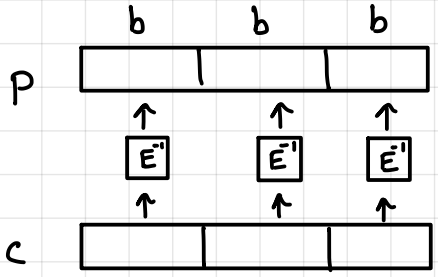
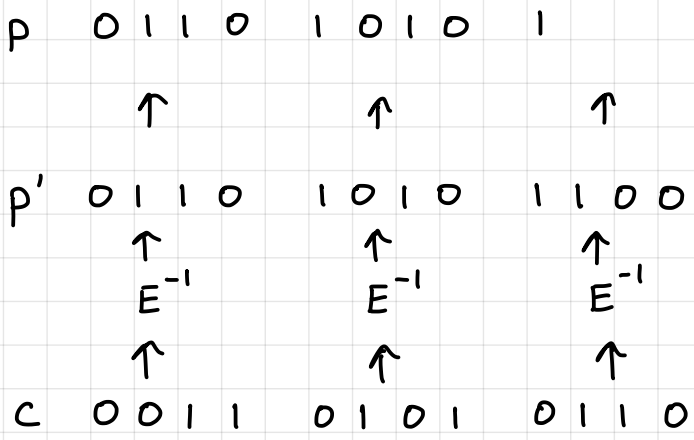
You are to *decrypt* a ciphertext that was *encrypted* using the permutation p : $\{0,1\}^4 \to \{0,1\}^4$ defined as p(x) = (x >>> 1), ie, rotate x RIGHT 1 bit. Thus $p^{-1}(x)$ = (x <<< 1). If you need an IV use 1001. If you need a nonce use 10. If the mode uses padding to handle arbitrary plaintext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

Decrypt the ciphertext 0011 0101 0110 given that it was produced using ECB mode. Write four bits per box, with the final box possibly having fewer bits.





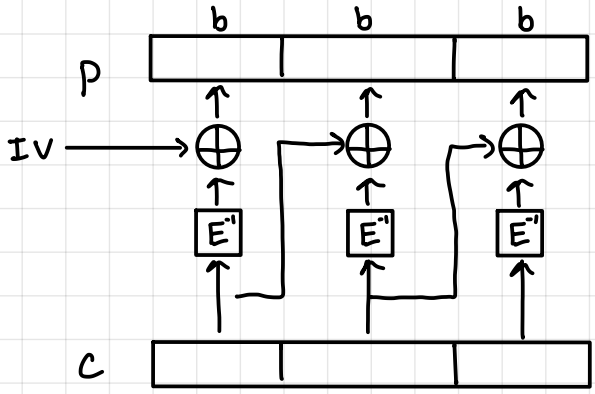
Encrypt: $p(x) = (x >>> 1)$

Decrypt: $p^{-1}(x) = (x <<< 1)$

mode uses padding: remove 10^*

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. Thus $p^{-1}(x)$ = (x <<< 1). If you need an IV use 1001. If you need a nonce use 10. If the mode uses padding to handle arbitrary plaintext lengths, remove 10^* padding. If you need a counter, begin at 1.

Decrypt the ciphertext 0011 0101 0110 given that it was produced using CBC mode. Write four bits per box, with the final box possibly having fewer bits.

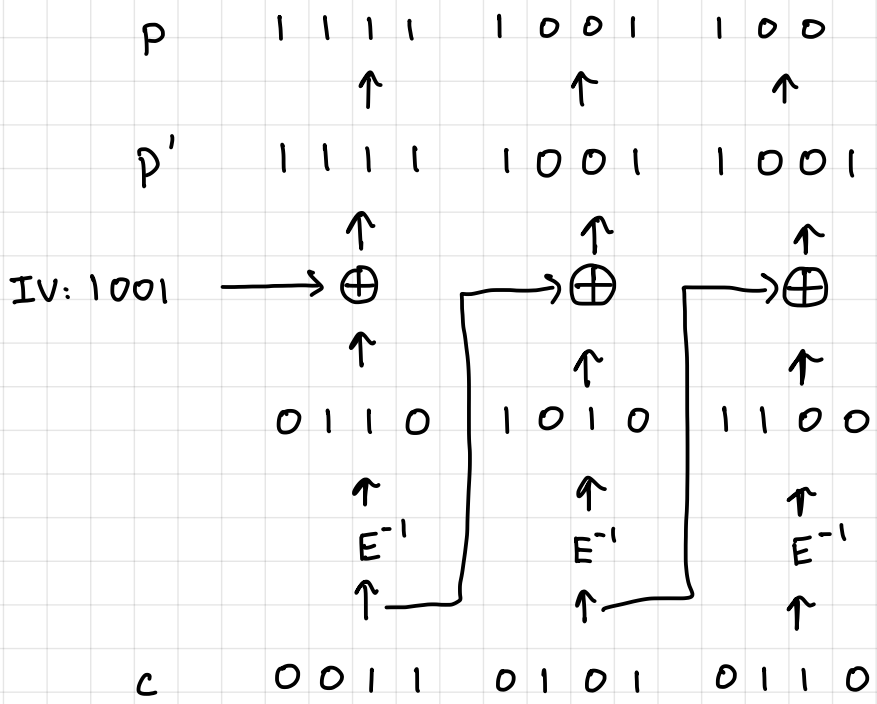


Encrypt: $p(x) = (x >>> 1)$

Decrypt: $p^{-1}(x) = (x <<< 1)$

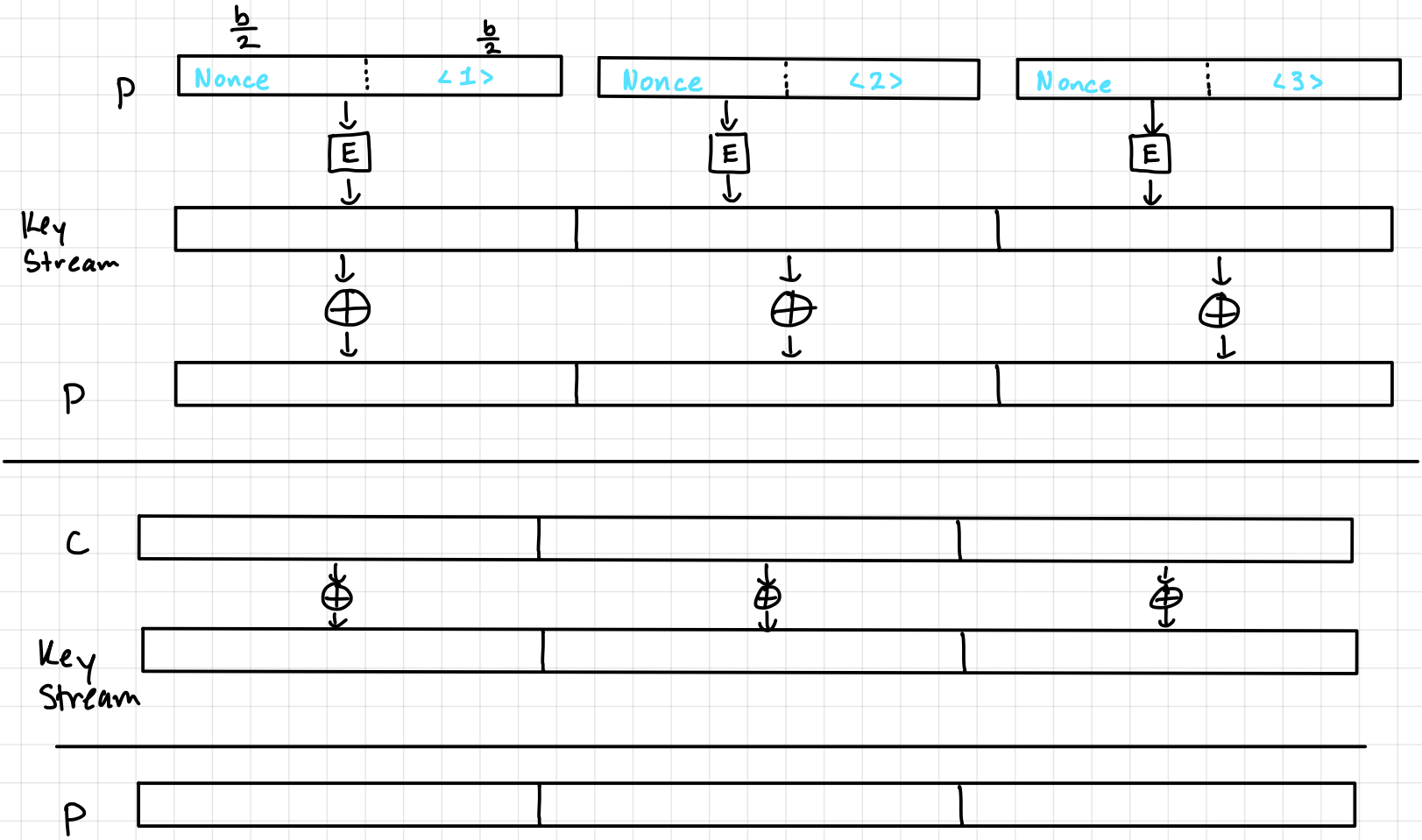
mode uses padding: remove 10^*

IV: 1001



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. Thus $p^{-1}(x)$ = (x <<< 1). If you need an IV use 1001. If you need a nonce use 10. If the mode uses padding to handle arbitrary plaintext lengths, remove 10^* padding. If you need a counter, begin at 1.

Decrypt the ciphertext 0011 0101 0110 given that it was produced using CTR mode. Write four bits per box, with the final box possibly having fewer bits.



Given: nonce: 10 Encrypt: p(x) = (x >>> 1) No padding
counter start at 1

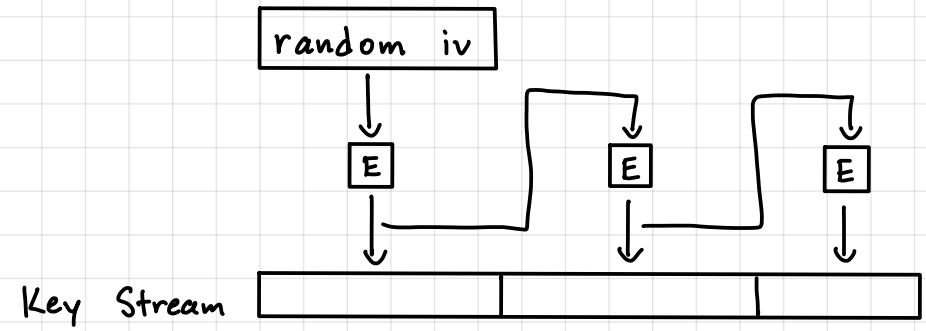
P	1001	1010	1011
	↓ E ↓	↓ E	↓ E
Key Stream	1100	0101	1101
	⊕	⊕	⊕
C	0011	0101	0110

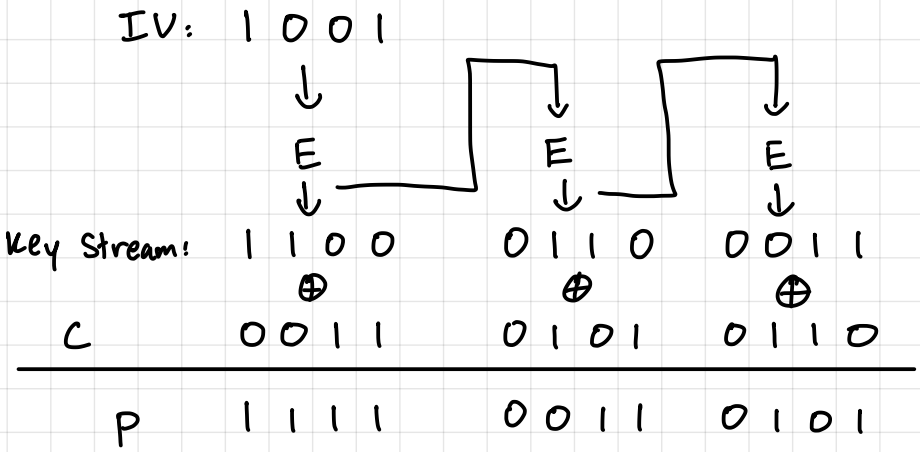
P	1111	0000	1011

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. Thus $p^{-1}(x)$ = (x <<< 1). If you need an IV use 1001. If you need a nonce use 10. If the mode uses padding to handle arbitrary plaintext lengths, remove 10^* padding. If you need a counter, begin at 1.

Decrypt the ciphertext 0011 0101 0110 given that it was produced using OFB mode. Write four bits per box, with the final box possibly having fewer bits.

No padding





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.

010 × 010 =

$$x^1 \times x^1$$

$$= x^2$$

$$= 1\ 0\ 0$$

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 × 011 =

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

$$= x^2 + x^0$$

$$= 1\ 0\ 1$$

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.

101 × 101 =

$$(x^2 + x^0) \times (x^2 + x^0)$$

$$= x^4 + x^0$$

$$= x^4 + x^0 \mod x^3 + x + 1$$

since $x^4 + x^0$ is greater than degree 3

$$x^3 + x + 1 \overline{)\ x^4 + \quad + 1}$$

$$x \quad (x^4 + x^2 + x)$$

$$x^2 + x + 1$$

$$= x^2 + x^1 + x^0$$

$$= 1\ 1\ 1$$

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.

010 + 010 =

Add the two polynomials, to keep coefficients 0 or 1, mod each coefficient by 2.

Concat the coefficients of the resulting degree

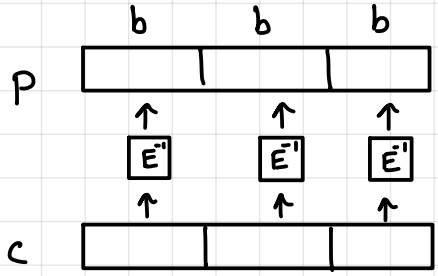
Shortcut: XOR the two bytes produces the same result

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

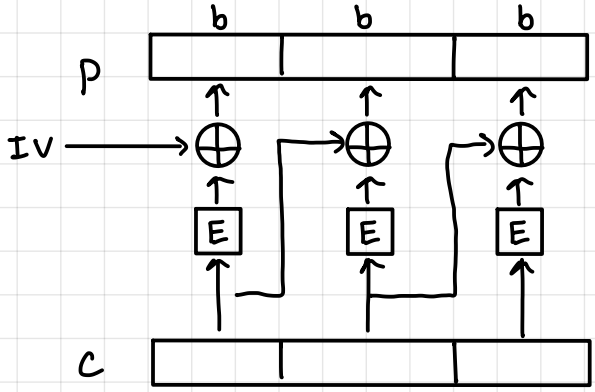
= 000

Let's say that you receive a ciphertext that was encrypted with a b-bit permutation and is nb-bits in length. (That is you receive an n-block ciphertext.) But, you did not receive an IV or nonce (if one was needed) along with the ciphertext. For each of the following modes indicate how many ciphertext blocks you could correctly decrypt into plaintext blocks without knowing an IV or nonce.

ECB: n ECB doesn't require an IV or nonce

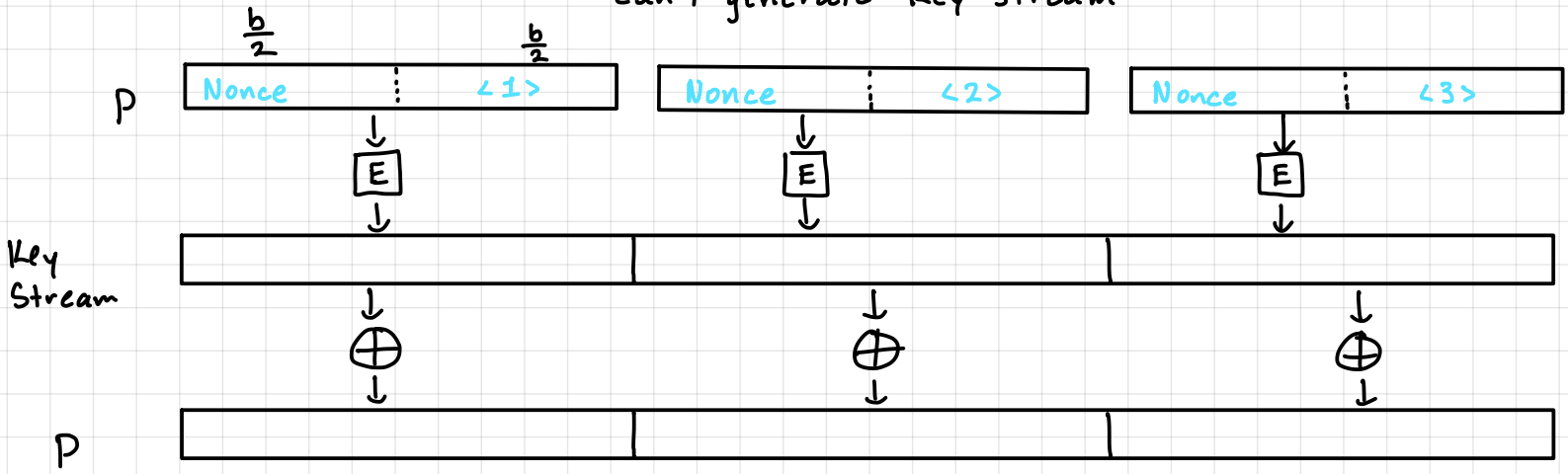


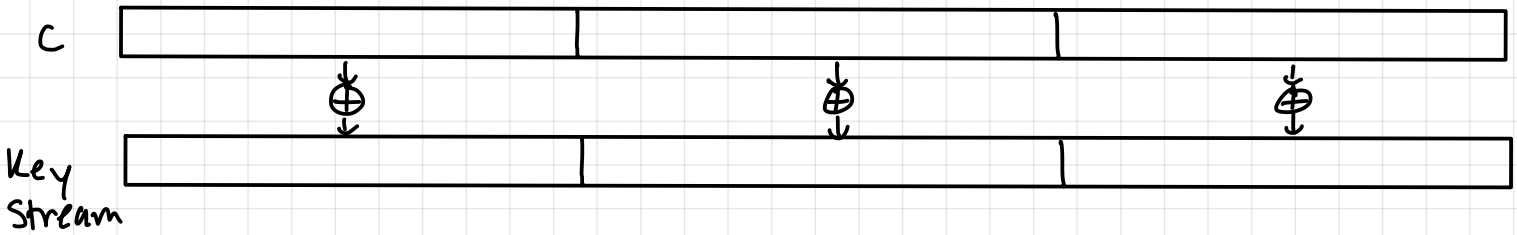
CBC: n - 1 CBC requires an IV for the first block

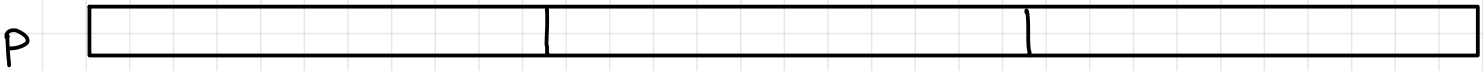


CTR: O

CTR requires a nonce for all blocks, can't generate Key Stream

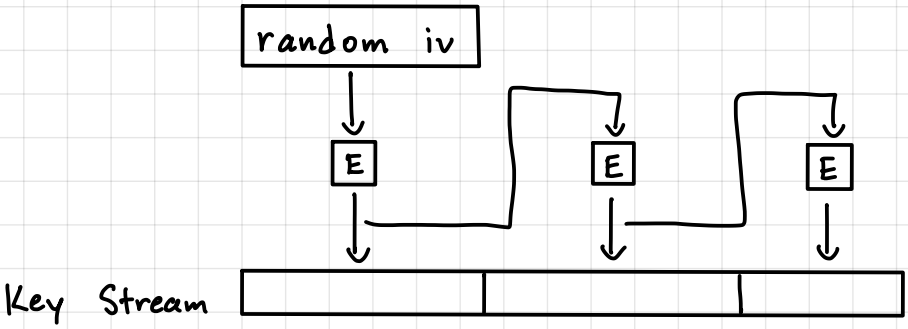






OFB: O

OFB requires an IV, can't generate Key Stream



2a) 010×010

$(x^1)(x^1) \mod x^3 + x + 1$

$x^2 \mod x^3 + x + 1$

$100 \mod 1011$

2b) 011×011

$(x^1 + x^0)(x^1 + x^0) \mod x^3 + x + 1$

$x^2 + x^0$

101

2c) 101×101

$(x^2 + x^0)(x^2 + x^0) \mod x^3 + x + 1$

$x^4 + x^0 \mod x^3 + x + 1$

$10001 \mod 1011$

$$\begin{array}{r} \quad\quad\quad 1 \\ 1011 \overline{)\,10001} \\ -1011 \\ \hline 00111 \end{array}$$

2d) $010 + 010$

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