

Two pages, 4 problems, 10 points. Show all work. No calculators.

Problem 1 (1 point). What is a man-in-the-middle attack?

It's when someone intercepts your messages by being "in the middle" between you and the recipient.

Problem 2 (1 point). Decode the following text using one of the cypher methods we have used:
sdrawkcaB nettirw

written backwards

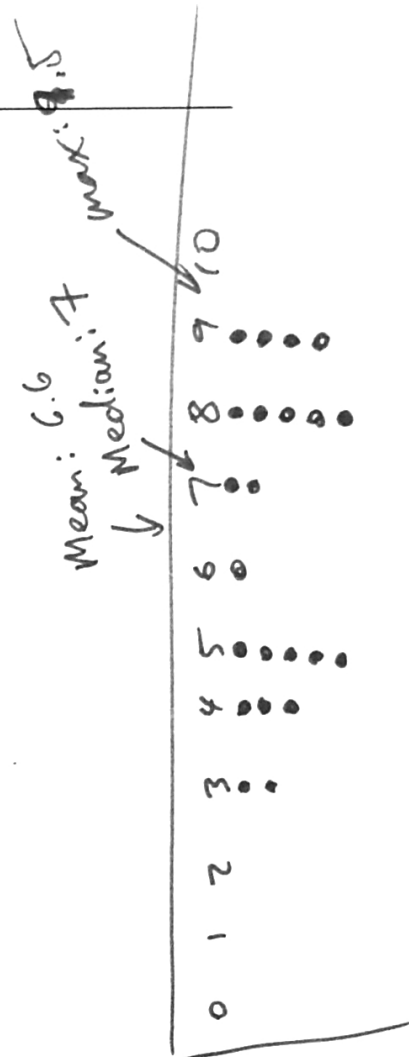
Problem 3 (3 points). Write out the truth table for " $(A \text{ xor } B) \text{ and } A$ ".

A	B	$A \text{ xor } B$	$(A \text{ xor } B) \text{ and } A$
T	T	F	F
T	F	T	T
F	T	T	F
F	F	F	F

$$\left. \begin{array}{l} T \\ T \\ F \\ F \end{array} \right\} \Rightarrow -2$$

Problem 4. (a) (1 point) Write the multiplication table mod 5.

1	2	3	4
2	4	1	3
3	1	4	2
4	3	2	1



(b) (1 point) What numbers are zero-divisors mod 5?

None.

(c) (1 point) What numbers have square roots mod 5?

4, 1, 0

optional since we didn't include it in class. → = 0

(d) (2 points) Use the quadratic formula to find all x satisfying $x^2 + 5x + 1 = 0, \text{ mod } 5$.

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$\frac{-0 \pm \sqrt{0^2 - 4}}{2}$$

$$\frac{-0 \pm \sqrt{-4}}{2}$$

$$\frac{\pm \sqrt{1}}{2}$$

$$\frac{\pm 1}{2}$$

$x^2 + 1 = 0 \Rightarrow b = 0$

~~$\frac{0 \pm \sqrt{0^2 - 4}}{2}$~~

$\frac{1}{2}$ or $-\frac{1}{2}$

so $\boxed{3 \text{ or } 2}$

Check:

$3^2 = 4$

$3^2 + 1 = 0 \quad \checkmark$

$2^2 = 4$

$2^2 + 1 = 0$