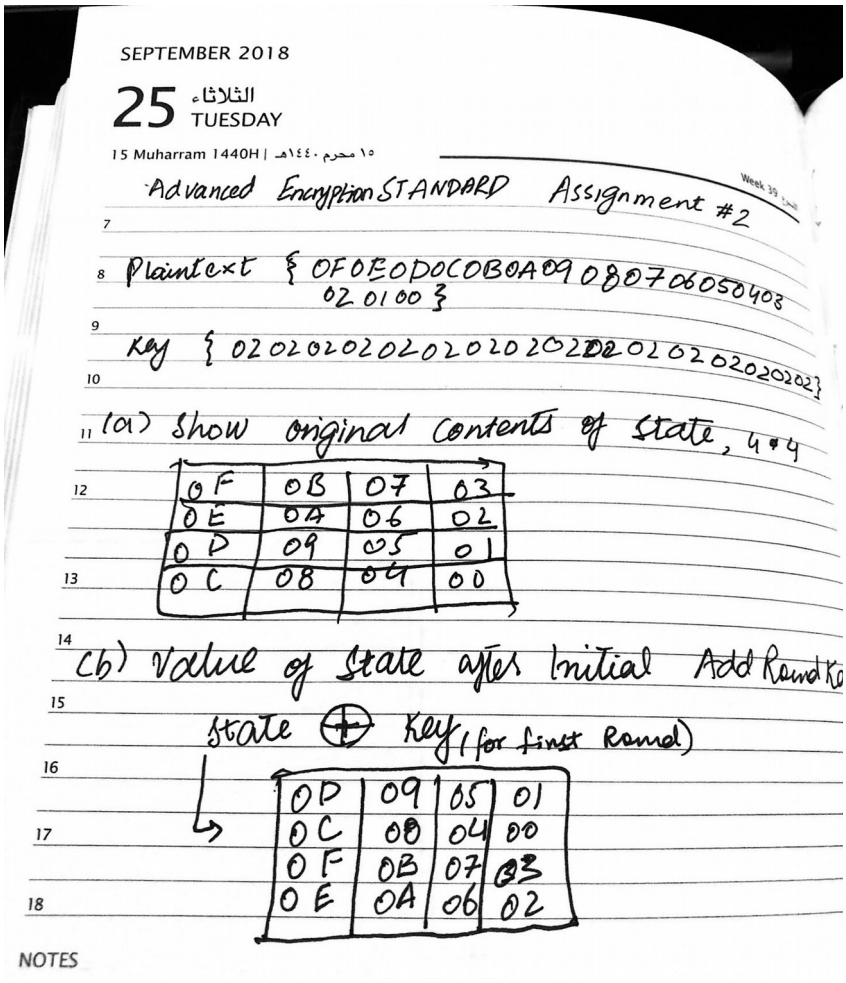
Mubariz Ahmed Khan P180010



SEPTEMBER 2018

25 الثلاثاء TUESDAY

15 Muharram 1440H | ١٥ محرم ١٤٤٠هـ

Week 39

Advanced Encryption STANDARD Assignment #2

Plaintext { OF OE OD OC OB OA 09 08 07 06 05 04 03 02 01 00 }

Key { 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 }

(a) Show original contents of State, 4*4

0F	0B	07	03
0E	04	06	02
0D	09	05	01
0C	08	04	00

(b) Value of State after Initial AddRoundKe

State ⊕ Key (for first Round)

0D	09	05	01
0C	08	04	00
0F	0B	07	03
0E	0A	06	02

NOTES

(c) Value of State after S-Box

D7	01	6B	7C
FE	30	F2	63
76	2B	C5	7B
AB	67	6F	77

(d) Show the value of State after Shift Rows

Shift (c) →

D7	01	6B	7C
30	F2	63	FE
C5	7B	76	2B
77	AB	67	6F