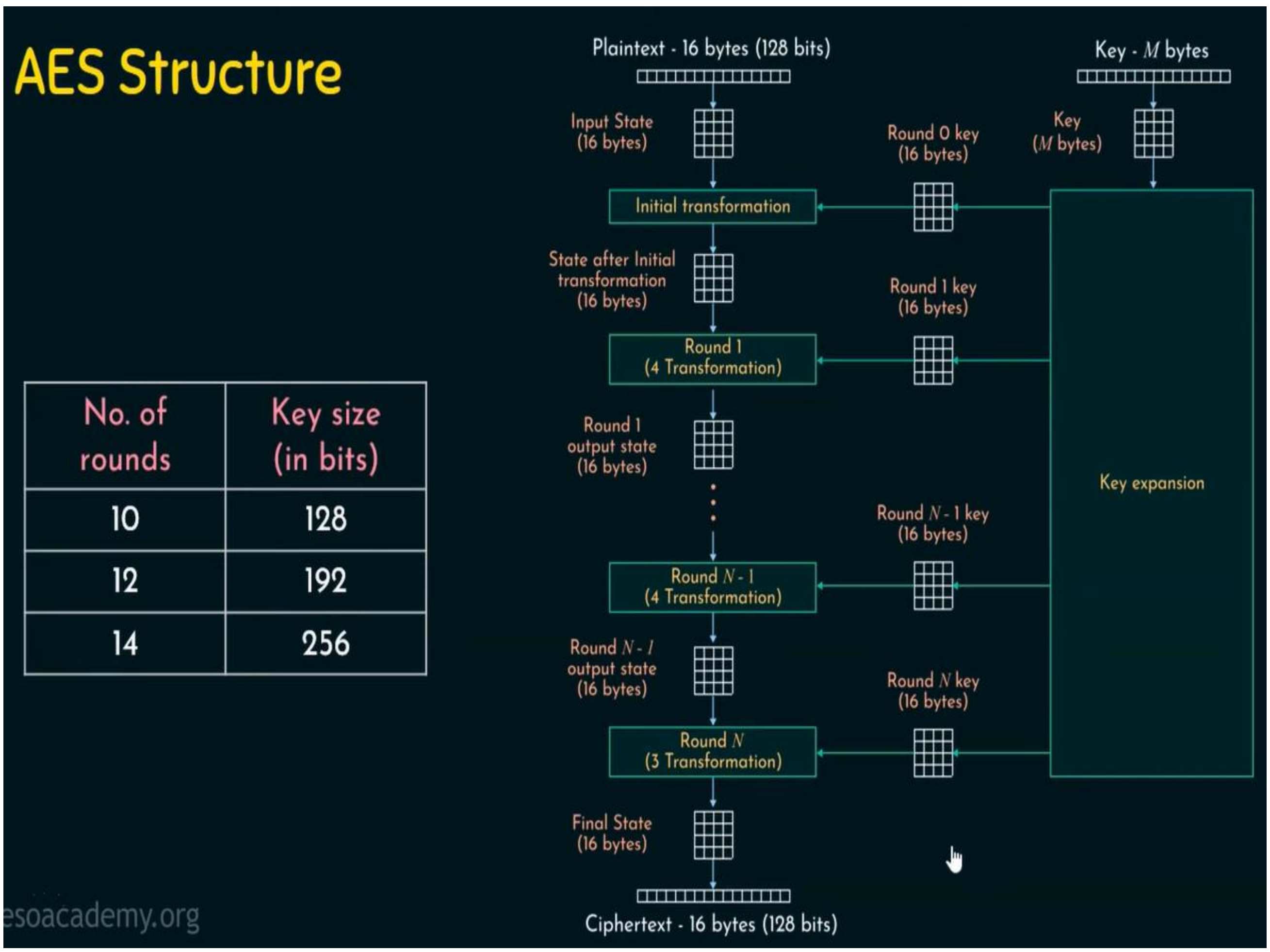
❖ What are the Features of AES?

1. Symmetric key symmetric block cipher
2. 128-bit data, 128/192/256-bit keys
3. Stronger and faster than Triple-DES

❖ Operation of AES

- AES is an iterative rather than Feistel cipher. It is based on substitution permutation network.
- It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

- Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix
- Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.
- The schematic of AES structure is given in the following illustration –



AES Parameters

	AES-128	AES-192	AES-256
Key Size	128	192	256
Plaintext Size	128	128	128
Number of rounds	10	12	14
Round Key Size	128	128	128

How Does AES Work?

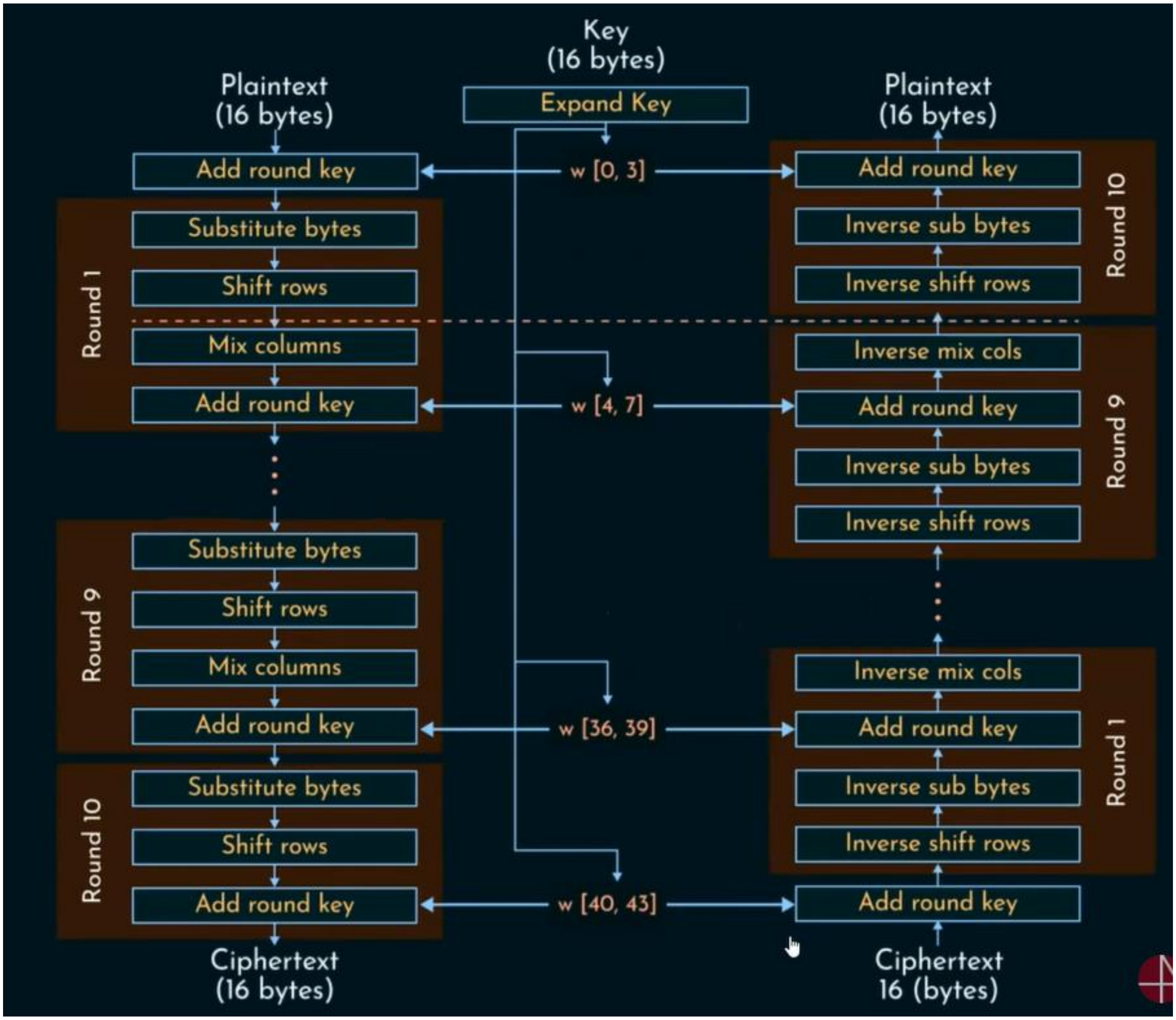
- To understand the way AES works, you first need to learn how it transmits information between multiple steps.
- Since a single block is 16 bytes, a 4x4 matrix holds the data in a single block, with each cell holding a single byte of information.

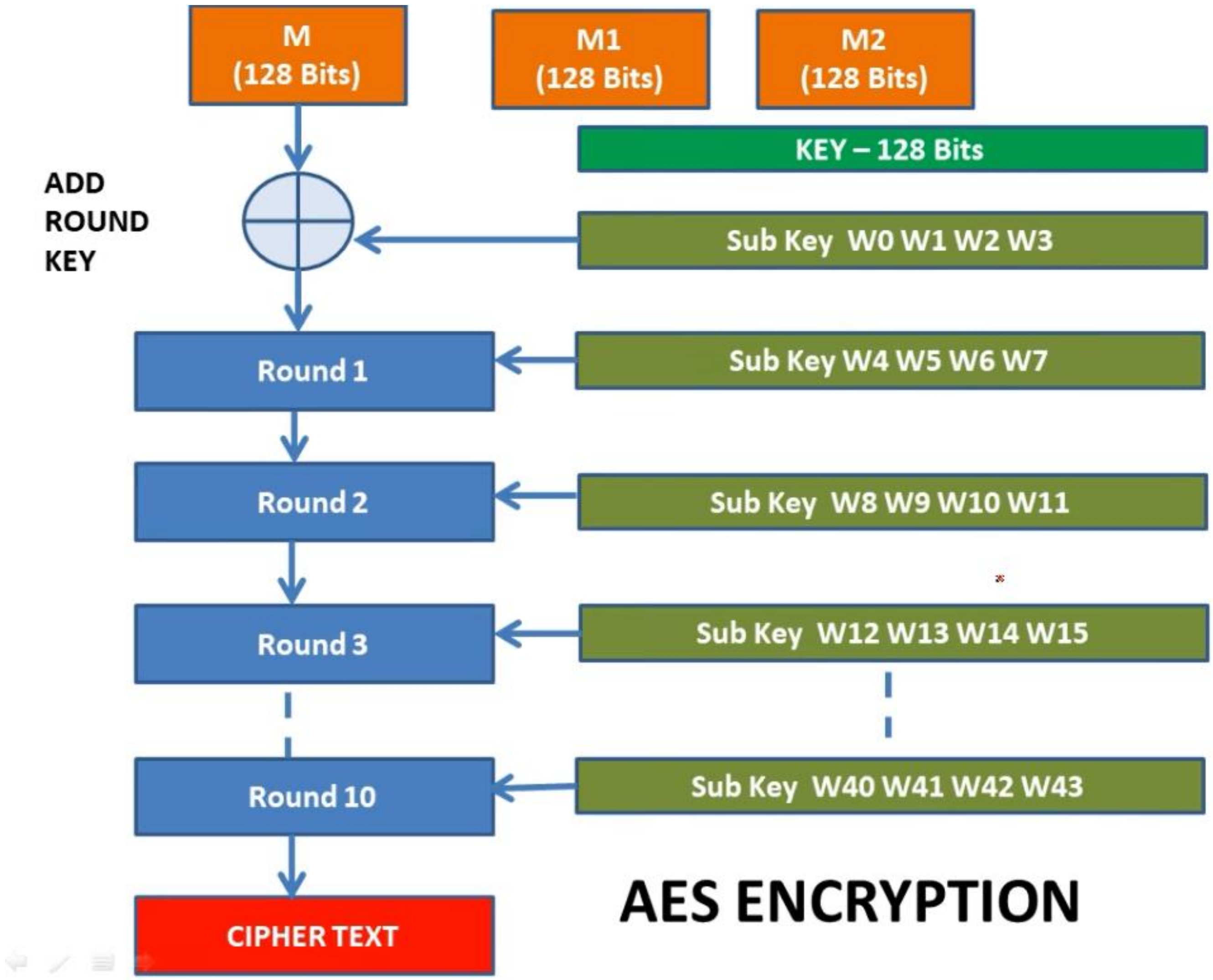
0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

- The matrix shown in the image above is known as a state array. Similarly, the key being used initially is expanded into (n+1) keys, with n being the number of rounds to be followed in the encryption process.
- So, for a 128-bit key, the number of rounds is 10, with no. of keys to be generated being 10+1, which is a total of 11 keys.

1. It takes the input of 16 bytes (128 bits) and outputs the ciphertext (128 bits).
2. Every 4 x 4 = 16 bytes are element state arrays that can store 16 bytes of information
3. Input state: it is storing input plain text of 16 bytes and gives to the initial transformation
4. In the initial transformation, the input plain text of 16 bytes along with the transformation function and the output is given to the state after initial transformation element arrays which is again given to the Round 1
5. Round 1 Take step 4 output and perform 4 transformations with it
6. Similarly, Round 2 takes the previous step round operations + 4 transformations output until Round N - 1
7. At the last Round N, the output of Round N - 1 is the input of Round N which is the last round and it has only 3 Transformation
8. The output of step 7 is now stored in element arrays. And the 16 bytes is the actual cipher that we want from this AES Encryption Structure.

AES Encryption and Decryption




M
(128 Bits)
M1
(128 Bits)
M2
(128 Bits)
KEY – 128 Bits
ADD
ROUND
KEY
Sub Key W0 W1 W2 W3
Round 1
Sub Key W4 W5 W6 W7
Round 2
Sub Key W8 W9 W10 W11
Round 3
Sub Key W12 W13 W14 W15
Round 10
Sub Key W40 W41 W42 W43
CIPHER TEXT
AES ENCRYPTION

Key Expansion in AES

Key in text= satishcjisboring

"satishcjisboring" = 16 characters → 1 character = 1 byte (in ASCII)

01110011 01100001 01110100 01101001 01110011 01101000 01100011 01101010 01101001 01110011 01100010 01101111 01110010 01101001 01101110 01100111

Hex representation:

73 61 74 69 73 68 63 6a 69 73 62 6f 72 69 6e 67

b_1 b_2 b_3 b_4 b_5 b_6 b_7 b_8 b_9 b_{10} b_{11} b_{12} b_{13} b_{14} b_{15} b_{16}

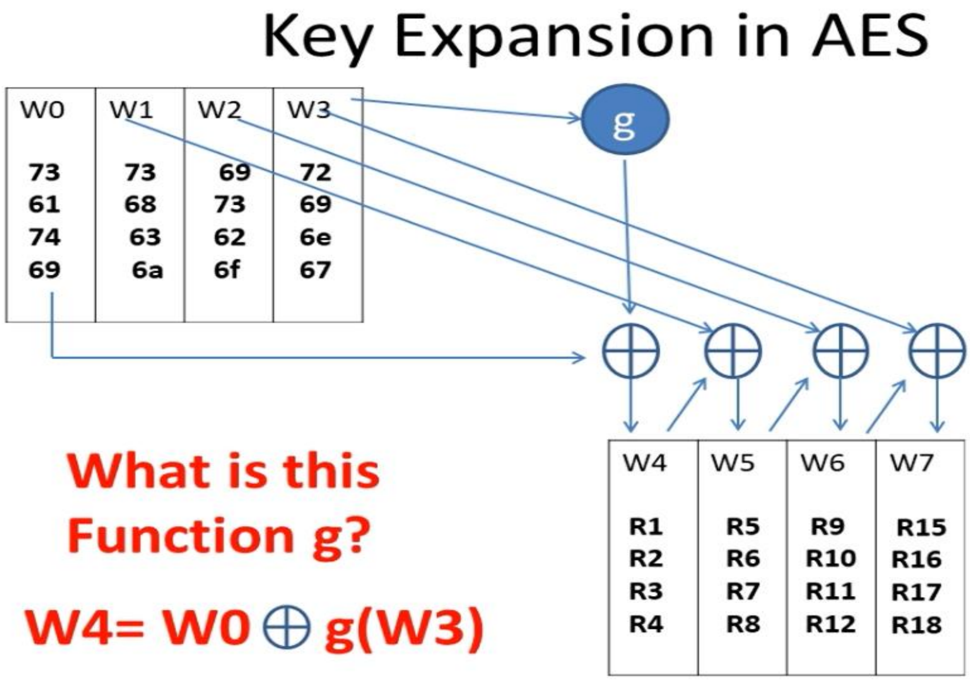
Now representing key in 4*4 matrix we get

$$\begin{bmatrix} b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \\ b_4 & b_8 & b_{12} & b_{16} \end{bmatrix}$$

W0	W1	W2	W3	W4	W5	W6	W7	......	....	W43
b_1 b_2 b_3 b_4	b_5 b_6 b_7 b_8	b_9 b_{10} b_{11} b_{12}	b_{13} b_{14} b_{15} b_{16}							

W0	W1	W2	W3	W4	W5	W6	W7	......	....	W43
73 61 74 69	73 68 63 6a	69 73 62 6f	72 69 6e 67							

Now how to expand available 4 words in to 40 words?



So, the idea is to generate enough keys (44 words) ie,.11 keys based on the initial key (16 bytes, 4 words) to be used in 10 rounds of the encryption process.

What is this function g?

$W4 = W0 \oplus g(W3)$

Step 1

- Take W3 do a cyclic left shift 1 for each byte and we will be able to get RotWord (X1).
- Rot word performs a one-byte circular left shift on a word.
- This means that an input word [B0, B1, B2, B3] is transformed into [B1, B2, B3, B0]

Step 2

- From RotWord we have to find Subword (Y1)
- SubWord performs a byte substitution on each byte of its input word, using the AES S-box

AES S-Box

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Step 3

- we have to perform XOR operation on subword with the constant called the round constant, Rcon[i]
- Round constant is

R1	R2	R3	R4	R5	R6	R7	R8	R9	R10
01	02	04	08	10	20	40	80	1B	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

W3	RotWord (X1)	SubWord (Y1)
72	69	f9
69	6e	9f
6e	67	85
67	72	40

The result Y1 is XORed with a round constant, Rcon[j].

Y1	11111001100111111000010101000000
R1	00000001000000000000000000000000
g(w3)	11111000100111111000010101000000

g(w3) = F8 9F 85 40

Now,

W4 = W0 ⊕ g(W3)

01110011 01100001 01110100 01101001

⊕

11111000 10011111 10000101 01000000

= 10001011 11111110 11110001 00101001

= 8b fe f1 29

After getting W4 it will be easy, now we have to take W4 and ⊕ with W1, we get w5.

Likewise, we have to take W5 and ⊕ with W2 we get W6.

Likewise, we have to take W6 and $\oplus$ with W3 we get W7.

So ,

W4 = 8b fe f1 29
W5 = f8 96 92 43
W6 = 91 e5 f0 2c
W7 = e3 8c 9e 4b

So, sub key for round 1 we get = 8b fe f1 29 f8 96 92 43 91 e5 f0 2c e3 8c 9e 4b

Now for sub key 2 we have to find W8 to W11

W8= W4 $\oplus$ g(W7)

W9 = W8 $\oplus$ W5

W10 = W9 $\oplus$ W6

W11 = W10 $\oplus$ W7

So, after combining output of W8 W9 W10 and W11 ae get sub key 2 for round 2.

Like that we have to achieve W0 to W43.

Add round key Or Initial Transformation

- In the initial transformation, we add the round key and the plain text of 16 bytes.
- W [0,1,2,3] is a round key given to the initial transformation and added rounded key with the plain text of 128 bits and finally XORed Operation is performed. Once the XORed Operation is performed it goes into round 1

M (128 Bits) **secretmessagenow**

73 65 63 72 65 74 6d 65 73 73 61 67 65 6e 6f 77

$$\begin{bmatrix} 73 & 65 & 73 & 65 \\ 65 & 74 & 73 & 6e \\ 63 & 6d & 61 & 6f \\ 72 & 65 & 67 & 77 \end{bmatrix} \oplus \begin{bmatrix} 73 & 73 & 69 & 72 \\ 61 & 68 & 73 & 69 \\ 74 & 63 & 62 & 6e \\ 69 & 6a & 6f & 67 \end{bmatrix}$$

73	**01110011**
73	**01110011**
Result	**00000000**

The output matrix we get is state array.

$$\begin{bmatrix} 00 & 16 & 1a & 17 \\ 04 & 1c & 00 & 07 \\ 17 & 0e & 03 & 01 \\ 1b & 0f & 0f & 10 \end{bmatrix}$$

AES Detailed Round Operations

- This section describes what happens in each round or the transformation functions.
- There are 4 operations in every round except (in round 10 or the last round of encryption).

1. Substitute Bytes (Sub-Bytes) - Substitution Operations
2. Shift Rows - Permutation Operation
3. Mix Columns - Substitution Operations
4. Add Round Key - Substitution Operations

Byte Substitution

- Does a simple replacement of each byte of the block data using a S-box.
- Left four bits determines row and right four bits determines column.
- **input to the round one is output of Add round key Or Initial Transformation**

$$\begin{bmatrix} 00 & 16 & 1a & 17 \\ 04 & 1c & 00 & 07 \\ 17 & 0e & 03 & 01 \\ 1b & 0f & 0f & 10 \end{bmatrix}$$

AES S-Box

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

- By using this S box Substitute each Bytes of output of **Add round key Or Initial Transformation.**
- Output will be

$$\begin{bmatrix} 63 & 47 & a2 & f0 \\ f2 & 9c & 63 & c5 \\ f0 & ab & 7b & 7c \\ af & 76 & 76 & ca \end{bmatrix}$$

Shift Rows

- ❖ Output state array (i.e., 4*4 matrix) of Byte Substitution will be input of Shift rows
- ❖ Shift rows simply shifts the rows bytes.
    - First row: No change
    - Second row: one byte cyclical left shift
    - Third row: two - byte cyclical left shift
    - Fourth row: three - byte cyclical left shift

$$\begin{bmatrix} 63 & 47 & a2 & f0 \\ f2 & 9c & 63 & c5 \\ f0 & ab & 7b & 7c \\ af & 76 & 76 & ca \end{bmatrix} = \begin{bmatrix} 63 & 47 & a2 & f0 \\ 9c & 63 & c5 & f2 \\ 7b & 7c & f0 & ab \\ ca & af & 76 & 76 \end{bmatrix}$$

- So, output of **Shift Rows in round function is given below**

$$\begin{bmatrix} 63 & 47 & a2 & f0 \\ 9c & 63 & c5 & f2 \\ 7b & 7c & f0 & ab \\ ca & af & 76 & 76 \end{bmatrix}$$

- And this state array 4*4 matrix will be input for mix column.

Mix Columns

- The third transformation function under round operation of AES is called as mix column, operates on each column individually.
- In AES mix column there is one pre-defined 4*4 matrix

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

Predefine Matrix

- So, this predefined matrix is multiplied with state array.
- Sate array = output of shift rows function.
- Here both predefined matrix and state array matrix is multiplied and generate new state array.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix} = \begin{bmatrix} S'_{0,0} & S'_{0,1} & S'_{0,2} & S'_{0,3} \\ S'_{1,0} & S'_{1,1} & S'_{1,2} & S'_{1,3} \\ S'_{2,0} & S'_{2,1} & S'_{2,2} & S'_{2,3} \\ S'_{3,0} & S'_{3,1} & S'_{3,2} & S'_{3,3} \end{bmatrix}$$

Predefine Matrix State Array New State Array

- New state array is the output of Mix Column transformation.
- Each byte of a column is mapped in to a new value that is a function of all four bytes in that column.

- For example:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 90 & EC \\ 46 & E7 & 4A & C3 \\ A6 & 8C & D8 & 95 \end{bmatrix} = \begin{bmatrix} ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{bmatrix}$$

Predefine Matrix **State Array** **New State Array**

❖ Here values in both matrix is in hexadecimal format. so, we cannot solve it as simple multiplication as in decimal. For this matrix multiplication we have to use binary number system and polynomial theorem based on the finite field arithmetic's.

AES Mix Column

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} * \begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 90 & EC \\ 46 & E7 & 4A & C3 \\ A6 & 8C & D8 & 95 \end{bmatrix} = \begin{bmatrix} ? & & & \\ & & & \\ & & & \\ & & & \end{bmatrix}$$

$$\{02\} * \{87\} \oplus \{03\} * \{6E\} \oplus \{01\} * \{46\} \oplus \{01\} * \{A6\}$$

$$\begin{array}{cccccccc} X^7 + & X^6 + & X^5 + & X^4 + & X^3 + & X^2 + & \boxed{X^1} + & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}$$

$02 = 0000\ 0010 = X$

$87 = 1000\ 0111 = X^7 + X^2 + X + 1$

$$\begin{array}{cccccccc} \boxed{X^7} + & X^6 + & X^5 + & X^4 + & X^3 + & \boxed{X^2} + & \boxed{X^1} + & \boxed{1} \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{array}$$

$$\begin{aligned} \{02\} * \{87\} &= X * (X^7 + X^2 + X + 1) \\ &= \boxed{X^8} + X^3 + X^2 + X \\ &= X^4 + \cancel{X^3} + \cancel{X} + 1 + \cancel{X^3} + X^2 + \cancel{X} \\ &= X^4 + X^2 + 1 \\ &= 0001\ 0101 \end{aligned}$$

Use irreducible Polynomial Theorem, GF (2^3)

$X^8 = X^4 + X^3 + X + 1$

$$\begin{array}{cccccccc} X^7 + & X^6 + & X^5 + & X^4 + & X^3 + & X^2 + & X^1 + & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}$$

- Here binary value is mapped with A Galois field, also known as a finite field GF (2^3) polynomial theorem. i.e., $(X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X^1 + 1)$
- If power is greater than 7 i.e., (X power >7) we use irreducible polynomial Theorem, **GF (2^3) = $(X^8 + X^4 + X^3 + X + 1)$ -- remember this always**

$= (X^8 + X^3 + X^2 + X) \bmod (X^8 + X^4 + X^3 + X + 1)$, **note: here reduce same element and write it once.**

$= X^4+X^2+1$

$= X^4+X^2+X^0 = 00010101$

AES Mix Column

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

*

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

=

?			

{02} * {87} ⊕ {03} * {6E} ⊕ {01} * {46} ⊕ {01} * {A6}

02 = 0000 0010 = X

87 = 1000 0111 = $X^7 + X^2 + X + 1$

02 * 87 $= X * (X^7 + X^2 + X + 1)$

$= X^8 + X^3 + X^2 + X$

$= X^4 + \cancel{X^3} + \cancel{X} + 1 + \cancel{X^3} + X^2 + \cancel{X}$

$= X^4 + X^2 + 1$

= 0001 0101

03 = 0000 0011 = $X + 1$

6E = 0110 1110 = $X^6 + X^5 + X^3 + X^2 + X$

03 * 6E $= (X+1) * (X^6 + X^5 + X^3 + X^2 + X)$

$= X^7 + \cancel{X^6} + X^4 + \cancel{X^3} + \cancel{X^2} + \cancel{X^6} + X^5 + \cancel{X^3} + \cancel{X^2} + X$

$= X^7 + X^5 + X^4 + X$

= 1011 0010

01 * 46 = 46 = 0100 0110

01 * A6 = A6 = 1010 0110

01= 0000 0001 = X^0 = 1

46 = 0100 0110 = $X^6 + X^2 + X^1$

= 01000110

$= (01) * (46) = 1 * (X^6 + X^2 + X^1) = X^6 + X^2 + X^1 = 01000110$

AES Mix Column

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

*

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

=

47			

$\{02\} * \{87\} \oplus \{03\} * \{6E\} \oplus \{01\} * \{46\} \oplus \{01\} * \{A6\} = \{47\}$

02 * 87 = 0 0 0 1 0 1 0 1
03 * 6E = 1 0 1 1 0 0 1 0
01 * 46 = 0 1 0 0 0 1 1 0
01 * A6 = 1 0 1 0 0 1 1 0

$$= \underbrace{0\,1\,0\,0}_{4}\ \underbrace{0\,1\,1\,1}_{7} = \{47\}$$

In Ex-or
Odd time 1's = 1
Even time 1's = 0

AES Mix Column

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

*

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

=

47			
?			

$\{01\} * \{87\} \oplus \{02\} * \{6E\} \oplus \{03\} * \{46\} \oplus \{01\} * \{A6\}$

01 * 87 = 87 = 1000 0111

02 = 0000 0010 = X
6E = 0110 1110 = $X^6 + X^5 + X^3 + X^2 + X$
02 * 6E = $X * (X^6 + X^5 + X^3 + X^2 + X)$
$= X^7 + X^6 + X^4 + X^3 + X^2$
= 1101 1100

03 = 0000 0110 = $X + 1$
46 = 0100 0110 = $X^6 + X^2 + X$
03 * 46 = $(X + 1) * (X^6 + X^2 + X)$
$= X^7 + X^3 + \cancel{X^2} + X^6 + \cancel{X^2} + X$
$= X^7 + X^6 + X^3 + X$
= 1100 1010

01 * A6 = A6 = 1010 0110

AES Mix Column

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

*

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

=

47			
?			

{01} * {87} ⊕ {02} * {6E} ⊕ {03} * {46} ⊕ {01} * {A6}

$$\left.\begin{array}{l} 01 * 87 = 1\,0\,0\,0\;\;0\,1\,1\,1 \\ 02 * 6E = 1\,1\,0\,1\;\;1\,1\,0\,0 \\ 03 * 46 = 1\,1\,0\,0\;\;1\,0\,1\,0 \\ 01 * A6 = 1\,0\,1\,0\;\;0\,1\,1\,0 \end{array}\right\}\text{ Perform Ex-or}$$

AES Mix Column

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

*

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

=

47			
37			

{01} * {87} ⊕ {02} * {6E} ⊕ {03} * {46} ⊕ {01} * {A6} = {37}

$$\begin{array}{l} 01 * 87 = 1\,0\,0\,0\;\;0\,1\,1\,1 \\ 02 * 6E = 1\,1\,0\,1\;\;1\,1\,0\,0 \\ 03 * 46 = 1\,1\,0\,0\;\;1\,0\,1\,0 \\ 01 * A6 = 1\,0\,1\,0\;\;0\,1\,1\,0 \\ \hline \qquad\;\; = \underbrace{0\,0\,1\,1}_{3}\;\;\underbrace{0\,1\,1\,1}_{7} = \{37\} \end{array}$$

AES Mix Column

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

*

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

=

47			
37			
?			

{01} * {87} ⊕ {01} * {6E} ⊕ {02} * {46} ⊕ {03} * {A6}

01 * 87 = 87 = 1000 0111

01 * 6E = 6E = 0110 1110

02 = 0000 0010 = X

46 = 0100 0110 = $X^6 + X^2 + X$

02 * 46 = $X * (X^6 + X^2 + X)$

$= X^7 + X^3 + X^2$

= 1000 1100

03 = 0000 0110 = X + 1

A6 = 1010 0110 = $X^7 + X^5 + X^2 + X$

03 * A6 = $(X + 1) * (X^7 + X^5 + X^2 + X)$

$= \boxed{X^8} + X^6 + X^3 + \cancel{X^2} + X^7 + X^5 + \cancel{X^2} + X$

$= X^4 + \cancel{X^3} + \cancel{X} + 1 + X^6 + \cancel{X^3} + X^7 + X^5 + \cancel{X}$

$= X^7 + X^6 + X^5 + X^4 + 1$

= 1111 0001

Use irreducible Polynomial Theorem, GF (2^3)

$X^8 = X^4 + X^3 + X + 1$

AES Mix Column

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

*

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

=

47			
37			
?			

{01} * {87} ⊕ {01} * {6E} ⊕ {02} * {46} ⊕ {03} * {A6}

01 * 87 = 1 0 0 0 0 1 1 1
01 * 6E = 0 1 1 0 1 1 1 0
02 * 46 = 1 0 0 0 1 1 0 0
03 * A6 = 1 1 1 1 0 0 0 1

Perform Ex-or

AES Mix Column

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} * \begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 90 & EC \\ 46 & E7 & 4A & C3 \\ A6 & 8C & D8 & 95 \end{bmatrix} = \begin{bmatrix} 47 & & & \\ 37 & & & \\ 94 & & & \\ & & & \end{bmatrix}$$

{01} * {87} ⊕ {01} * {6E} ⊕ {02} * {46} ⊕ {03} * {A6} = {94}

01 * 87 = 1 0 0 0 0 1 1 1
01 * 6E = 0 1 1 0 1 1 1 0
02 * 46 = 1 0 0 0 1 1 0 0
03 * A6 = 1 1 1 1 0 0 0 1

$$= \underbrace{1\,0\,0\,1}_{9}\ \underbrace{0\,1\,0\,0}_{4} = \{94\}$$

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} * \begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 90 & EC \\ 46 & E7 & 4A & C3 \\ A6 & 8C & D8 & 95 \end{bmatrix} = \begin{bmatrix} 47 & & & \\ 37 & & & \\ 94 & & & \\ ? & & & \end{bmatrix}$$

{03} * {87} ⊕ {01} * {6E} ⊕ {01} * {46} ⊕ {02} * {A6}

03 = 0000 0011 = $X + 1$
87 = 1000 0111 = $X^7 + X^2 + X + 1$

$$\begin{aligned} 03 * 87 &= (X + 1) * (X^7 + X^2 + X + 1) \\ &= \boxed{X^8} + X^3 + \cancel{X^2} + \cancel{X} + X^7 + \cancel{X^2} + \cancel{X} + 1 \\ &= X^4 + \cancel{X^3} + X + \cancel{1} + \cancel{X^3} + X^7 + \cancel{1} \\ &= X^7 + X^4 + X \\ &= 1001\ 0010 \end{aligned}$$

01 * 6E = 6E = 0110 1110

01 * 46 = 46 = 0100 0110

02 = 0000 0010 = X
A6 = 1010 0110 = $X^7 + X^5 + X^2 + X$

$$\begin{aligned} 02 * A6 &= X * (X^7 + X^5 + X^2 + X) \\ &= \boxed{X^8} + X^6 + X^3 + X^2 \\ &= X^4 + \cancel{X^3} + X + 1 + X^6 + \cancel{X^3} + X^2 \\ &= X^6 + X^4 + X^2 + X + 1 \\ &= 0101\ 0111 \end{aligned}$$

Use irreducible Polynomial Theorem, GF (2^3)
$X^8 = X^4 + X^3 + X + 1$

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} * \begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 90 & EC \\ 46 & E7 & 4A & C3 \\ A6 & 8C & D8 & 95 \end{bmatrix} = \begin{bmatrix} 47 & & & \\ 37 & & & \\ 94 & & & \\ ? & & & \end{bmatrix}$$

$\{03\} * \{87\} \oplus \{01\} * \{6E\} \oplus \{01\} * \{46\} \oplus \{02\} * \{A6\}$

$$\left.\begin{aligned} 03 * 87 &= 1\,0\,0\,1\;\;0\,0\,1\,0 \\ 01 * 6E &= 0\,1\,1\,0\;\;1\,1\,1\,0 \\ 01 * 46 &= 0\,1\,0\,0\;\;0\,1\,1\,0 \\ 02 * A6 &= 0\,1\,0\,1\;\;0\,1\,1\,1 \end{aligned}\right\} \text{Perform Ex-or}$$

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} * \begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 90 & EC \\ 46 & E7 & 4A & C3 \\ A6 & 8C & D8 & 95 \end{bmatrix} = \begin{bmatrix} 47 & & & \\ 37 & & & \\ 94 & & & \\ ED & & & \end{bmatrix}$$

$\{03\} * \{87\} \oplus \{01\} * \{6E\} \oplus \{01\} * \{46\} \oplus \{02\} * \{A6\} = \{ED\}$

$$\begin{aligned} 03 * 87 &= 1\,0\,0\,1\;\;0\,0\,1\,0 \\ 01 * 6E &= 0\,1\,1\,0\;\;1\,1\,1\,0 \\ 01 * 46 &= 0\,1\,0\,0\;\;0\,1\,1\,0 \\ 02 * A6 &= 0\,1\,0\,1\;\;0\,1\,1\,1 \\ \hline &= \underbrace{1\,1\,1\,0}_{E}\;\;\underbrace{1\,1\,0\,1}_{D} = \{ED\} \end{aligned}$$

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

*

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

=

47	?		
37			
94			
ED			

{02} * {F2} ⊕ {03} * {4C} ⊕ {01} * {E7} ⊕ {01} * {8C}

02 = 0000 0010 = X

F2 = 1111 0010 = $X^7 + X^6 + X^5 + X^4 + X$

02 * F2 $= X * (X^7 + X^6 + X^5 + X^4 + X)$

$= \boxed{X^8} + X^7 + X^6 + X^5 + X^2$

$= X^4 + X^3 + X + 1 + X^7 + X^6 + X^5 + X^2$

$= X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$

= 1111 1111

Use irreducible Polynomial Theorem, GF (2^3)

$\mathbf{X^8 = X^4 + X^3 + X + 1}$

03 = 0000 0011 = $X + 1$

4C = 0100 1100 = $X^6 + X^3 + X^2$

03 * 4C $= (X+1) * (X^6 + X^3 + X^2)$

$= X^7 + X^4 + \cancel{X^3} + X^6 + \cancel{X^3} + X^2$

$= X^7 + X^6 + X^4 + X^2$

= 1101 0100

01 * E7 = E7 = 1110 0111

01 * 8C = 8C = 1000 1100

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

*

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

=

47	?		
37			
94			
ED			

{02} * {F2} ⊕ {03} * {4C} ⊕ {01} * {E7} ⊕ {01} * {8C}

02 * F2 = 1 1 1 1 1 1 1 1

03 * 4C = 1 1 0 1 0 1 0 0

01 * E7 = 1 1 1 0 0 1 1 1

01 * 8C = 1 0 0 0 1 1 0 0

Perform Ex-or

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

*

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

=

47	40		
37			
94			
ED			

{02} * {F2} ⊕ {03} * {4C} ⊕ {01} * {E7} ⊕ {01} * {8C} = {40}

02 * F2 = 1 1 1 1 1 1 1 1
03 * 4C = 1 1 0 1 0 1 0 0
01 * E7 = 1 1 1 0 0 1 1 1
01 * 8C = 1 0 0 0 1 1 0 0

$$= \underbrace{0\,1\,0\,0}_{4}\ \underbrace{0\,0\,0\,0}_{0} = \{40\}$$

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

*

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

=

47	40		
37	?		
94			
ED			

{01} * {F2} ⊕ {02} * {4C} ⊕ {03} * {E7} ⊕ {01} * {8C}

- Like this we convert all byte of 4 * 4 matrix and final byte will be as…

AES Mix Column

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

*

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

=

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	?

{03} * {97} ⊕ {01} * {EC} ⊕ {01} * {C3} ⊕ {02} * {95}

03 = 0000 0011 $= X + 1$

97 = 1001 0111 $= X^7 + X^4 + X^2 + X + 1$

03 * 97 $= (X + 1) * (X^7 + X^4 + X^2 + X + 1)$

$= \boxed{X^8} + X^5 + X^3 + \cancel{X^2} + \cancel{X} + X^7 + X^4 + \cancel{X^2} + \cancel{X} + 1$

$= \cancel{X^4} + \cancel{X^3} + X + \cancel{1} + X^7 + X^5 + \cancel{X^4} + \cancel{X^3} + \cancel{1}$

$= X^7 + X^5 + X$

= 1010 0010

02 = 0000 0010 $= X$

95 = 1001 0101 $= X^7 + X^4 + X^2 + 1$

02 * 95 $= X * (X^7 + X^4 + X^2 + 1)$

$= \boxed{X^8} + X^5 + X^3 + X$

$= X^4 + \cancel{X^3} + \cancel{X} + 1 + X^5 + \cancel{X^3} + \cancel{X}$

$= X^5 + X^4 + 1$

= 0011 0001

01 * EC = EC = 1110 1100

01 * C3 = C3 = 1100 0011

Use irreducible Polynomial Theorem, GF (2^3)

$X^8 = X^4 + X^3 + X + 1$

-

AES Mix Column

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} * \begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 90 & EC \\ 46 & E7 & 4A & C3 \\ A6 & 8C & D8 & 95 \end{bmatrix} = \begin{bmatrix} 47 & 40 & A3 & 4C \\ 37 & D4 & 70 & 9F \\ 94 & E4 & 3A & 42 \\ ED & A5 & A6 & BC \end{bmatrix}$$

$$\{03\} * \{97\} \oplus \{01\} * \{EC\} \oplus \{01\} * \{C3\} \oplus \{02\} * \{95\} = \{BC\}$$

$$\begin{aligned} 03 * 97 &= 1010\ 0010 \\ 01 * EC &= 1110\ 1100 \\ 01 * C3 &= 1100\ 0011 \\ 02 * 95 &= 0011\ 0001 \\ \hline &= \underbrace{1011}_{B}\ \underbrace{1100}_{C} = \{BC\} \end{aligned}$$

❖ So, output of Mix column will become input to 4th transformation of round function i.e., **Add Round key**

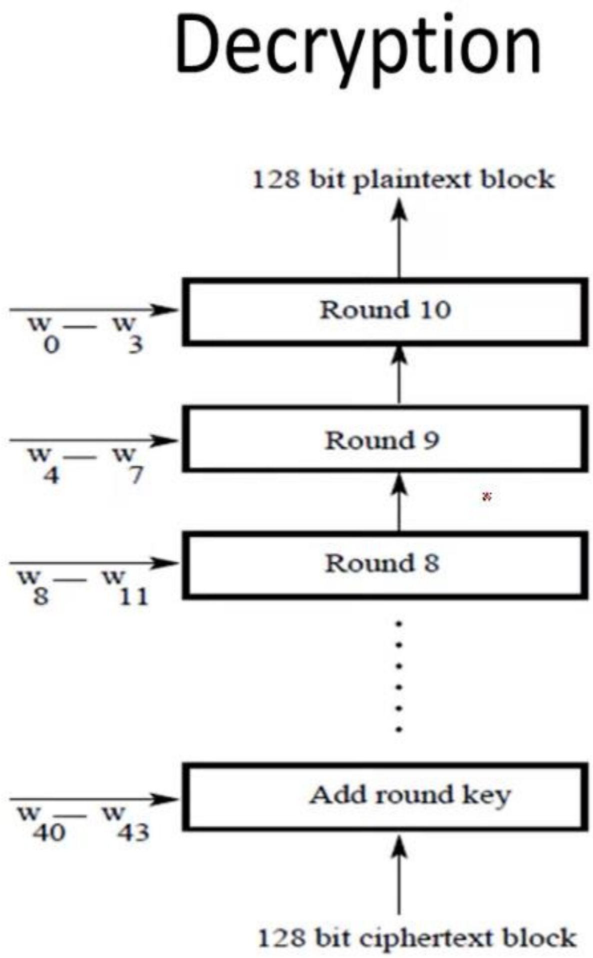
Add Round key

- In the forward add round key transformation, called AddRoundKey, the 128 bits of State are bitwise XORed with the 128 bits of the round key.
- For round 1 it is W4, W5, W6, W7 (sub key) is used.

$$\begin{bmatrix} r_1 & r_5 & r_9 & r_{13} \\ r_2 & r_6 & r_{10} & r_{14} \\ r_3 & r_7 & r_{11} & r_{15} \\ r_4 & r_8 & r_{12} & r_{16} \end{bmatrix} \oplus \boxed{\text{Sub Key W4 W5 W6 W7}}$$

- And output of round 1 i.e,.4*4 matrix will be input of round 2.
- Like this we have to perform up to N-1 Round.
- At the last Round N, the output of Round N - 1 is the input of Round N which is the last round and it has only 3 Transformation i.e., Substitute Bytes (Sub-Bytes), Shift Rows and Add Round Key. We do not perform Mix columns in last round.
- And output of last round is Cipher text.

AES Decryption



Decryption -Round

- Substitute Bytes (Sub-Bytes)
- Shift Rows
- Mix Columns – (Not applicable for last round)
- Add Round Key

Substitute Bytes (Sub-Bytes)

- Substitute Bytes- an inverse S box is used for Bytes Substitution

Inverse S-Box

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
10	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
20	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
30	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
40	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
50	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
60	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
70	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
80	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
90	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a0	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b0	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c0	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d0	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e0	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f0	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

- Shift Rows – Rows are shifted right in decryption
  - First row: No change
  - Second row: one-byte cyclical right shift
  - Third row: two - byte cyclical right shift
  - Fourth row: three - byte cyclical right shift

$$\begin{bmatrix} 63 & 47 & a2 & f0 \\ 9c & 63 & c5 & f2 \\ 7b & 7c & f0 & ab \\ ca & af & 76 & 76 \end{bmatrix}$$

$$\begin{bmatrix} 63 & 47 & a2 & f0 \\ f2 & 9c & 63 & c5 \\ f0 & ab & 7b & 7c \\ af & 76 & 76 & ca \end{bmatrix}$$

- Mix Columns

We use pre-defined 4*4 matrix in encryption

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} 63 & 47 & a2 & f0 \\ 9c & 63 & c5 & f2 \\ 7b & 7c & f0 & ab \\ ca & af & 76 & 76 \end{bmatrix}$$

Here we use another pre-defined 4*4 matrix in decryption and multiply with output of shift rows state array matrix.

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

$$* \begin{bmatrix} r_1 & r_5 & r_9 & r_{13} \\ r_2 & r_6 & r_{10} & r_{14} \\ r_3 & r_7 & r_{11} & r_{15} \\ r_4 & r_8 & r_{12} & r_{16} \end{bmatrix}$$

- Add Round Key
    - ✓ Here output of mix columns will be xored with subkey of round 1 i.e., W36, W37, W38 and W39.
    - ✓ And after performing all round we get plaintext.