
None of the problems on this assignment are graded. Instead, after completing it, please fill out the associated Google form. That form is the only graded component.

Math Background

Exercise 1. *Express the following decimal (base 10) integers in binary (base 2).*

- *17*
- *32*
- *67*

Exercise 2. *If we have an encryption scheme that may be written as* $E(p,k) : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ *where p is a plaintext message, and k is a key, what are their respective lengths in terms of variables in that representation of the function.*

Cryptography

Exercise 3. *In the class we talked about the exclusive or (XOR) operator, there is also an inclusive or operator (written as* $b_1 \vee b_2$*), the only difference is that the* $1 \vee 1 = 1$ *as opposed to the exclusive or where* $1 \oplus 1 = 0$*.*

Consider the a cipher like the XOR cipher we discussed in class. If you replaced the exclusive or with the inclusive or does this still create a cipher? Why or why not?

Exercise 4. *Try and come up with your own block cipher by combining various bitwise operations. Remember, it must have an inverse. Look at the lecture notes for a link to a page with many bitwise operations.*

Bonus

Exercise 5. *We said that in the key lenght must divide the plaintext lenght. For a plaintext message of bit length n, and a key of bit length k, where k divides n, what ratio of k and n do you expect will produce the most secure cipher?*