Nathan Walzer - nwalzer

1a)

Using expansion function on 10110011000011111100100010100110, we get:
010110 100110 100001 011111 111001 010001 010100 001101

1b)

Key - 000010 011100 110001 100010 110111 101011 100000 001111
^ 010110 100110 100001 011111 111001 010001 010100 001101
010100 111010 010000 111101 001110 111010 110100 000010

1c)

S_1 - 010100 -> row 0, col 10 -> **0110**
S_2 - 111010 -> row 2, col 13 -> **0011**
S_3 - 010000 -> row 0, col 8 -> **0001**
S_4 - 111101 -> row 3, col 14 -> **0010**
S_5 - 001110 -> row 0, col 7 -> **0110**
S_6 - 111010 -> row 2, col 13 -> **1101**
S_7 - 110100 -> row 2, col 10 -> **0110**
S_8 - 000010 -> row 0, col 1 -> **0010**

0110 0011 0001 0010 0110 1101 0110 0010

1d)

Using permutation table P, we get:
01010100 01010110 11100110 10001000

2a) Input as hex = **56E2 19B2 44B3 DB43 811E 9D3A 9E85 F34F**

2b) As a state diagram, bits are added sequentially to a column before filling the next column to the right:

56	44	81	9E
E2	B3	1E	85
19	DB	9D	F3
B2	43	3A	4F

2c) *2b* matrix after AES S-Box

B1	1B	0C	0B

98	6D	72	97
D4	B9	5E	0D
37	1A	80	84

2d) *2c* matrix after shifting row 1 by 1, row 2 by 2, and row 3 by 3 to the left

B1	1B	0C	0B
6D	72	97	98
5E	0D	D4	B9
84	37	1A	80

2e) MixColumns

The mixColumns step was performed with the help of the mixColumns python script I wrote

14	9A	74	9C
0D	DF	44	70
F7	2A	06	61
E8	3C	63	27

2f) addRoundKey

This step was performed with the help of the addRoundKey python script I wrote

20	EC	A1	6D
04	4C	40	C5
51	02	CE	13
3E	7F	AE	55

3a)

I. $37 \cdot 3 \ mod\ 23$ = **111 % 23 = 19**

II. $19 \cdot 13 \ mod\ 23$ = **247 % 23 = 17**

III. $18 \cdot 15 \ mod\ 12$ = **270 % 12 = 6**

IV. $15 \cdot 29 + 11 \cdot 15 \ mod\ 23$ = **600 % 23 = 2**

3b)

V. $8^{-1} \ mod\ 17$

17 is prime, so GCD is 1 and inverse exists
Through an exhaustive search of 8*x % 17 = 1, {x | 2->16}, we find 8 inverse to be **15**

VI. $5^{-1} \, mod \, 17$
17 is prime, so GCD is 1 and inverse exists
Through an exhaustive search of 5*x % 17 = 1, {x | 2->16}, we find 5 inverse to be **7**

VII. $5^{-1} \, mod \, 37$
37 is prime, so GCD is 1 and inverse exists
Through an exhaustive search of 5*x % 17 = 1, {x | 2->16}, we find 5 inverse to be **15**

VIII. $10^{-1} \, mod \, 15$
GCD is 5, so this inverse **does not exist**

3c)
The prime factors of 216 are (2, 3), **the numbers that will not have an inverse will be all multiples of 2 and all multiples of 3** (There are way too many to write)