AES KEY ENCRYPTION

1. KEY & Hexadecimal values:-

KEY: MY NAME IS LAIBAAMB

~~KEY: M Y N A M E IS L A I B A A M B~~
~~HEX: 4D~~

KEY: M Y N A M E I S L
HEX: 4D 59 4E 41 4D 45 49 53 4C
KEY: A I B A A M B
HEX: 41 49 42 41 41 4D 42

2. AES Scheduling algo:- to generate 2 random keys.

KEY WORDS

w_0 = 4D 59 4E 41
w_1 = 4D 45 49 53
w_2 = 4C 41 49 42
w_3 = 41 41 4D 42

Auxiliary Functions

→ Circular byte L.S(w_3):
= (41 4D 42 41)

→ Byte Substitution (S-box):
(83 E3 2C 83)

→ Adding round constant:
For round 1, g[w_3] (01 00 00 00)

R.C ⊕ B.S

~~= (01 00 00 00) ⊕ (83 E3 2C 83)~~
= (01 00 00 00) ⊕ (83 E3 2C 83)
= (82 E3 2C 83)

AES KEY ENCRYPTION

1. KEY & Hexadecimal values:-
   KEY: MY NAME IS LAIBAAMB

KEY:	M	Y	N	A	M	E	I	S
HEX:	4D	59	4E	41	4D	45	49	53
KEY:	L	A	I	B	A	A	M	B
HEX:	4C	41	49	42	41	41	4D	42

2. Generation of two round keys:-

KEY WORDS

w_0 = 4D 59 4E 41
w_1 = 4D 45 49 53
w_2 = 4C 41 49 42
w_3 = 41 41 4D 42

Auxiliary functions:- Pass w_3 from g function
- Circular byte left shift of w_3:
  (41 4D 42 41)
- Byte substitution (S-box):
  (83 E3 2C 83)
- Adding Round Constant:

For round 1: ~~g(w3)~~ (01 00 00 00)

$g(w_3) = R.C \oplus B.S$
= (01 00 00 00) ⊕ (83 E3 2C 83)
= (82 E3 2C 83)

$W_4 = W_0 \oplus g(W_3)$

$= (4D\ 59\ 46\ 41) \oplus (82\ E3\ 2C\ 83)$

$= (CF\ BA\ 62\ C2)$

$W_5 = W_1 \oplus W_4$

$= (4D\ 45\ 49\ 53) \oplus (CF\ BA\ 62\ C2)$

$= (82\ FF\ 2B\ 91)$

$W_6 = W_2 \oplus W_5$

$= (4C\ 41\ 49\ 42) \oplus (82\ FF\ 2B\ 91)$

$= (CE\ BE\ 62\ D3)$

$W_7 = W_3 \oplus W_6$

$= (41\ 41\ 4D\ 42) \oplus (CE\ BE\ 62\ D3)$

$= (8F\ FF\ 2F\ 91)$

Now, Auxiliary Function of W_7:-

Pass W_7 from g-function:-

- Circular byte left shift of W_7:
  (FF 2F 91 8F)
- Byte substitution (S-box):
  (16 15 81 73)
- Adding round constant:

for round 2: (02 00 00 00)

$g(W_7) = R.C + B.S$

$= (02\ 00\ 00\ 00) + (16\ 15\ 81\ 73)$

$= (14\ 15\ 81\ 73)$

$W_8 = W_4 + g(W_7)$

$= (CF\ BA\ 62\ C2) \oplus (14\ 15\ 81\ 73)$

$= (DB\ AF\ E3\ B1)$

$W_9 = W_5 + g\ W_8$

$= (82\ FF\ 2B\ 91) \oplus (DB\ AF\ E3\ B1)$

$= (59\ 50\ C8\ 20)$

$W_{10} = W_6 + W_9$

$= (CE\ BE\ 62\ D3) \oplus (59\ 50\ C8\ 20)$

$= (97\ EE\ AA\ F3)$

$W_{11} = W_7 + W_{10}$

$= (8F\ FF\ 2F\ 91) \oplus (97\ EE\ AA\ F3)$

$= (18\ 11\ 85\ 62)$

Now,

KEY WORDS

$W_0 = 4D\ 59\ 4E\ 41$

$W_1 = 4D\ 45\ 49\ 53$

$W_2 = 4C\ 41\ 49\ 42$

$W_3 = 41\ 41\ 4D\ 42$

$W_4 = CF\ BA\ 62\ C2$

$W_5 = 82\ FF\ 2B\ 91$

$W_6 = CE\ BE\ 62\ D3$

$W_7 = 8F\ FF\ 2F\ 91$

$W_8 = DB\ AF\ E3\ B1$

$W_9 = 59\ 50\ C8\ 20$

$W_{10} = 97\ EE\ AA\ F3$

$W_{11} = 18\ 11\ 85\ 62$

KEY 0:

4D	4D	4C	41
59	45	41	41
4E	49	49	4D
41	53	42	42

KEY 1:

CF	82	CE	8F
BA	FF	BE	FF
62	2B	62	2F
C2	91	D3	91

KEY 2:

DB	59	97	18
AF	50	EE	11
E3	C8	AA	85
B1	20	F3	62

Initialization Vector:

$$I.V = \begin{bmatrix} 12 & 90 & FE & 76 \\ 34 & AB & DC & 54 \\ 56 & CD & BA & 32 \\ 78 & EF & 98 & 10 \end{bmatrix}$$

Plaintext: I S I A M A B A
Hex: 49 53 4C 41 4D 41 42 41
Plaintext: D I S T H E C A
Hex: 44 49 53 54 48 45 43 41

$$P = \begin{bmatrix} 49 & 4D & 44 & 48 \\ 53 & 41 & 49 & 45 \\ 4C & 42 & 53 & 43 \\ 41 & 41 & 54 & 41 \end{bmatrix}$$

AES Using CBC Mode of Encryption

XOR Initialization vector with plaintext:-

$$\begin{bmatrix} 49 & 4D & 44 & 48 \\ 53 & 41 & 49 & 45 \\ 4C & 42 & 53 & 43 \\ 41 & 41 & 54 & 41 \end{bmatrix} \oplus \begin{bmatrix} 12 & 90 & FE & 76 \\ 34 & AB & DC & 54 \\ 56 & CD & BA & 32 \\ 78 & EF & 98 & 10 \end{bmatrix}$$

$$= \begin{bmatrix} 5B & DD & BA & 3E \\ 67 & EA & 95 & 11 \\ 1A & 8F & E9 & 71 \\ 39 & AE & CC & 51 \end{bmatrix}$$

Initialization Vector:

$$I.V = \begin{bmatrix} 12 & 90 & FE & 76 \\ 34 & AB & DC & 54 \\ 56 & CD & BA & 32 \\ 78 & EF & 98 & 10 \end{bmatrix}$$

Plaintext: I S I A M A B A
Hex: 49 53 4C 41 4D 41 42 41
Plaintext: D I S T H E C A
Hex: 44 49 53 54 48 45 43 41

$$P = \begin{bmatrix} 49 & 4D & 44 & 48 \\ 53 & 41 & 49 & 45 \\ 4C & 42 & 53 & 43 \\ 41 & 41 & 54 & 41 \end{bmatrix}$$

AES Using CBC Mode of Encryption

XOR Initialization vector with plaintext:-

$$\begin{bmatrix} 49 & 4D & 44 & 48 \\ 53 & 41 & 49 & 45 \\ 4C & 42 & 53 & 43 \\ 41 & 41 & 54 & 41 \end{bmatrix} \oplus \begin{bmatrix} 12 & 90 & FE & 76 \\ 34 & AB & DC & 54 \\ 56 & CD & BA & 32 \\ 78 & EF & 98 & 10 \end{bmatrix}$$

$$= \begin{bmatrix} 5B & DD & BA & 3E \\ 67 & EA & 95 & 11 \\ 1A & 8F & E9 & 71 \\ 39 & AE & CC & 51 \end{bmatrix}$$

Add Round key 0 :-

5B	DD	BA	3E
67	EA	95	11
1A	8F	E9	71
39	AE	CC	51

⊕

4D	4D	4C	4C
59	45	41	41
4E	49	49	4D
41	53	42	42

=

16	90	F6	7F
3E	AF	D4	50
54	C6	A0	3C
78	FD	8E	13

Round 1

Substitution Bytes :-

47	60	42	D2
B2	79	48	53
20	B4	E0	EB
BC	54	19	7D

Shift Rows :-

47	60	42	D2
79	48	53	B2
E0	EB	20	B4
7D	BC	54	19

MIX Columns :-

02	03	01	01			47	60	42	D2
01	02	03	01		*	79	48	53	B2
01	01	02	03			E0	EB	20	B4
03	01	01	02			7D	BC	54	19

after MIX Column :-

9C	ED	FE	47
F2	6A	52	79
6F	3A	9F	33
A2	F9	45	96

Add Round key 1:-

$$\begin{bmatrix} 9C & ED & FE & 97 \\ F2 & 6A & 52 & 79 \\ 6F & 3A & 9F & 33 \\ A2 & F9 & 45 & 96 \end{bmatrix}$$

$$\oplus \begin{bmatrix} CF & 82 & CE & 8F \\ BA & FF & BE & FF \\ 62 & 2B & 62 & 2F \\ C2 & 91 & D3 & 91 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 53 & 6F & 30 & C8 \\ 48 & 95 & EC & 86 \\ 0D & 11 & FD & 1C \\ 60 & 68 & 96 & 07 \end{bmatrix}$$

Round 2

Substitution Bytes:-

$$\begin{bmatrix} ED & A8 & 04 & E8 \\ 52 & 2A & CE & 44 \\ D7 & 82 & 54 & 9C \\ D0 & 45 & 90 & C5 \end{bmatrix}$$

Shift Rows :-

$$\begin{bmatrix} ED & A8 & 04 & E8 \\ 52 & 2A & CE & 44 \\ D7 & 82 & 54 & 9C \\ D0 & 45 & 90 & C5 \end{bmatrix}$$

Add Round Key 2 :-

$$\begin{bmatrix} ED & A8 & 04 & E8 \\ 52 & 2A & CE & 44 \\ D7 & 82 & 54 & 9C \\ D0 & 45 & 90 & C5 \end{bmatrix} \oplus \begin{bmatrix} DB & 59 & 97 & 18 \\ AF & 50 & EE & 11 \\ E3 & C8 & AA & 85 \\ B1 & 20 & F3 & 62 \end{bmatrix}$$

$$\begin{bmatrix} 36 & F1 & 93 & F0 \\ FD & 7A & 20 & 55 \\ 34 & 4A & FE & 19 \\ 61 & 65 & 63 & A7 \end{bmatrix}$$

NEXT Block Plain text and their corresponding hexadecimal values:-

Plaintext: P I T A L O F P
Hex: 50 49 54 41 4C
Plaintext: A K I S T A N
Hex:

Plaintext: P I T A L O F
Hex: 50 49 54 41 4C 4F 46 50
Plaintext: P A K I S T A N
Hex: 41 4B

~~Plaintext~~: P I T A L O F
Hex: P A K I S T A N

Plaintext: P I T A L O F
Hex: 50 49 54 41 4C 4F 46
Plaintext: P A K I S T A N .
Hex: 50 41 4B 49 53 54 41 4E 2E

$$P = \begin{bmatrix} 50 & 4C & 41 & 54 \\ 49 & 4F & 4B & 41 \\ 54 & 46 & 49 & 4E \\ 41 & 50 & 53 & 2E \end{bmatrix}$$

XOR Plaintext with previous block Cipher text:-

$$= \begin{bmatrix} 50 & 4C & 41 & 54 \\ 49 & 4F & 4B & 41 \\ 54 & 46 & 49 & 42 \\ 41 & 50 & 53 & 2E \end{bmatrix} \oplus \begin{bmatrix} 36 & F1 & 93 & F0 \\ FD & 7A & 20 & 55 \\ 34 & 4A & FE & 19 \\ 61 & 65 & 63 & A7 \end{bmatrix}$$

$$= \begin{bmatrix} 66 & BD & D2 & A4 \\ B4 & 35 & 6B & 14 \\ 60 & 0C & B7 & 57 \\ 20 & 35 & 30 & 89 \end{bmatrix}$$

Add Round key 0:-

$$\begin{bmatrix} 66 & BD & D2 & A4 \\ B4 & 35 & 6B & 14 \\ 60 & 0C & B7 & 57 \\ 20 & 35 & 30 & 89 \end{bmatrix} \oplus \begin{bmatrix} 4D & 4D & 4C & 41 \\ 59 & 48 & 41 & 41 \\ 4E & 49 & 49 & 4D \\ 41 & 53 & 42 & 42 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 2B & F0 & 9E & E5 \\ ED & 70 & 2A & 55 \\ 2E & 45 & FE & 1A \\ 61 & 66 & 72 & CB \end{bmatrix}$$

Round 1

Substitution Bytes:-

F1	8C	0B	D9
55	51	E5	FC
31	6E	BB	A2
EF	33	40	1F

Shift Rows:-

F1	8C	0B	D9
51	E5	FC	55
BB	A2	31	6E
1F	EF	33	40

MIX Columns:-

D2	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

F1	8C	0B	D9
51	E5	FC	55
BB	A2	31	6E
1F	EF	33	40

A4	53	15	6D
F2	C8	23	75
9F	D2	9E	D0
C1	F0	8B	2E

Add Round key 1:-

A4	53	15	6D
F2	C8	23	75
9F	D2	9E	DD
C1	F0	8B	2E

⊕

CF	82	CE	31
BA	FF	BE	FF
62	2B	62	2F
C2	91	D3	91

=

6B	D1	DB	E2
48	37	9D	81
FD	F9	FC	FF
03	61	58	BD

Round 2

Substitution Bytes:

7F	3E	B9	98
52	9A	5E	7E
54	99	B0	16
7B	EF	6A	7A

Shift Rows:-

7F	3E	B9	98
9A	5E	7E	52
B0	16	54	99
7A	7B	EF	6A

Add Round Key 2:-

7F	3E	B9	9A	⊕ key2 =>	44	5F	AB	9A
9A	5E	7E	52		35	0E	9a	43
B0	16	54	99		53	DE	FE	1C
7A	7B	EF	6A		CB	5B	1C	0B

AES Decryption using CBC Mode

Add cipher of block 1 with round key 2:-

36	F1	93	F0		DB	59	97	1B
FD	7A	20	55	⊕	AF	50	EE	11
34	4A	FE	19		E3	C8	AA	85
61	65	63	A7		B1	20	F3	62

ED	A8	04	E8
52	2A	CE	44
D7	82	54	9C
D0	45	90	C5

Round 1

Inverse Shift Rows:-

ED	A8	04	E8
44	52	2A	CE
54	9C	D7	82
C5	D0		

ED	A8	04	E8
52	2A	CE	44
D7	82	54	9C
D0	45	90	C5

Inverse Substitution bytes:-

53	6F	30	C8
48	95	EC	86
0D	11	FD	1C
60	68	96	07

Inverse Mix Columns:-

$$\begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} 53 & 6F & 30 & C8 \\ 48 & 95 & 6C & 86 \\ 0D & 71 & FD & 1C \\ 60 & 68 & 96 & 07 \end{bmatrix}$$

$$\begin{bmatrix} 61 & F3 & 55 & 5F \\ 53 & 33 & F3 & 10 \\ 0D & 96 & 9A & 13 \\ 3D & C9 & 73 & 8B \end{bmatrix}$$

Add Round Key 1:-

$$\begin{bmatrix} 61 & F3 & 55 & 5F \\ 53 & 33 & F3 & 10 \\ 0D & 96 & 9A & 13 \\ 3D & C9 & 73 & 8B \end{bmatrix} \oplus \begin{bmatrix} CF & 82 & CE & 8F \\ BA & FF & BE & EF \\ 62 & 28 & 62 & 2F \\ C2 & 91 & D3 & 91 \end{bmatrix}$$

$$\begin{bmatrix} AF & 71 & 9B & D0 \\ E9 & CC & 4D & EF \\ 6F & BD & F8 & 3C \\ FF & 58 & A0 & 1A \end{bmatrix}$$

Round 2

Inverse Shift Row:-

A7	71	9B	D0
EF	E9	CC	4D
F8	3C	6F	BD
58	A0	1A	FF

Inverse Substitution Bytes:-

E4	A3	14	70
DF	1E	4B	E3
41	EB	A8	7A
6A	E0	A2	16

Add Round key 0:-

E4	A3	14	70
DF	1E	4B	E3
41	EB	A8	7A
6A	E0	A2	16

⊕

4D	4D	4C	41
59	45	41	41
4E	49	49	4D
41	53	42	42

A9	EE	58	31
86	5B	0A	A2
0F	A2	E1	37
2B	B3	E0	54

XOR Above with its I.V:-

A9	6E	58	31
86	5B	0A	A2
0F	A2	E1	37
2B	B3	E0	54

⊕

12	90	F6	76
34	AB	DC	54
56	CD	BA	32
78	EF	98	10

=

49	4D	44	48
53	41	49	45
4C	42	53	43
41	41	54	41

Add Cipher of block 2 with round key 2:-

44	5F	AB	98
35	0E	90	43
53	DE	FE	1C
CB	5B	1C	08

$\oplus$

DB	59	97	18
AF	50	EE	11
E3	CB	AA	85
B1	20	F3	62

7F	3E	B9	98
9A	5E	7E	52
B0	16	54	99
7A	7B	EF	6A

Round 1

ISR:-

~~7F~~	~~3E~~	~~B9~~	~~98~~
~~9A~~	5E	7E	52

7F	3E	B9	98
52	9A	5E	7E
54	99	B0	16
7B	EF	6A	7A

ISB :-

6B	D1	DB	E2
48	37	9D	8A
F0	F9	FC	FF
03	61	58	BD

IMC :-

0e	0b	0d	09
09	0e	0b	0d
0d	09	0e	0b
0b	0d	09	0e

6B	D1	DB	E2
48	37	9D	8A
F0	F9	FC	FF
03	61	58	BD

4D	68	67	1A
41	3D	0D	95
E7	95	C4	E5
28	4D	42	53

Add Round Key 1:-

4D	68	67	1A
41	3D	0D	95
E7	95	C4	E5
28	4D	42	53

⊕

CF	82	CE	9F
BA	FF	BF	FF
62	2B	62	2F
C2	91	B3	91

87	EA	A9	95
FB	C2	B3	6A
85	BE	A6	CA
EA	DC	91	C2

Round 2

ISR:-

83	EA	A9	95
6A	FB	C2	B3
A6	CA	85	BE
DC	91	C2	EA

ISB:-

EC	87	D3	2A
02	0F	25	6D
24	74	97	AE
86	81	25	87

Add Round key 0:-

EC	87	D3	2A
02	0F	25	6D
24	74	97	AE
86	81	25	87

⊕

4D	4D	4C	4D
59	45	41	41
4E	49	49	4D
41	53	42	42

A1	CA	1F	6B
5B	4A	64	2C
6A	3D	DE	E3
C7	D2	67	C5

XOR above with cipher text of block 1:-

$$\begin{bmatrix} 36 & F1 & 93 & F0 \\ FD & 7A & 20 & 55 \\ 34 & 4A & FE & 19 \\ 61 & 65 & 63 & A7 \end{bmatrix}$$

$$\oplus \begin{bmatrix} A1 & CA & 1F & 6B \\ 5B & 4A & 64 & 2C \\ 64 & 3D & DE & E3 \\ C7 & D2 & 67 & C5 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 50 & 4C & 41 & 54 \\ 49 & 4F & 4B & 41 \\ 54 & 46 & 49 & 4E \\ 41 & 50 & 53 & 2E \end{bmatrix}.$$