ome : Faiez Tariq
ll # 22F-3873
ection - 7F

"AES WORKING"

•) Plaintext = TWO_ONE_NINE_TWO → 16 byte
•) key = THATS_MY_KUNG_FU → 16 byte

•) key generation :-

Step #01)

"Convert key into hexadecimal matrix"

→

T	H	A	T	S	_	M	Y	_	K	U	N	G	_	F	U
54	68	61	74	73	20	6D	79	20	4B	75	6E	67	20	46	75

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

Step # 02 (to 03)

"Take rot word and sub byte of last column"

67		20		B7
20	rot word →	46	sub byte →	SA
46		75		9D
75		67		85

Step-11>

"Taking XOR with RCON & generate full key"

54		B7		01		F6
68	⊕	SA	⊕	00	=	36
61		9D		00		FC
74		85		00		F1

FG	87	F7	C6
36	16	SF	7F
FC	99	EC	C8
F1	68	16	61

.
.
.
.

Upto 10th round and we will get the Final key!

• Text encryption :-

T	W	O	–	O	N	E	–	N	I	N	E	–	T	W	O
54	77	6F	20	4F	6E	65	20	6E	69	6E	65	20	54	77	6F

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

• Initial Round :-

"Taking XOR with Cipher Key

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

⊕

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

00	3E	5E	47
1F	5E	32	74
3E	08	1B	31
54	59	0B	1A

⊙ Main Round:-

00	3E	5E	47
1F	5E	32	74
3E	08	1B	3A
54	59	0B	1A

Step01 >

"Sub-byte"

0	63	b2	58	a0
1	c0	58	23	92
2	b2	30	af	80
3	20	cb	2b	a2

Step 02 >

"Shift Rows"

63	b2	58	a0
58	23	92	c0
af	80	b2	30
a2	20	cb	2b

Step 03)

"Mix Column"

given matrix

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

① 63 - 58 - AF - A2

63·02 ⊕ b2·01 ⊕ 58·01 ⊕ ab·a3

58·02 ⊕ 23·01 ⊕ a2·01 ⊕ c9·a3

AF·02 ⊕ 80·01 ⊕ B2·01 ⊕ 30·03

A2·02 ⊕ 20·01 ⊕ CB·01 ⊕ 28·03

Final matrix

F9	D9	E9	F9
D5	66	FB	4F
A5	F5	D0	B9
D0	D9	C4	96

Step 04 >

"Add Round key"

F9	D9	E9	F9
D5	66	FB	4F
A5	F5	D0	B9
D0	D9	C4	96

⊕

01	1B	A7	CB
A1	23	9A	72
F9	36	C2	31
C1	67	BC	80

8F	81	9C	20
A2	C1	41	EF
B7	74	9F	AC
63	74	A1	63

Cipher text

Upto 9 rounds!

•) Decryption:-

InvRows -> InvSubbyte -> Addroundky -> invMixcolum

⊙ ROUND 1>

"Taking XOR with key"

0	00	6D	38	B6
1	DD	CC	25	B4
2	72	D4	46	4D
3	2E	4D	A9	5E

Round #02)

→ INVShiftedRows :-

0	00	6D	38	B6
1	DD	CC	25	B4
2	72	D4	46	4D
3	2E	4D	A9	5E

00	6D	38	B6
B4	DD	CC	25
46	4D	72	D4
4D	A9	5E	2E

→ Inv subbyte :-

2C	13	AC	9B
1D	4C	13	CD
67	9F	84	A1
89	7D	92	1D

→ Add Roundkey

1A	BC	B9	81
35	9A	F2	92
41	DE	3B	AA
78	A1	66	BA

→ Inverse Mix column :-

81	2C	19	F2
AC	CA	26	D9
1F	FF	35	C8
AB	9F	4F	9B

upto 10 Rounds

then we will get the original plain text