

1. How do you decrypt a message that has been encrypted using this [XOR] scheme?

The inverse of the XOR function is the XOR function. To decrypt it. You just need to reapply XOR

2. How do you shift left in LC3? How do you right shift in LC3?

- a. Multiply by 2 for every left shift

- b. Divide by 2 for right shifts

3.

Subroutines

Encrypt- Ran encryption subroutines

Decrypt- Ran Decryption Subroutines

Caesar- Took the keys y_1 y_2 y_3 and added the 3 digit number $y_1y_2y_3$ to each character in the message. It then took the mod128 of this result and restored them in memory

Vignenere- This took the key x_1 and ran x_1 XOR (character) on each character and restored them in memory

UnCaesar- caesar but it did $((128 - \text{key}) + (\text{char})) \bmod 128$

UnVignenere- Vignenere except it stores the values at x5000 in the decrypt memory

getKey- Stores the key values at x4100

getMessage- Stores the inputted message at x4000

checkKey- checks if the key fits the specs (1 int between 0 and 8, one non numerical char or 0, a 3 digit number between 0 and 127)

checkMsg- checks if the msg fits the specs (10 printable characters)