Question 1

2 / 2 pts

Which of the following AES steps supplies NO diffusion?

- (•) Key Addition
- ( ) Byte Substitution
- ( ) Shift Rows
- ( ) Mix Columns

All other AES steps provide some form of diffusion.

Question 2

2 / 2 pts

GF(8) is defined like GF(256) except the polynomials all have degree less than 3 and the modulus is $x^3 + x + 1$. Which of the following is the multiplicative inverse of 010 in GF(8)?

- ( ) 001
- ( ) 011
- ( ) 110
- ( ) 100
- (•) None of these

$010 \times 101 = 1$

$(x) \cdot (x^2 + 1)$

$x^3 + x$

$$\begin{array}{r} 1 \\ x^3 + x + 1 \;\overline{)\; x^3 + 0x^2 + x + 0} \\ \underline{x^3 \qquad + x + 1} \\ 0 \quad 0 \quad 0 \quad +1 \end{array}$$

For each y in F, except 0, there exists a z in F such that $(y \cdot z) = 1$

(Multiplicative inverse)

$010 + 010 = 0$

$$\begin{array}{r} 010 \\ \oplus\; 010 \\ \hline 000 \end{array}$$

For each y in F, there exists a z in F such that $(y + z) = 0$

(Additive inverse)

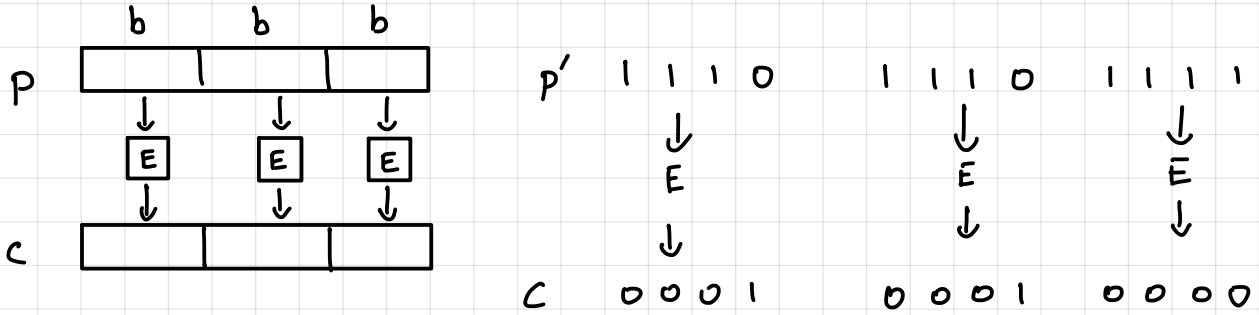
Question 3a

8 / 8 pts

You are to *encrypt* a ciphertext using the permutation p : $\{0,1\}^4 \rightarrow \{0,1\}^4$ defined as p(x) = ~x, ie, toggle each bit (0 to 1 and 1 to 0). If you need an IV use 1010. If you need a nonce use 01. If the mode uses padding to handle arbitrary plaintext lengths, add 10* padding. If you need a counter, begin at 1.

Encrypt the ciphertext 1110 1110 111 using ECB mode. Write four bits per box, with the final box possibly having fewer bits.

0001	0001	0000



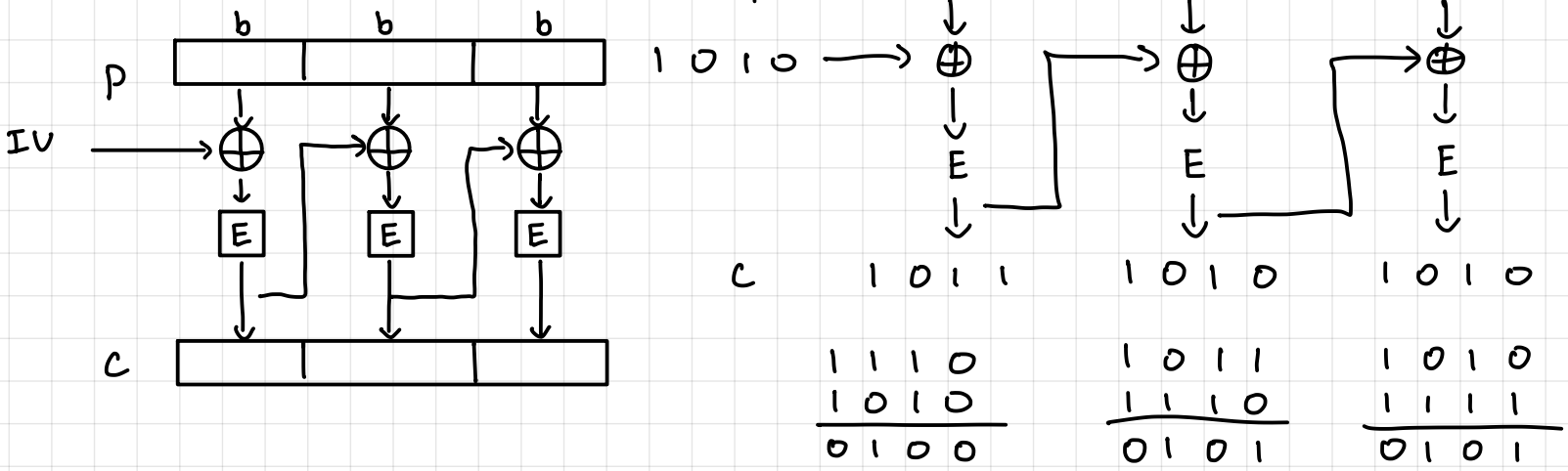
Question 3b

8 / 8 pts

You are to *encrypt* a ciphertext using the permutation p : $\{0,1\}^4 \rightarrow \{0,1\}^4$ defined as p(x) = ~x, ie, toggle each bit (0 to 1 and 1 to 0). If you need an IV use 1010. If you need a nonce use 01. If the mode uses padding to handle arbitrary plaintext lengths, add 10* padding. If you need a counter, begin at 1.

Encrypt the ciphertext 1110 1110 111 using CBC mode. Write four bits per box, with the final box possibly having fewer bits.

1011	1010	1010



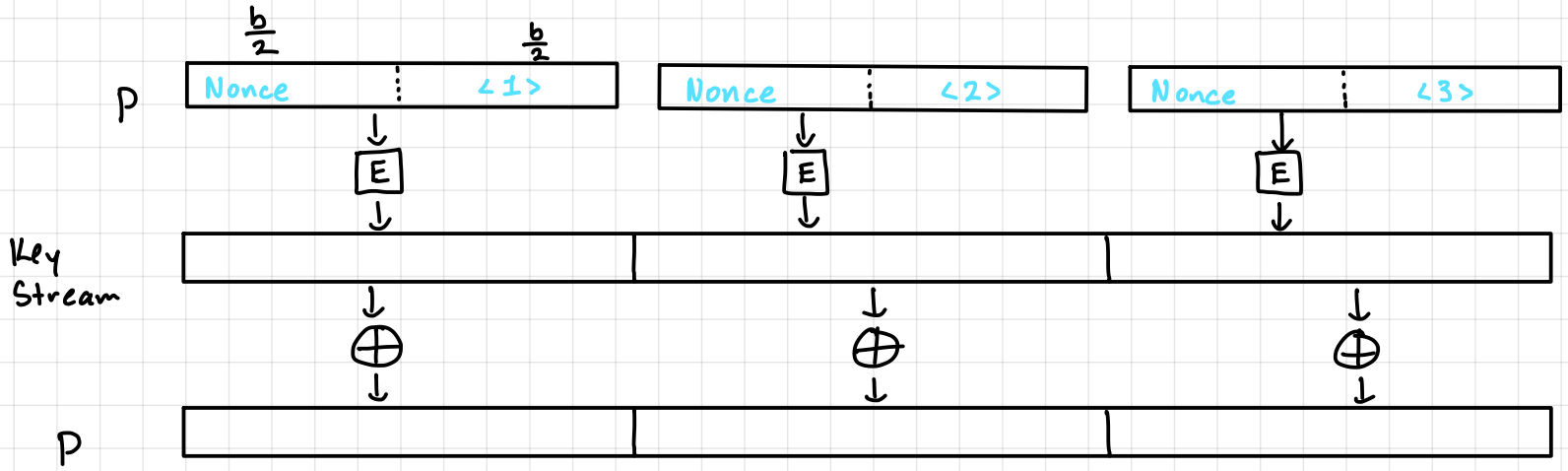
Question 3c

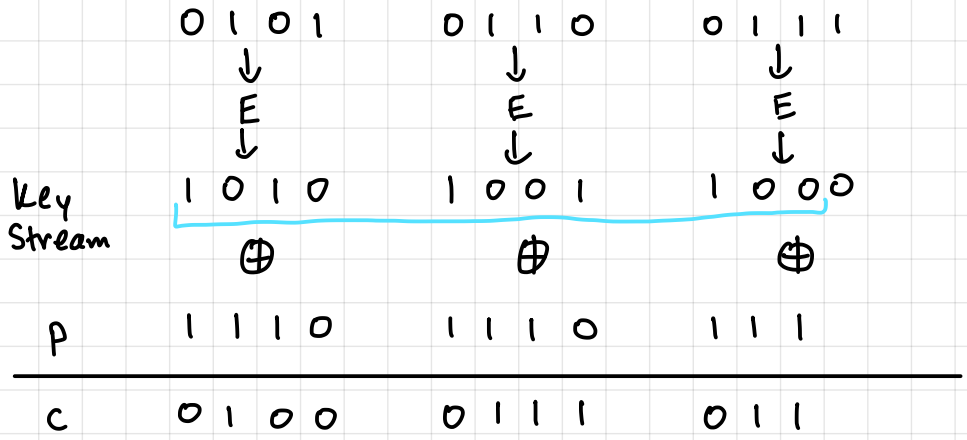
8 / 8 pts

You are to *encrypt* a ciphertext using the permutation $p : \{0,1\}^4 \to \{0,1\}^4$ defined as p(x) = ~x, ie, toggle each bit (0 to 1 and 1 to 0). If you need an IV use 1010. If you need a nonce use 01. If the mode uses padding to handle arbitrary plaintext lengths, add 10^* padding. If you need a counter, begin at 1.

Encrypt the ciphertext 1110 1110 111 using CTR mode. Write four bits per box, with the final box possibly having fewer bits.

0100	0111	011

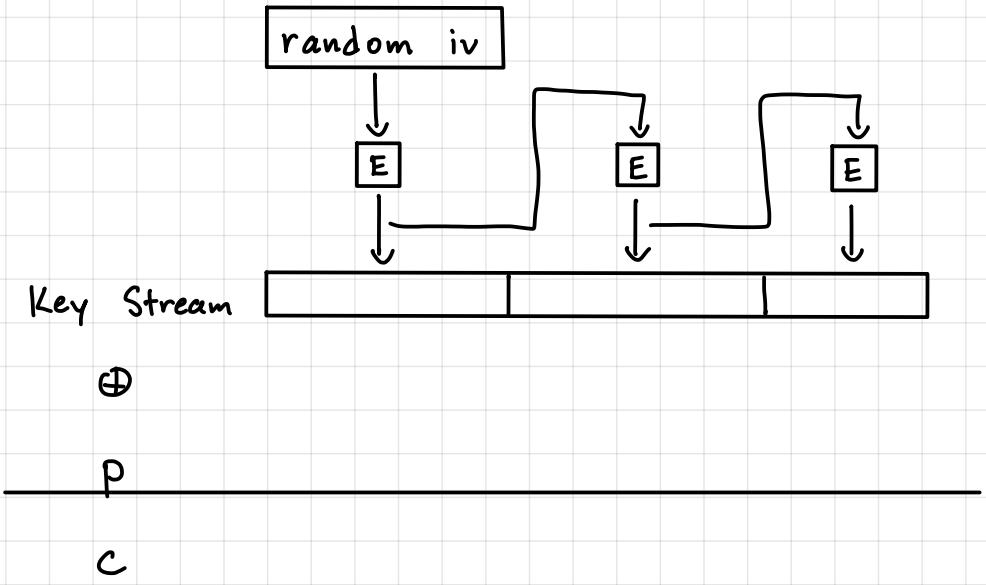


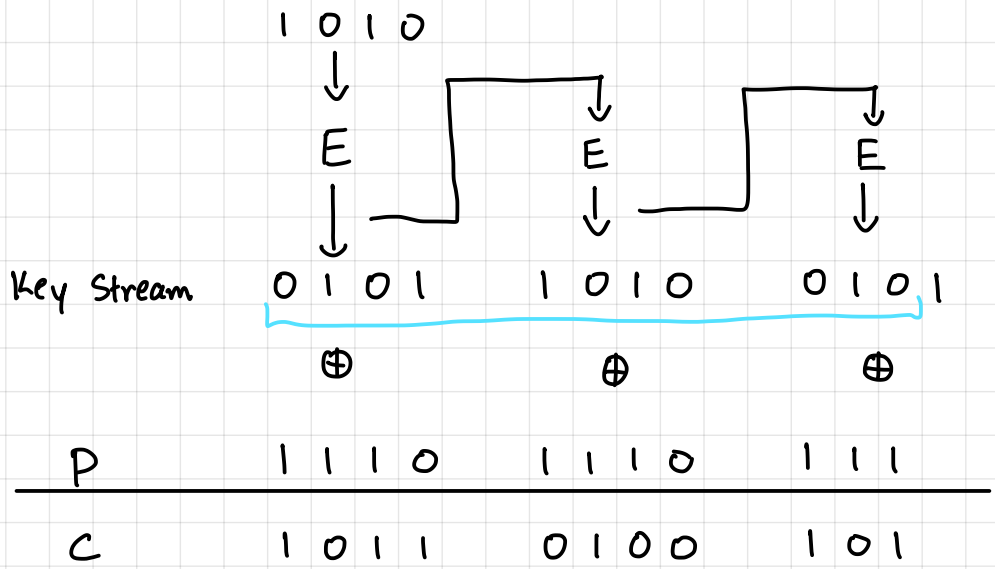


Question 3d

8 / 8 pts

You are to *encrypt* a ciphertext using the permutation p : $\{0,1\}^4 \rightarrow \{0,1\}^4$ defined as p(x) = ~x, ie, toggle each bit (0 to 1 and 1 to 0). If you need an IV use 1010. If you need a nonce use 01. If the mode uses padding to handle arbitrary plaintext lengths, add 10* padding. If you need a counter, begin at 1.



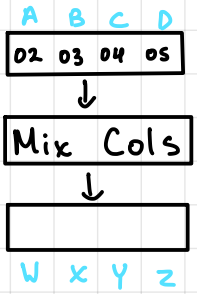


Question 4

4 / 4 pts

Let's say that the four bytes 02 03 04 05 were supplied to the AES MixColumns operation. Of the four bytes returned, what would be the first byte? Write using exactly two hex digits (using lower-case hex for a-f). You may look at these slides or this chapter if you wish.

00



02 = 0010 04 = 0100

03 = 0011 05 = 0101

$w = 2 \cdot A + 3 \cdot B + 1 \cdot C + 1 \cdot D$

$= (x)(x) + (x+1)(x+1) + (x^2) + (x^2+1)$

$= (x^2) + (x^2 + 1) + (x^2) + (x^2 + 1)$

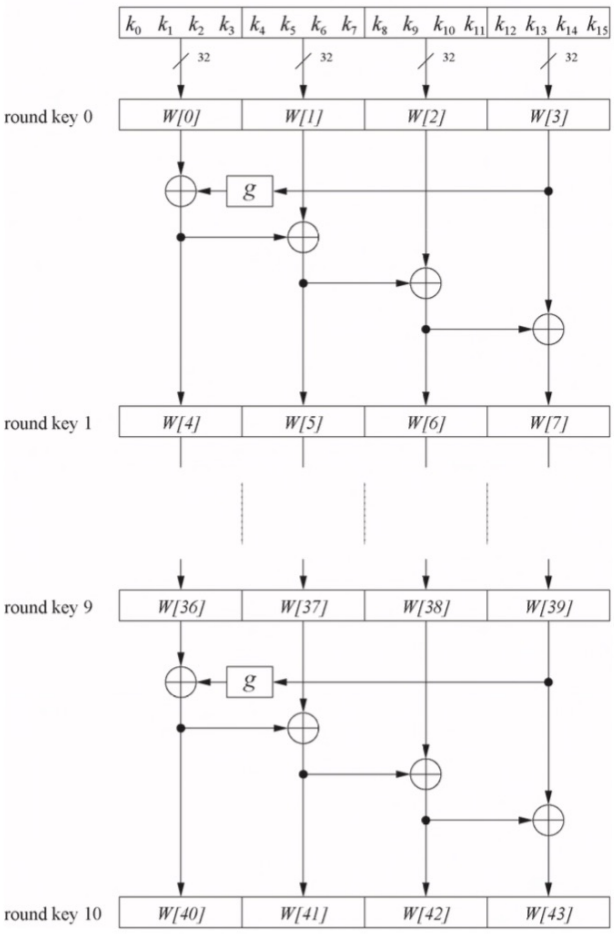
$= 00$

Question 5

4 / 4 pts

Let's say that an AES-128 key was 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00 04. (It's a bad key because it's not random, but we'll use it in this problem anyway.) This is used as "round key 0" what are the first four bytes in "round key 1"? Write each using exactly two hex digits (using lower-case hex for a-f). You may look at these slides or this chapter if you wish.

62 | 63 | f2 | 62



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

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

x^i represents an element in a Galois field

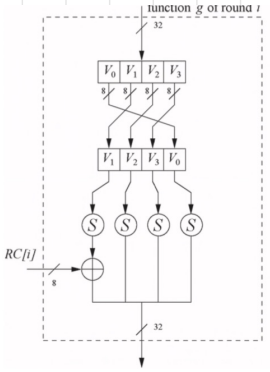
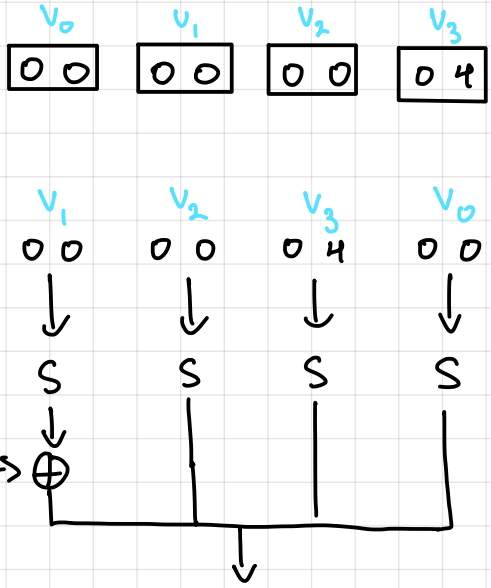


Table 4.3 AES S-Box: Substitution values in hexadecimal notation for input byte (xy)

	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
x 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



$S(0x00) \oplus 1$

$0x63 \oplus 1 = 0x62$

Round 0:

W[0] = 0 0 0 0 0 0 0 1
W[1] = 0 0 0 0 0 0 0 2
W[2] = 0 0 0 0 0 0 0 3
W[3] = 0 0 0 0 0 0 0 4

Round 1:

$W[4] = W[0] \oplus g(W[3])$

$= W[0] \oplus g(0x00, 0x00, 0x00, 0x04)$

$= W[0] \oplus (S(0x00) \oplus 1, S(0x00), S(0x04), S(0x00))$

$= W[0] \oplus (0x62, 0x63, 0xF2, 0x63)$

$= (0x00, 0x00, 0x00, 0x01) \oplus (0x62, 0x63, 0xF2, 0x63)$

$W[4] = (0x62, 0x63, 0xF2, 0x62)$