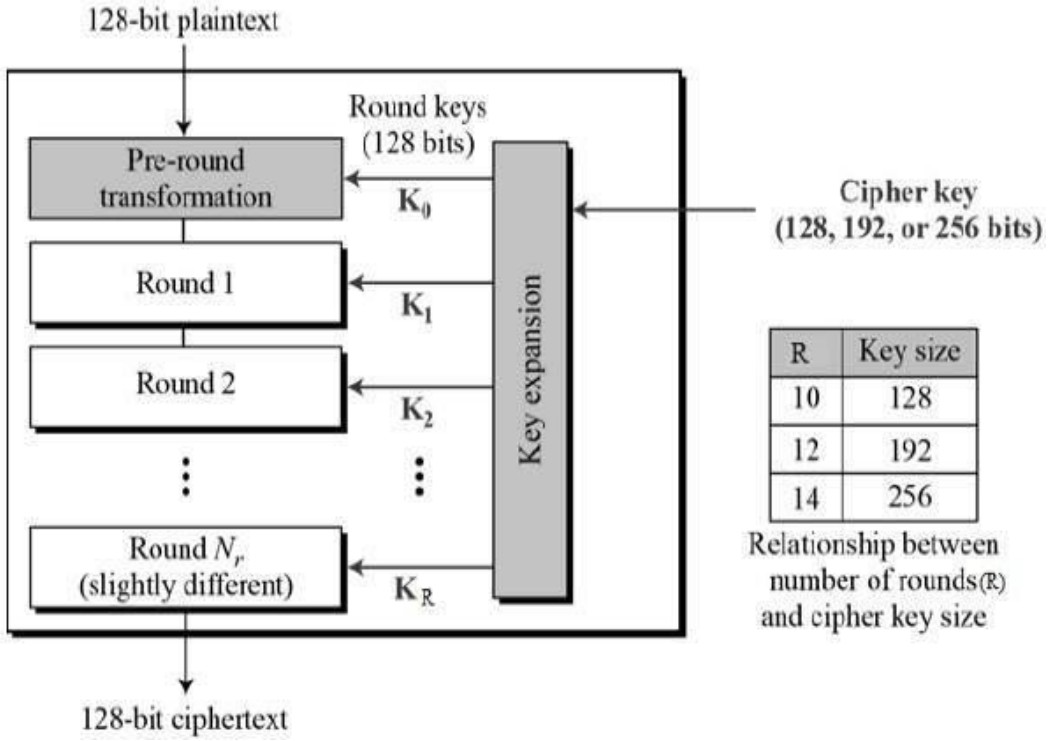
AES Algorithm

ADVANCED ENCRYPTION STANDARD

Overview

- **Overview of the AES Algorithm.**
- **It's a Block Cipher**
- **Encrypts blocks of size 128 bits where DES 64 bits.**
- **Uses a key of size 128, 192, and 256 bits where DES 56 bits.**



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

- Symmetric cipher: uses same key for encryption and decryption.
- Uses multiple rounds which all perform the identical operations.
- Different subkey in each round derived from main key

Key Generation

- **Key in binary is 128,192 and 256 bits.**
- **Key is in hexadecimal (16 bytes).**
- **We will divide key into words (8 bit each).**
- **We will fill the words into the matrix.**

Key (128 bits) –

01110011011000010111010001101001011100110
11010000110001101101010011010010111001101
10001001101111011100100110100101101110011
00111

Key in Hex

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

$$\begin{bmatrix} b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \\ b_4 & b_8 & b_{12} & b_{16} \end{bmatrix} \quad \begin{bmatrix} 73 & 73 & 69 & 72 \\ 61 & 68 & 73 & 69 \\ 74 & 63 & 62 & 6e \\ 69 & 6a & 6f & 67 \end{bmatrix}$$

Key Generation

$$\begin{bmatrix} b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \\ b_4 & b_8 & b_{12} & b_{16} \end{bmatrix} \qquad \begin{bmatrix} 73 & 73 & 69 & 72 \\ 61 & 68 & 73 & 69 \\ 74 & 63 & 62 & 6e \\ 69 & 6a & 6f & 67 \end{bmatrix}$$

- **Key 128 bits.**
- **Word is a 32 bits = 4 byte.**
- **For 128 key bit we will have from W0 to W43.**
- **For 192 key bit we will have from W0 to W51.**
- **For 256 key bit we will have from W0 to W59.**

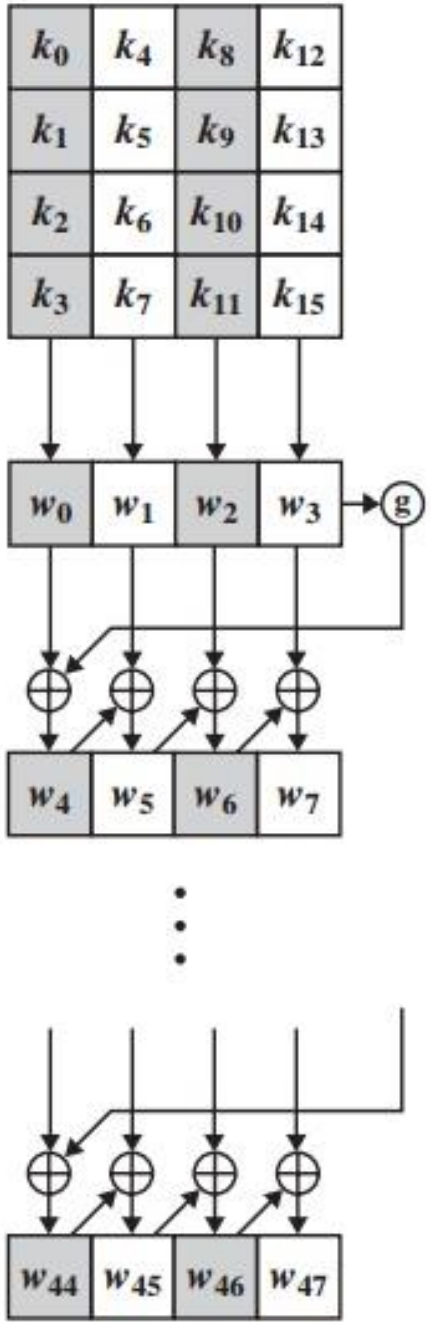
- **HOW CAN WE GENERATE OTHER WORDS?**

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							

Key Generation

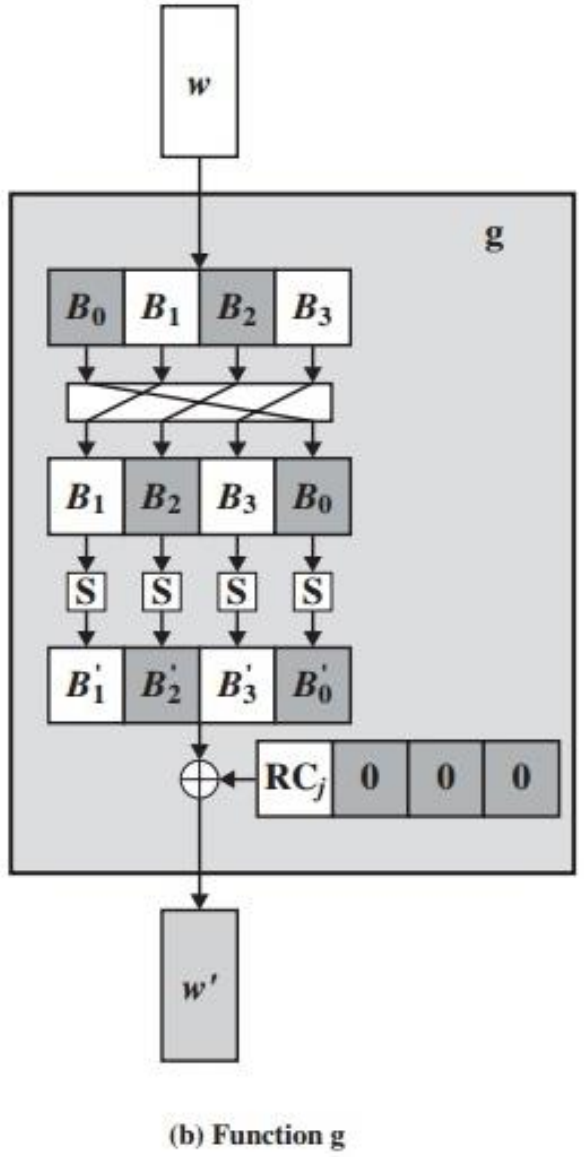
W0	W1	W2	W3	W4	W5	W6	W7	.....	.....	W43
73 61 74 69	73 68 63 6a	69 73 62 6f	72 69 6e 67							



- **W4 = W0 XOR g(W3)**
- **WHAT IS g FUNCTION?**

Key Generation

W3	RotWord (X1)
72	69
69	6e
6e	67
67	72



(b) Function g

❖ **g FUNCTION**

1. **RotWord 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].**
2. **SubWord performs a byte substitution on each byte of its input word, using the S-box.**
3. **The result of steps 1 and 2 is XORed with a round constant, Rcon[j].**

S-Box

		Y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
X	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

Key Generation

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

- **g FUNCTION**

1. **RotWord 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].**
2. **SubWord performs a byte substitution on each byte of its input word, using the S-box.**
3. **The result of steps 1 and 2 is XORed with a round constant, Rcon[j].**

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

g(w3) F8 9F 85 40

Y1	11111001100111111000010101000000
R1	00000001000000000000000000000000
g(w3)	11111000100111111000010101000000

Key Generation

- **W4 = W0 XOR g(W3)**

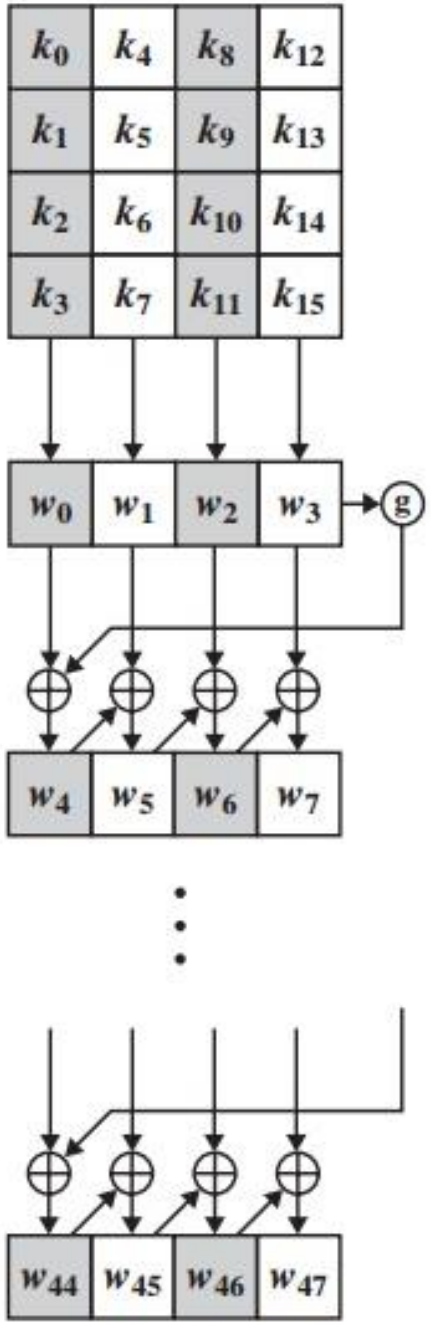
W0	W1	W2	W3	W4	W5	W6	W7	.....	.....	W43
73 61 74 69	73 68 63 6a	69 73 62 6f	72 69 6e 67	8b fe f1 29	f8 96 92 43	91 e5 f0 2c	e3 8c 9e 4b			

W0 01110011011000010111010001101001

g(w3) 11111000100111111000010101000000

W4 10001011111111011111000100101001

8b fe f1 29

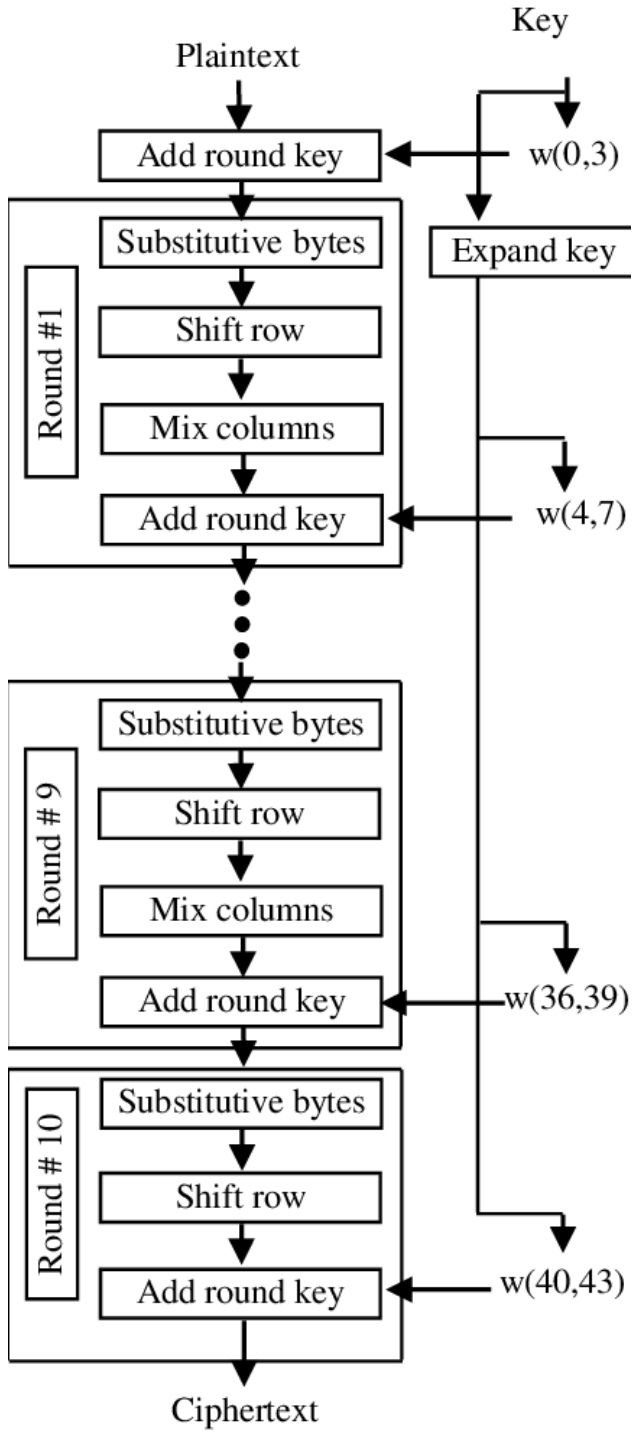


AES Encryption

- **Divide plain text to blocks of 128 bit block size**
- **Add round Key XOR with Plaintext**
- **Each round consists of a number of layers:**
  - **Byte substitution layer**
  - **Diffusion layer**
    - **Shift Rows**
    - **Mix Columns**
  - **Key addition layer**

After XORING

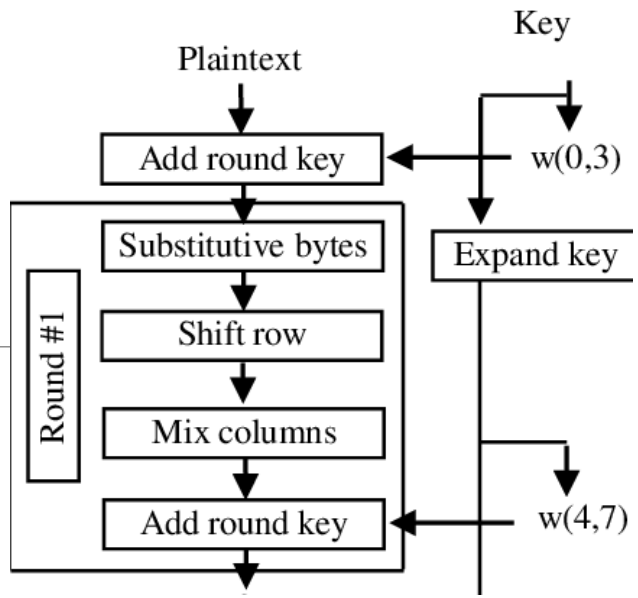
$$\begin{bmatrix} 00 & 16 & 1a & 17 \\ 04 & 1c & 00 & 07 \\ 17 & 0e & 03 & 01 \\ 1b & 0f & 0f & 10 \end{bmatrix}$$



S-Box

		Y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
X	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

AES Encryption

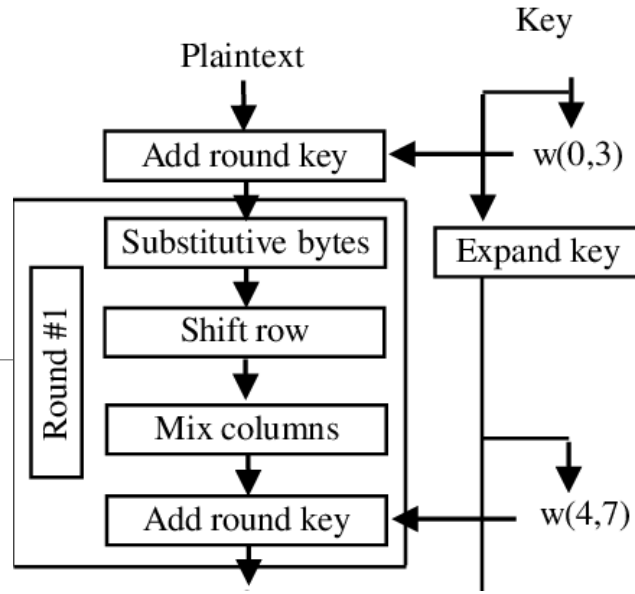


- **Byte substitution layer**

$$\begin{bmatrix} 00 & 16 & 1a & 17 \\ 04 & 1c & 00 & 07 \\ 17 & 0e & 03 & 01 \\ 1b & 0f & 0f & 10 \end{bmatrix} \rightarrow \begin{bmatrix} 63 & 47 & a2 & f0 \\ f2 & 9c & 63 & c5 \\ f0 & ab & 7b & 7c \\ af & 76 & 76 & ca \end{bmatrix}$$

AES Encryption

- **Diffusion layer**
  - **Shift Rows**
  - **Mix Columns**



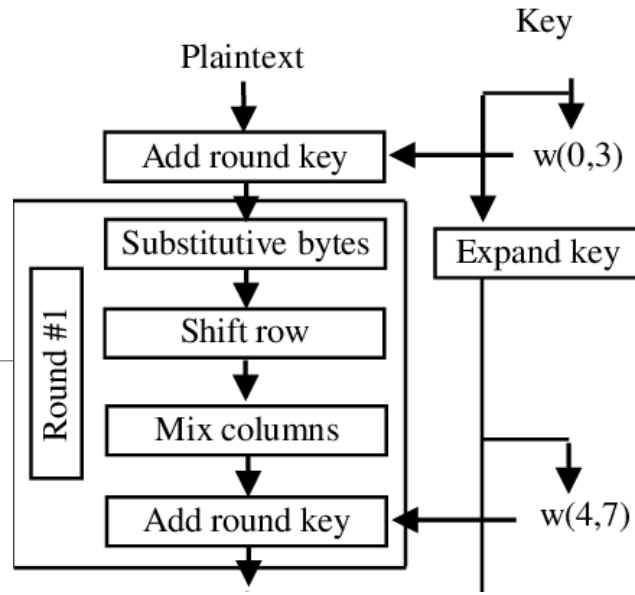
$$\begin{bmatrix} 63 & 47 & a2 & f0 \\ f2 & 9c & 63 & c5 \\ f0 & ab & 7b & 7c \\ af & 76 & 76 & ca \end{bmatrix} \rightarrow \begin{bmatrix} 63 & 47 & a2 & f0 \\ 9c & 63 & c5 & f2 \\ 7b & 7c & f0 & ab \\ ca & af & 76 & 76 \end{bmatrix}$$

B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

the output is the new state:

B_0	B_4	B_8	B_{12}	no shift
B_5	B_9	B_{13}	B_1	← one position left shift
B_{10}	B_{14}	B_2	B_6	← two positions left shift
B_{15}	B_3	B_7	B_{11}	← three positions left shift

AES Encryption



- **Diffusion layer**
  - **Shift Rows**
  - **Mix Columns (Last Round doesn't involve Mix Columns)**

$$\begin{bmatrix} 63 & 47 & a2 & f0 \\ 9c & 63 & c5 & f2 \\ 7b & 7c & f0 & ab \\ ca & af & 76 & 76 \end{bmatrix} * \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \rightarrow \begin{bmatrix} r_1 & r_5 & r_9 & r_{13} \\ r_2 & r_6 & r_{10} & r_{14} \\ r_3 & r_7 & r_{11} & r_{15} \\ r_4 & r_8 & r_{12} & r_{16} \end{bmatrix}$$

r1 -> 63*02 + 9c*03 + 7b*01 + ca*01
63: 01100011 -> x^6 + x^5 + x + 1
02: 00000010 -> x
63*02 -> (x^6 + x^5 + x+1)*x -> x^7+x^6+x^2+x -> 11000110
r1 -> x^8 + x^7 + x^6 + x^4 + x +1 (111010011) Where p(x) -> x^8 + x^4 + x^3 + x+1 (100011011)
R1 -> C8

111010011
divided
100011011
11001000 (C8)

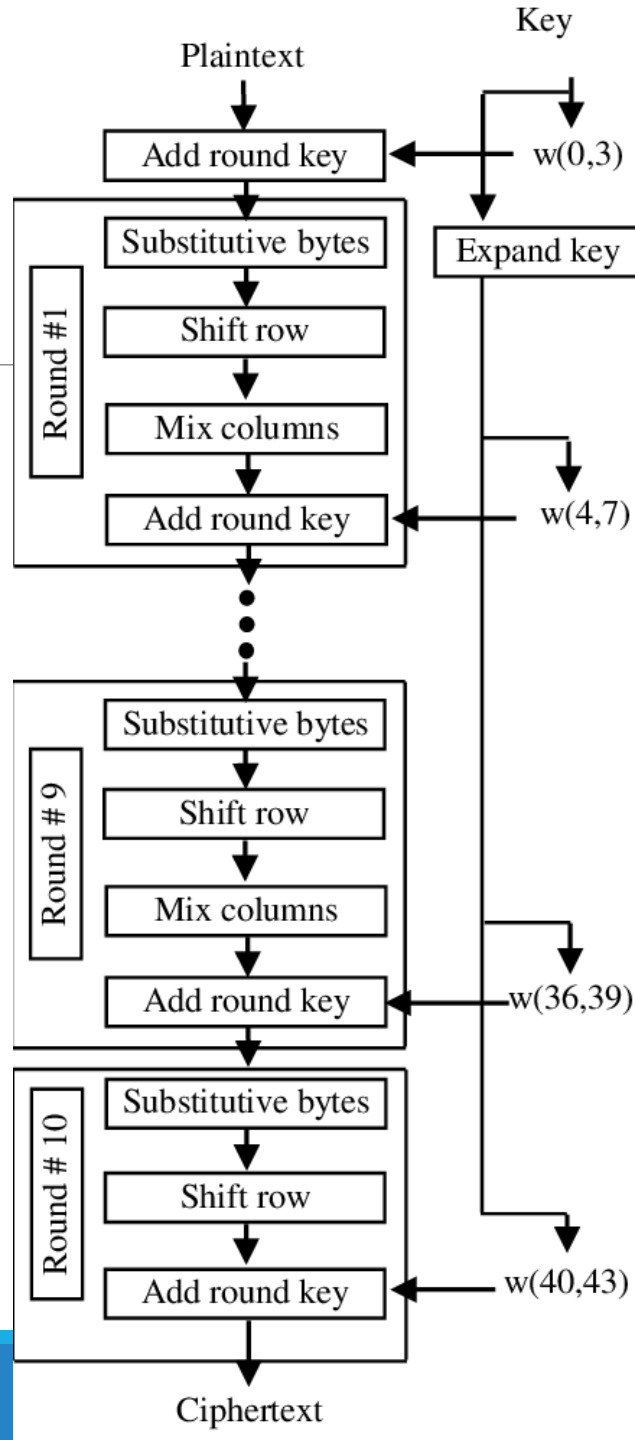
AES Encryption

- **Key addition layer**

W0	W1	W2	W3	W4	W5	W6	W7	.....	.....	W43
73	73	69	72	8b	f8	91	e3			
61	68	73	69	fe	96	e5	8c			
74	63	62	6e	f1	92	f0	9e			
69	6a	6f	67	29	43	2c	4b			

XORING

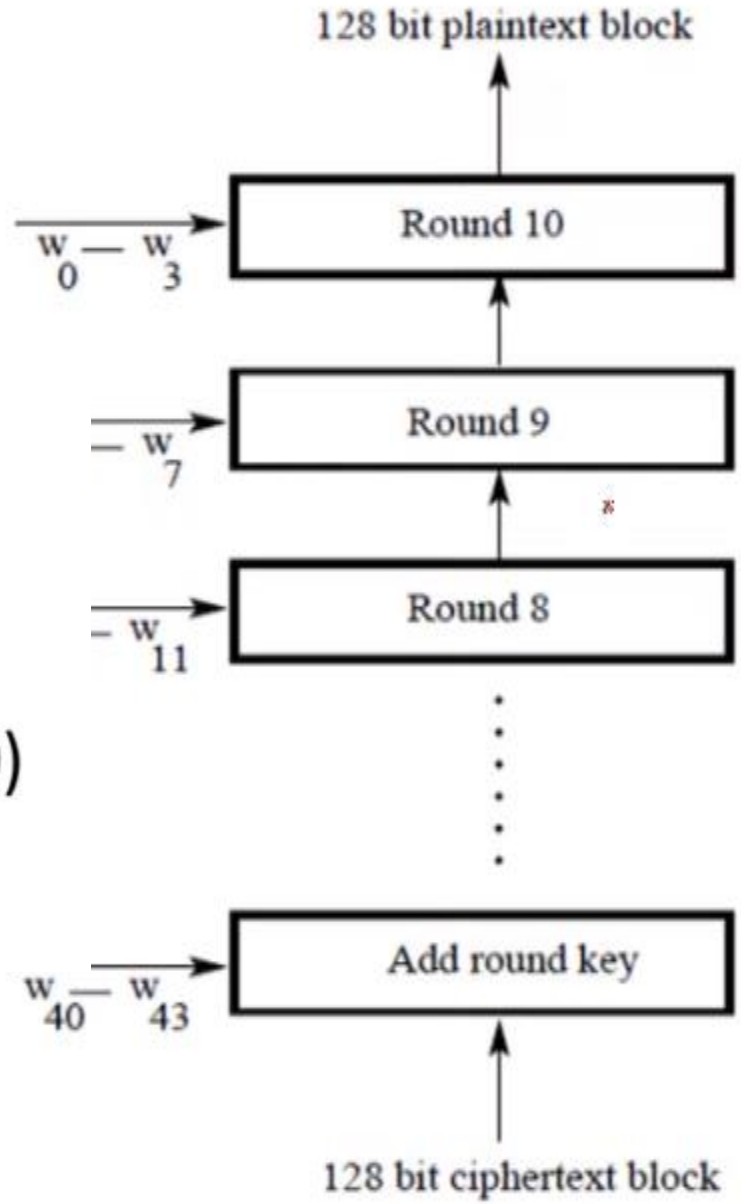
$$\begin{bmatrix} r_1 & r_5 & r_9 & r_{13} \\ r_2 & r_6 & r_{10} & r_{14} \\ r_3 & r_7 & r_{11} & r_{15} \\ r_4 & r_8 & r_{12} & r_{16} \end{bmatrix}$$



AES Decryption

Round has the following steps

- Substitution Bytes
- Shift Rows
- Mixing Columns (Not applicable for Round 10)
- Add round key



AES Decryption

- **Byte substitution layer**
- **Diffusion layer**
  - **Inv Shift Rows**
  - **Inv Mix Columns (Last Round doesn't involve Mix Columns)**

x \ y	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

B_0	B_4	B_8	B_{12}
B_{13}	B_1	B_5	B_9
B_{10}	B_{14}	B_2	B_6
B_7	B_{11}	B_{15}	B_3

no shift

→ one position right shift

→ two positions right shift

→ three positions right shift

$$\begin{pmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix}$$

Assignment

Use AES to encrypt and decrypt a message with the following requirements for the AES:

- You will make the user choose between 128 bits, 192 bits 256 bits key.
- Key will be entered in hexadecimal format.
- Message will be entered in hexadecimal format.
- You have to show every step results in the CLI.
- Sbox will be the same as mentioned in the slides (in hexadecimal format).
- You should decrypt the message and get the original one in hexadecimal format.
- Note: the whole team must understand the whole code.
- Will be submitted on blackboard by max 18th of Dec 2021, and will be discussed on that next lab.