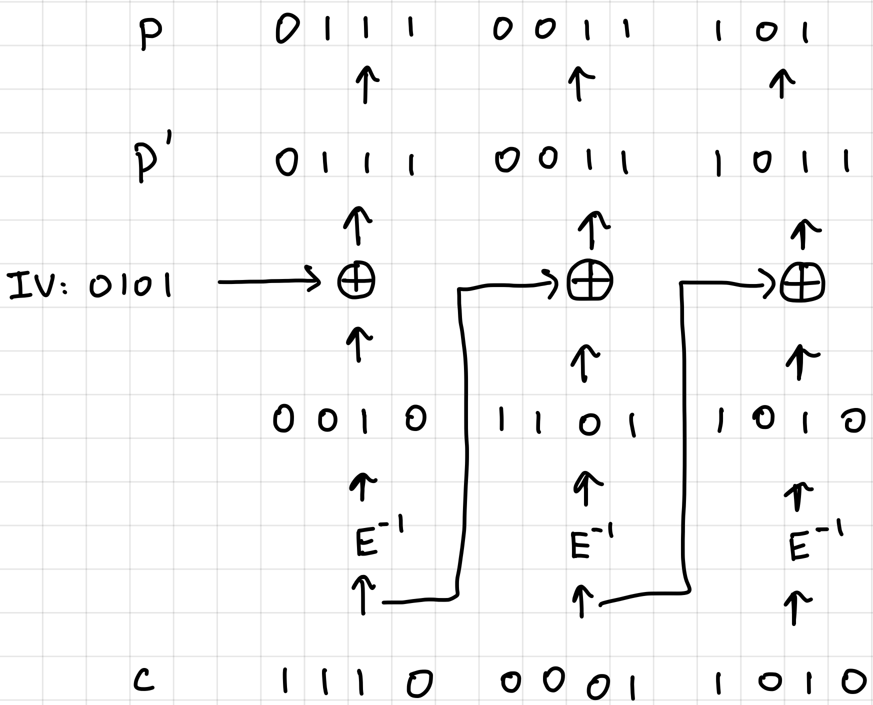
You are to *decrypt* a ciphertext that was *encrypted* using the permutation p : $\{0,1\}^4 \to \{0,1\}^4$ defined as p(x) = ~(x >>> 1), ie, rotate x RIGHT 1 bit and then negate all the bits. For example p(0011) = 0110 because 0011>>>1 = 1001 and ~1001 = 0110. Thus $p^{-1}(x)$ = (~x <<< 1). If you need an IV use 0101. If you need a nonce use 01. If the mode uses padding to handle arbitrary plaintext lengths, remove 10* padding. If you need a counter, begin at 1.

Decrypt the ciphertext 1110 0001 1010 given that it was produced using ECB mode. Write four bits per box, with the final box possibly having fewer bits.

P	0010	1101	10
	↑	↑	↑
P'	0010	1101	1010
	↑	↑	↑
	E^{-1}	E^{-1}	E^{-1}
	↑	↑	↑
C	1110	0001	1010

You are to *decrypt* a ciphertext that was *encrypted* using the permutation p : $\{0,1\}^4 \rightarrow \{0,1\}^4$ defined as p(x) = ~(x >>> 1), ie, rotate x RIGHT 1 bit and then negate all the bits. For example p(0011) = 0110 because 0011>>>1 = 1001 and ~1001 = 0110. Thus $p^{-1}(x)$ = (~x <<< 1). If you need an IV use 0101. If you need a nonce use 01. If the mode uses padding to handle arbitrary plaintext lengths, remove 10* padding. If you need a counter, begin at 1.

Decrypt the ciphertext 1110 0001 1010 given that it was produced using CBC mode. Write four bits per box, with the final box possibly having fewer bits.



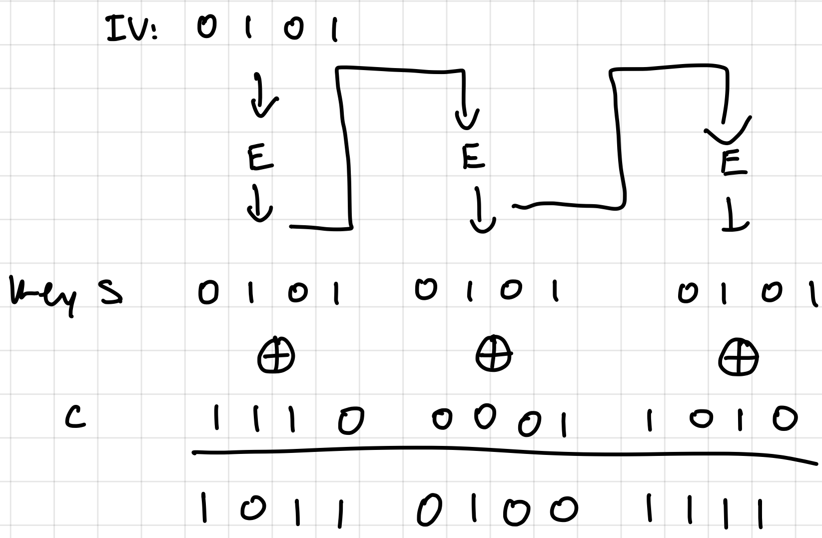
$$\begin{array}{r} 0010 \\ 0101 \\ \hline 0111 \end{array} \qquad \begin{array}{r} 1110 \\ 1101 \\ \hline 0011 \end{array} \qquad \begin{array}{r} 0001 \\ 1010 \\ \hline 1011 \end{array}$$

You are to *decrypt* a ciphertext that was *encrypted* using the permutation p : $\{0,1\}^4 \rightarrow \{0,1\}^4$ defined as p(x) = ~(x >>> 1), ie, rotate x RIGHT 1 bit and then negate all the bits. For example p(0011) = 0110 because 0011>>>1 = 1001 and ~1001 = 0110. Thus $p^{-1}(x)$ = (~x <<< 1). If you need an IV use 0101. If you need a nonce use 01. If the mode uses padding to handle arbitrary plaintext lengths, remove 10* padding. If you need a counter, begin at 1.

Decrypt the ciphertext 1110 0001 1010 given that it was produced using CTR mode. Write four bits per box, with the final box possibly having fewer bits.

p	0101	0110	0111
	↓	↓	↓
	E	E	E
	↓	↓	↓
keystream	0101	1100	0100
	⊕	⊕	⊕
c	1110	0001	1010
p	1011	1101	1110

You are to *decrypt* a ciphertext that was *encrypted* using the permutation p : $\{0,1\}^4 \rightarrow \{0,1\}^4$ defined as p(x) = ~(x >>> 1), ie, rotate x RIGHT 1 bit and then negate all the bits. For example p(0011) = 0110 because 0011>>>1 = 1001 and ~1001 = 0110. Thus $p^{-1}(x)$ = (~x <<< 1). If you need an IV use 0101. If you need a nonce use 01. If the mode uses padding to handle arbitrary plaintext lengths, remove 10* padding. If you need a counter, begin at 1.



GF(8) is defined like GF(256) except the polynomials all have degree less than 3 and the modulus is $x^3 + x + 1$. Calculate the following. Give each of your answers as exactly three binary digits.

011 × 010

$$011 \quad x \quad 010$$

$$(x^1 + x^0)(x^1)$$

$$x^2 + x$$

$$110$$

100 × 010

$$\begin{matrix} 2 & 1 & 0 \end{matrix}$$

$$100 \quad x \quad 010$$

$$x^2 \quad x \quad x^1$$

$$x^3 \mod x^3 + x + 1 = 011$$

$$1000 \qquad 1011$$

$$\begin{array}{r|l} & 1 \\ \hline x^3 + x + 1 & x^3 + 0x^2 + 0x + 0 \\ & x^3 + x + 1 \\ \hline & x + 1 \end{array}$$

110 × 100

$$\begin{matrix} 2 & 1 & 0 \end{matrix}$$

$$110 \quad x \quad 100$$

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

$$x^4 + x^3$$

$$11000 \mod 1011 = 101$$

$$\begin{array}{r|l} & x + 1 \\ \hline x^3 + x + 1 & x^4 + x^3 + 0x^2 + 0x + 0 \\ & -x^4 + x^2 + x \\ \hline & x^3 + x^2 + x \\ & x^3 + x + 1 \\ \hline & 0 \quad x^2 + 1 \end{array}$$

011 + 010

$$\begin{array}{r} 0\,1\,1 \\ \oplus\ \underline{0\,1\,0} \\ 0\,0\,1 \end{array}$$

Let's say you are designing a secure communication system that has two AES units in it (ie, it can compute AES or AES^{-1} on two blocks at the same time). Also, let's say that security, encryption speed, and decryption speed are all equally important to you. Which mode-of-operation would you select? Explain your answer in one or two sentences.

CTR is the only mode that both secure and allows parallel encryption and decryption