Math 314 - Fall 2019 **Name:**
Mission 5 Due October 14th, 2019

It used to be expensive to make things public and cheap to make them private. Now its expensive to make things private and cheap to make them public.

— Clay Shirky

Guidelines

- All work must be shown for full credit.
- You can choose to use SageMath code to help you solve the problems. If you do, print out your code.
- Either print out this assignment and write your answers on it, or edit the latex source. Make sure you still show your work! There is one point of extra credit available on this assignment if you use LaTeX
- You may work with classmates, but be sure to turn in your own written solutions. Write down the name(s) of anyone who helps you.
- Check one:
  □ I worked with the following classmate(s): ______________________
  □ I did not receive any help on this assignment.

1. Graded Problems

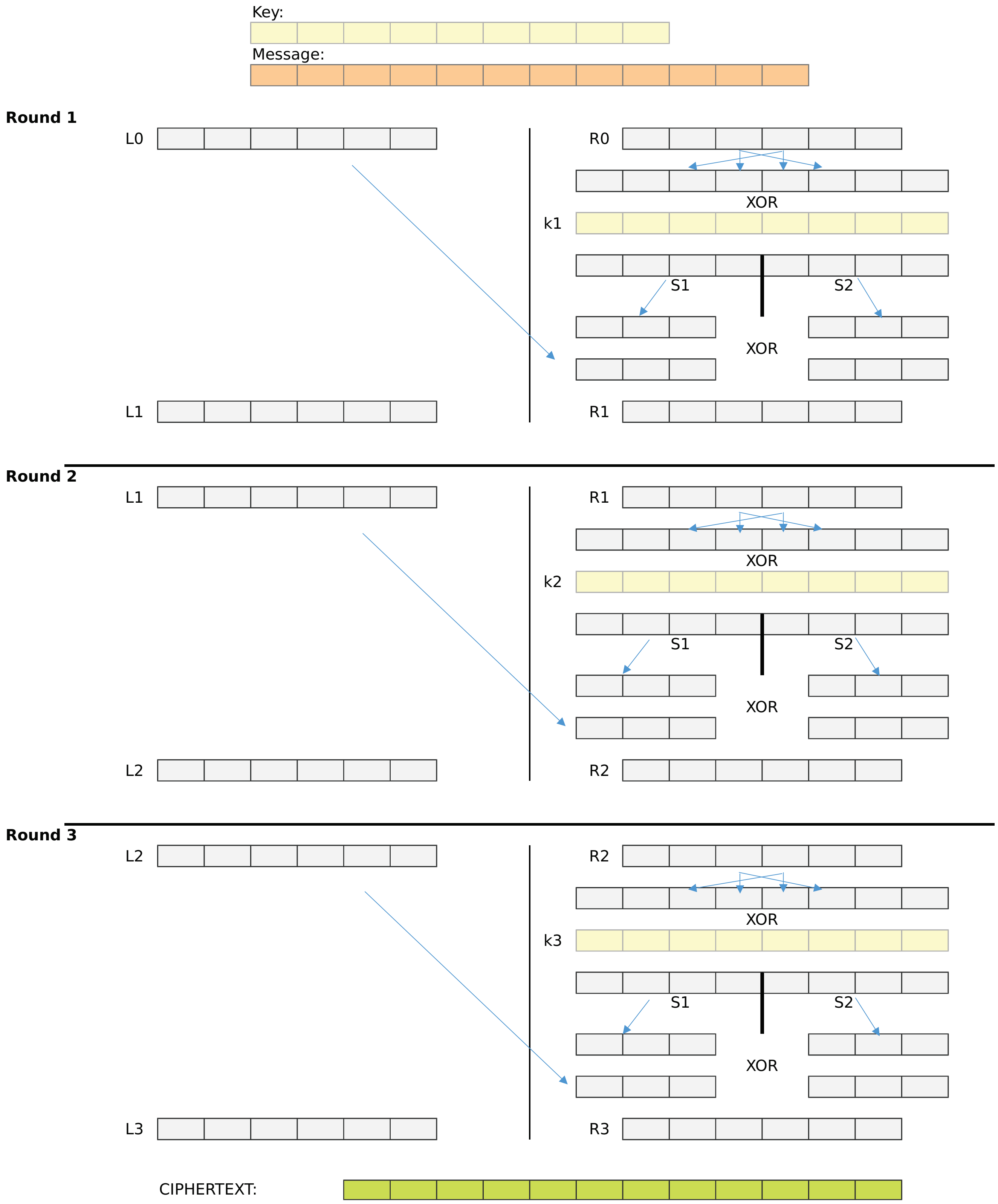
1. Use the rules for Jacobi Symbols instead to determine whether 41 is a square modulo 71.

2. Let $p \equiv 3 \pmod 4$ be prime, and write $p = 4k + 3$. Give a proof that the equation $x^2 \equiv -1 \pmod p$ has no solutions. (Hint: Suppose x exists. Raise both sides to the power $(p-1)/2$ and use Fermats theorem.)

3. Use Fermat's primality test to test 31 and 33 for primality using the bases 2 and 5.

4. Use the worksheet attached to encrypt the plaintext $P = 001110101110$ using SDES with Master Key $K = 011101110$. (Note this problem must be written on this sheet, other submission formats won't be accepted.)

Simplified DES algorithm from Trappe and Washington


Key:
Message:
Round 1
L0
R0
XOR
k1
S1
S2
XOR
L1
R1
Round 2
L1
R1
XOR
k2
S1
S2
XOR
L2
R2
Round 3
L2
R2
XOR
k3
S1
S2
XOR
L3
R3
CIPHERTEXT: