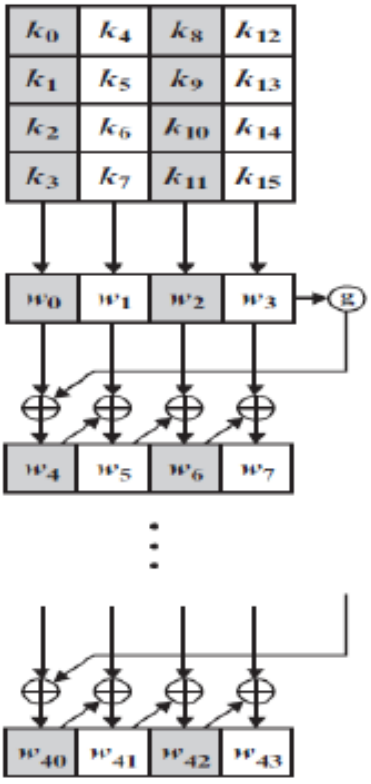
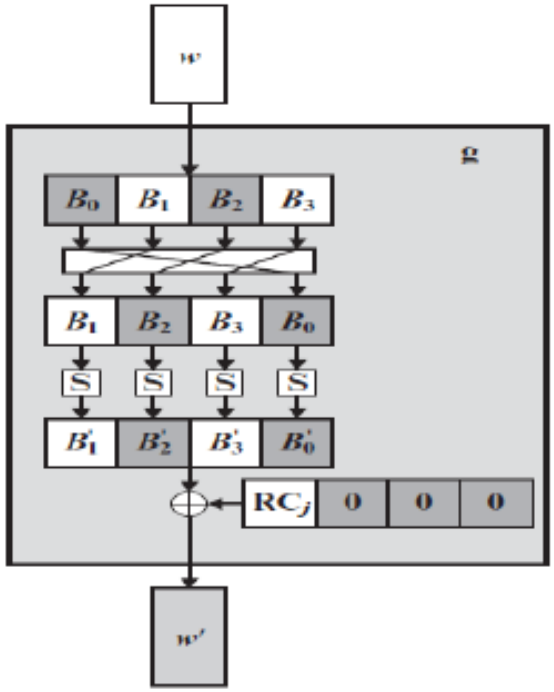
Example: Encrypt the given plaintext using AES algorithm. Consider the given master key to generate the round keys.

Plaintext in Hex : 54 77 6F 20 4F 6E 65 20 4E 69 6E 65 20 54 77 6F

Master key in Hex: 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75

Solution: We generate the 10 round key form given master key, we divide the given key into four word each word has 4 bytes.





Function g

Key in matrix form:

54	73	20	67
68	20	4B	20
61	6D	75	46
74	79	6E	75

Key in word form:

w_0	w_1	w_2	w_3
54 68 61 74	73 20 6D 79	20 4B 75 6E	67 20 46 75

Step1: RotWord performs a one-byte circular left shift on word (w_3).

$w_{[3]}$			
B_0	B_1	B_2	B_3
67	20	46	75

$w_{[3]}$			
B_1	B_2	B_3	B_0
20	46	75	67

Step2: SubWord performs a byte substitution on each byte of its input word, using the S-box.

x \ y	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

B_1	B_2	B_3	B_0
B7	5A	9D	85

Step3: The result of step 2 is XORed with a round constant, Rcon [j].

j	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36

Adding round constant (01 00 00 00) to do XOR with the results form step 2:

RC_1	0000 0001	0000 0000	0000 0000	0000 0000
$W_{[3]}$	1011 0111	0101 1010	1001 1101	1000 0101
XOR ($g(W_{[3]})$)	1011 0110	0101 1010	1001 1101	1000 0101
$g(W_{[3]})$ HEX	B6	5A	9D	85

$g(W_{[3]})$	B6	5A	9D	85
$W_{[0]}$	54	68	61	74
XOR($W_{[4]}$)	E2	32	FC	F1

$W_{[4]}$	E2	32	FC	F1
$W_{[1]}$	73	20	6D	79
XOR($W_{[5]}$)	91	12	91	88

$W_{[5]}$	91	12	91	88
$W_{[2]}$	20	4B	75	6E
XOR($W_{[6]}$)	B1	59	E4	E6

$W_{[6]}$	B1	59	E4	E6
$W_{[3]}$	67	20	46	75
XOR($W_{[7]}$)	D6	79	A2	93

First round key: E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93

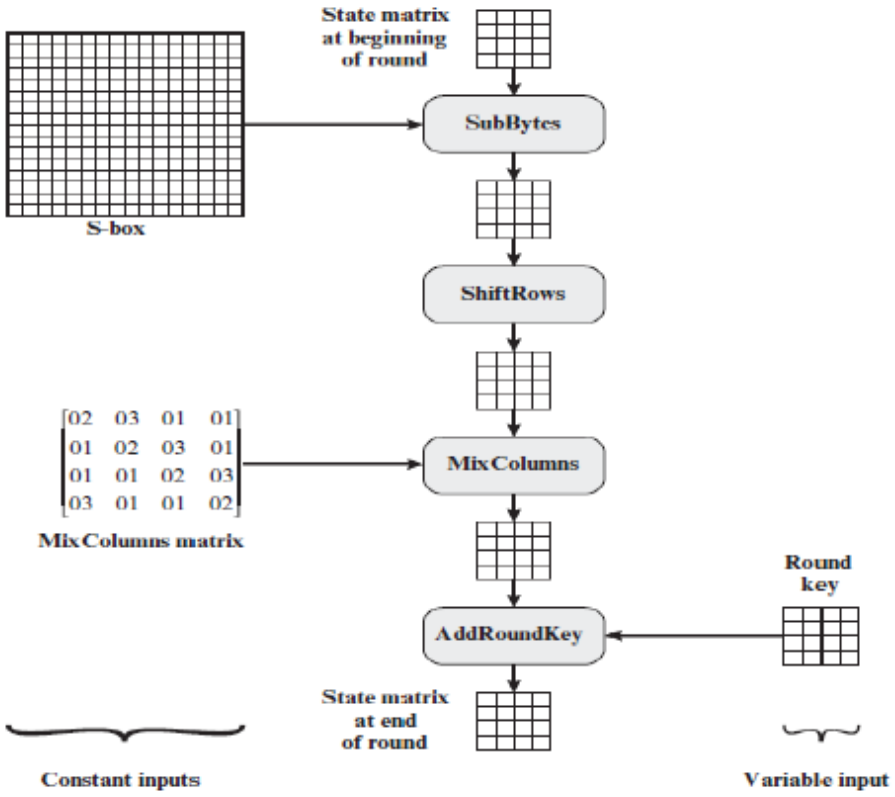
By using the same procedure to get the full 10 rounds sub key:

Initial round	54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75
Round 1	E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93
Round 2	56 08 20 07 C7 1A B1 8F 76 43 55 69 A0 3A F7 FA
Round 3	D2 60 0D E7 15 7A BC 68 63 39 E9 01 C3 03 1E FB
Round 4	A1 12 02 C9 B4 68 BE A1 D7 51 57 A0 14 52 49 5B
Round 5	B1 29 3B 33 05 41 85 92 D2 10 D2 32 C6 42 9B 69
Round 6	BD 3D C2 B7 B8 7C 47 15 6A 6C 95 27 AC 2E 0E 4E
Round 7	CC 96 ED 16 74 EA AA 03 1E 86 3F 24 B2 A8 31 6A
Round 8	8E 51 EF 21 FA BB 45 22 E4 3D 7A 06 56 95 4B 6C
Round 9	BF E2 BF 90 45 59 FA B2 A1 64 80 B4 F7 F1 CB D8
Round 10	28 FD DE F8 6D A4 24 4A CC C0 A4 FE 3B 31 6F 26

For the main process:

Step1: Plaintext is broken into blocks consisting of 16 bytes

54	4F	4E	20
77	6E	69	54
6F	65	6E	77
20	20	65	6F



The initial key adding (XOR) between plaintext and initial key as following:

54	4F	4E	20
77	6E	69	54
6F	65	6E	77
20	20	65	6F

$\oplus$

54	73	20	67
68	20	4B	20
61	6D	75	46
74	79	6E	75

=

00	3C	6E	47
1F	4E	22	74
0E	08	1B	31
54	59	0B	1A

Step 2: **(Round 1)**: The 4 × 4 byte matrix undergoes a **Substitute bytes** using an S-box table to perform a 4 × 4 substitution of the block. The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value.

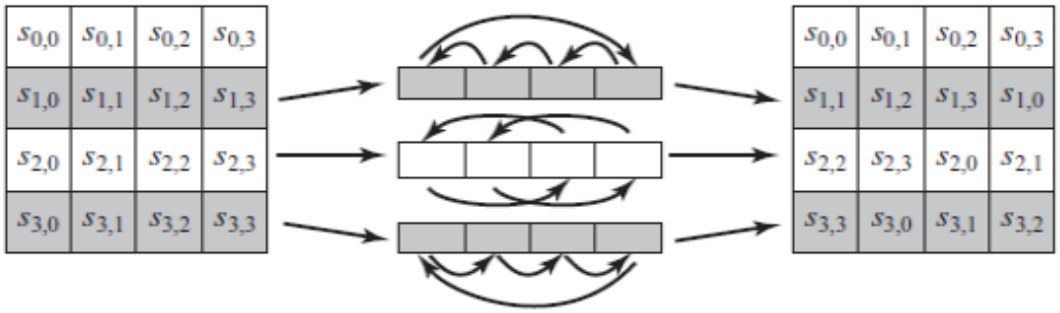
		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	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

00	3C	6E	47
1F	4E	22	74
0E	08	1B	31
54	59	0B	1A

S-Box substitution

63	EB	9F	A0
C0	2F	93	92
AB	30	AF	C7
20	CB	2B	A2

Step3: The output of Substitute bytes **is** 4 × 4 byte matrix need to throughout **shift row transformation**.



63	EB	9F	A0
C0	2F	93	92
AB	30	AF	C7
20	CB	2B	A2

Lift shift

63	EB	9F	A0
2F	93	92	C0
AF	C7	AB	30
A2	20	CB	2B

Step4: The output of shift row transformation bytes is 4×4 byte matrix need to throughout **mix column transformation (MixColumns)** operates on each column individually.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{bmatrix} = \begin{bmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{bmatrix}$$

02.63	$x\,(x^6 + x^5 + x + 1)$	$x^7 + x^6 + x^2 + x$	**1100 0110**
$03.2F$	$(x + 1)(x^5 + x^3 + x^2 + x + 1)$	$x^6 + x^5 + x^4 + 1$	**01110001**
$01.AF$	$(1)(x^7 + x^5 + x^3 + x^2 + x + 1)$	$(x^7 + x^5 + x^3 + x^2 + x + 1)$	**10101111**
$01.A2$	$(1)(x^7 + x^5 + x)$	$(x^7 + x^5 + x)$	**10100010**
		XOR	**10111010**

Step5: add round key transformation, the 128 bits (4 × 4 byte matrix) of the results from MixColumns are bitwise XORed with the 128 bit (4 × 4 byte matrix) round key.

BA	84	E8	1B
75	A4	8D	40
F4	8D	06	7D
7A	32	0E	5D

$\oplus$

E2	91	B1	D6
32	12	59	79
FC	91	E4	A2
F1	88	E6	93

=

58	15	59	CD
47	B6	D4	39
08	1C	E2	DF
8B	BA	E8	CE

After applying the same process to complete the results of all 9 round. The results of last one round 10 are:

After substitute byte the results is:

01	3A	8C	21
33	3E	B0	E2
3D	B8	8E	04
BC	4D	1C	A7

After shift rows:

01	3A	8C	21
3E	B0	E2	33
8E	04	3D	B8
A7	BC	4D	1C

Note: no Mixcolumns in last round

After XOR with round key 10:

29	57	40	1A
C3	14	22	02
50	20	99	D7
5F	F6	B3	3A

The final cipher text is: **29 C3 50 5F 57 14 20 F6 40 22 99 B3 1A 02 D7 3A**