Question 1

1.5 / 3 pts

The security model for encryption that we learned in class involved distinguishing a black box containing real encryption from a black box that returned the same number of random bits.

For each of the following modes, if the permutation's block length is b bits, at about how many permutation calls does the mode become easy to distinguish?

Note: popup menus can't do math formatting, so sqrt is square root and pow(a,b) is a^b.

ECB

CTR

ECB 2 Same thing twice = ECB

CTR sqrt(pow(2,b))

$$\text{prob} = \frac{q^2}{2^b}$$ * birthday prob

$$1 = \frac{q^2}{2^b}$$ solve for q

$$2^b = q^2$$

$$\sqrt{2^b} = q$$

Question 2

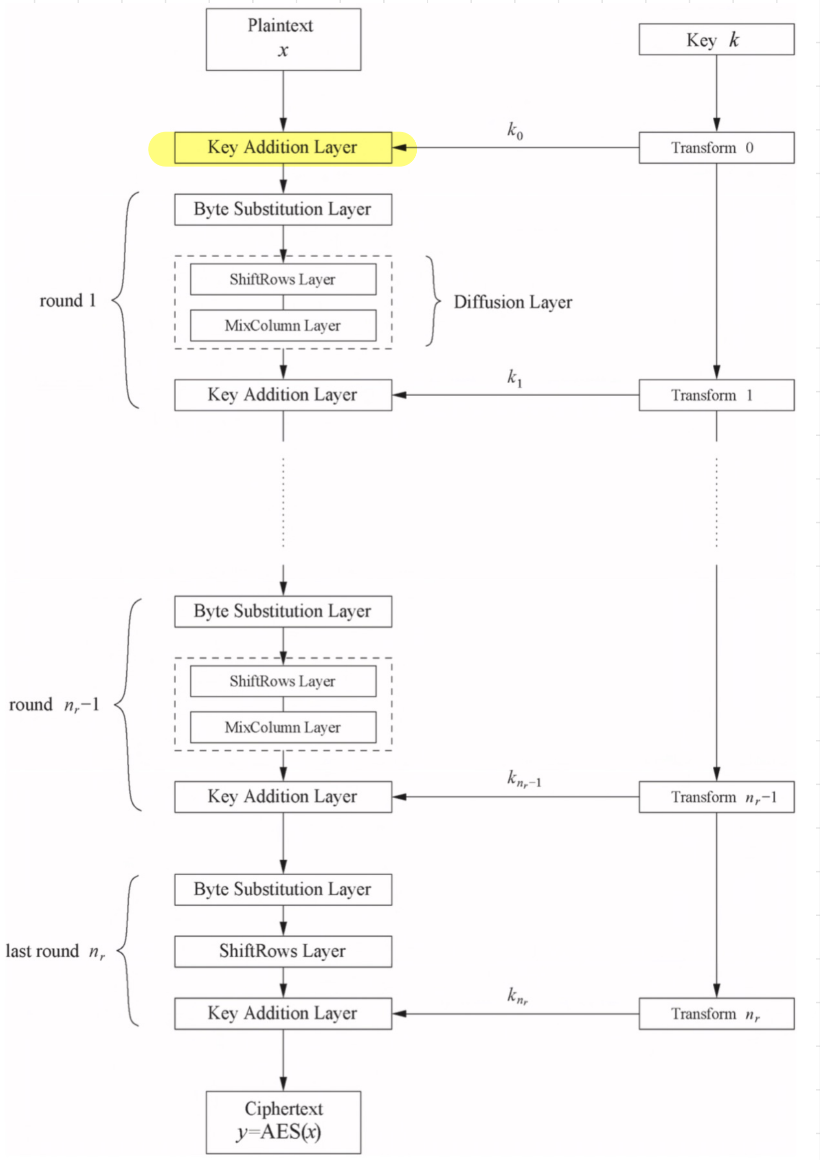
3 / 3 pts

These remaining problems have you simulate 1 round of AES. Each uses a different input so that if you get one step wrong it does not affect the others.

Consider the picture of AES from the textbook reading (Page 91) or these slides (Page 8). Let x and k be the following 16 bytes (in hex)

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

What are the first four bytes (ie, leftmost) of the output from the first Key Addition Layer (the one at the top of the figure)? Express each byte as exactly two hexadecimal digits without any spaces.



In Transform 0, the key is not changed so XORing each byte of k with x will result in the first 4 bytes being:

$\boxed{00 \quad 01 \quad 02 \quad 03}$

Question 3

3 / 3 pts

These remaining problems have you simulate 1 round of AES. Each uses a different input so that if you get one step wrong it does not affect the others.

Consider the picture of AES from the textbook reading (Page 91) or these slides (Page 8). Let the input to round 1's Byte Substitution Layer be the 16 bytes

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

What are the first four bytes (ie, leftmost) of the output from round 1's Byte Substitution Layer? Express each byte as exactly two hexadecimal digits without any spaces.

Table 4.3 AES S-Box: Substitution values in hexadecimal notation for input byte (xy)

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

We simply need to find the $S(xy)$ value for each byte in our input

Refering to the table above:

$S(00) = 63$

$S(01) = 7C$

$S(02) = 77$

$S(03) = 7B$

So $\boxed{63 \quad 7C \quad 77 \quad 7B}$

Question 4

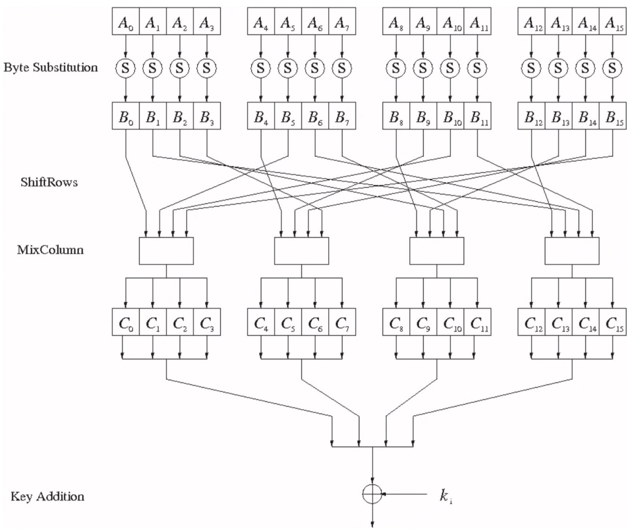
3 / 3 pts

These remaining problems have you simulate 1 round of AES. Each uses a different input so that if you get one step wrong it does not affect the others.

Consider the picture of AES from the textbook reading (Page 91) or these slides (Page 8). Let the input to round 1's Shift Rows Layer be the 16 bytes

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

What are the first four bytes of output from round 1's Shift Rows Layer? Express each byte as exactly two hexadecimal digits without any spaces.



Input matrix

B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

Output matrix

B_0	B_4	B_8	B_{12}	no shift
B_5	B_9	B_{13}	B_1	← one position left shift
B_{10}	B_{14}	B_2	B_6	← two positions left shift
B_{15}	B_3	B_7	B_{11}	← three positions left shift

Using either the diagram on left or matrix on right:

Inputs		Outputs
$B_0 = 00$	=>	$B_0 = 00$
$B_1 = 01$	=>	$B_5 = 05$
$B_2 = 02$	=>	$B_{10} = 0A$
$B_3 = 03$	=>	$B_{15} = 0F$

So, $\boxed{00\ 05\ 0A\ 0F}$

Question 5

1 / 4 pts

These remaining problems have you simulate 1 round of AES. Each uses a different input so that if you get one step wrong it does not affect the others.

Consider the picture of AES from the textbook reading (Page 91) or these slides (Page 8). Let the input to round 1's Mix Column Layer be the 16 bytes

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

What are the first four bytes of output from round 1's Mix Column Layer? Express each byte as exactly two hexadecimal digits without any spaces (using upper-case letters when needed).

- Each 4-byte column is considered as a vector and multiplied by a fixed 4x4 matrix, e.g.,

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

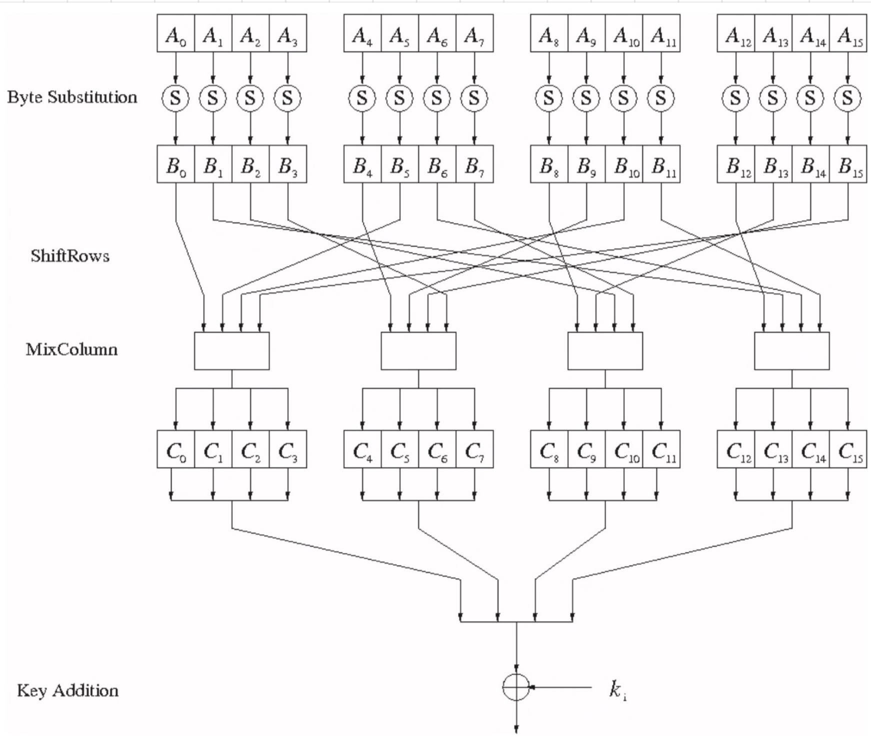
where 01, 02 and 03 are given in hexadecimal notation

Input matrix

B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

Output matrix

B_0	B_4	B_8	B_{12}	no shift
B_5	B_9	B_{13}	B_1	← one position left shift
B_{10}	B_{14}	B_2	B_6	← two positions left shift
B_{15}	B_3	B_7	B_{11}	← three positions left shift



$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \end{bmatrix}$$

$$C_0 = 2 \cdot B_0 + 3 \cdot B_1 + 1 \cdot B_2 + 1 \cdot B_3$$
$$= (x)(0) + (x+1)(1) + (x) + (x+1)$$
$$= 0 + x + 1 + x + x + 1$$
$$= x$$

$$\boxed{C_0 = 02}$$

$$C_1 = 1 \cdot B_0 + 2 \cdot B_1 + 3 \cdot B_2 + 1 \cdot B_3$$
$$= (0) + (x)(1) + (x+1)(x) + (x+1)$$
$$= x + x^2 + x + x + x + 1$$
$$= x^2 + x + 1$$

$$\boxed{C_1 = 07}$$

$$C_2 = 1 \cdot B_0 + 1 \cdot B_1 + 2 \cdot B_2 + 3 \cdot B_3$$
$$= (0) + (1) + (x)(x) + (x+1)(x+1)$$
$$= \cancel{1} + \cancel{x^2} + \cancel{x^2} + \cancel{1} + \cancel{x} + \cancel{x}$$

$$\boxed{C_2 = 00}$$

$$C_3 = 3 \cdot B_0 + 1 \cdot B_1 + 1 \cdot B_2 + 2 \cdot B_3$$
$$= (x+1)(0) + (1) + (x) + (x)(x+1)$$
$$= 0 + 1 + \cancel{x} + x^2 + \cancel{x}$$
$$= x^2 + 1$$

$$\boxed{C_3 = 05}$$

Question 6

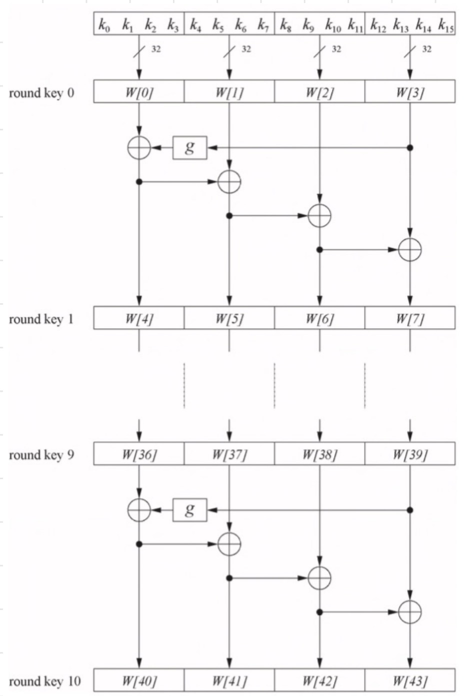
4 / 4 pts

These remaining problems have you simulate 1 round of AES. Each uses a different input so that if you get one step wrong it does not affect the others.

Consider the picture of AES from the textbook reading (Page 91) or these slides (Page 8). Let the input to round 1's Transform 1 be the 16 bytes

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

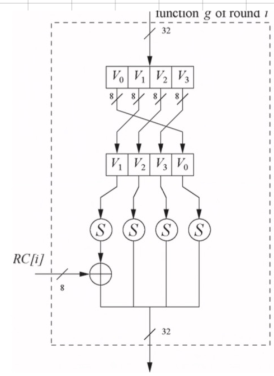
What are the first four bytes of output from round 1's Transform 1? Express each byte as exactly two hexadecimal digits without any spaces (using upper-case letters when needed).



The round coefficient RC is only added to the leftmost byte and varies from round to round:

$$RC[1] = x^0 = (00000001)_2$$
$$RC[2] = x^1 = (00000010)_2$$
$$RC[3] = x^2 = (00000100)_2$$
$$\ldots$$
$$RC[10] = x^9 = (00110110)_2$$

x^i represents an element in a Galois field



$$\underbrace{00\ 01\ 02\ 03}_{W[0]}\ \underbrace{04\ 05\ 06\ 07}_{W[1]}\ \underbrace{08\ 09\ 0A\ 0B}_{W[2]}\ \underbrace{0C\ 0D\ 0E\ 0F}_{W[3]}$$

$$W[4] = W[0] \oplus g(W[3])$$
$$= W[0] \oplus g(0C, 0D, 0E, 0F)$$
$$= W[0] \oplus (S(0D) \oplus 1, S(0E), S(0F), S(0C))$$
$$= W[0] \oplus (D7 \oplus 1, AB, 76, FE)$$
$$= 00\,01\,02\,03 \oplus D6, AB, 76, FE$$
$$W[4] = D6, AA, 74, FD$$