

Cryptography succeeds when its no longer the weakest link.

— Ron Rivest

GUIDELINES

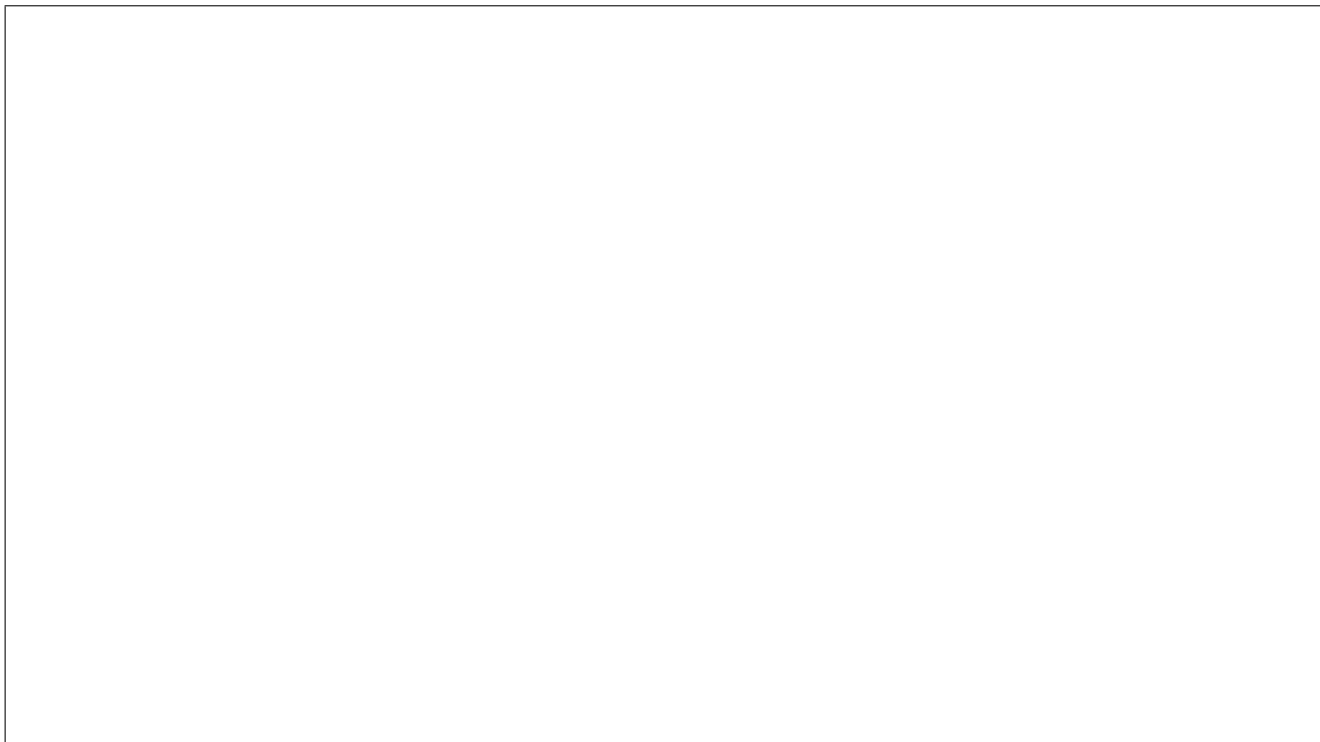
- All work must be shown for full credit.
- You can use CoCalc to help solve the problems. If you do, print out your code.
- You may work with classmates, but be sure to turn in your own written solutions. Write down the name(s) of anyone who helps you.
- Check one:
 - I worked with the following classmate(s): _____
 - I did not receive any help on this assignment.

1. GRADED PROBLEMS

1. Use the Euclidean Algorithm to find the gcd of 191 and 72.

2. Use the Euclidean algorithm to find x and y so that $23x + 79y = 1$. What is $23^{-1} \pmod{79}$?

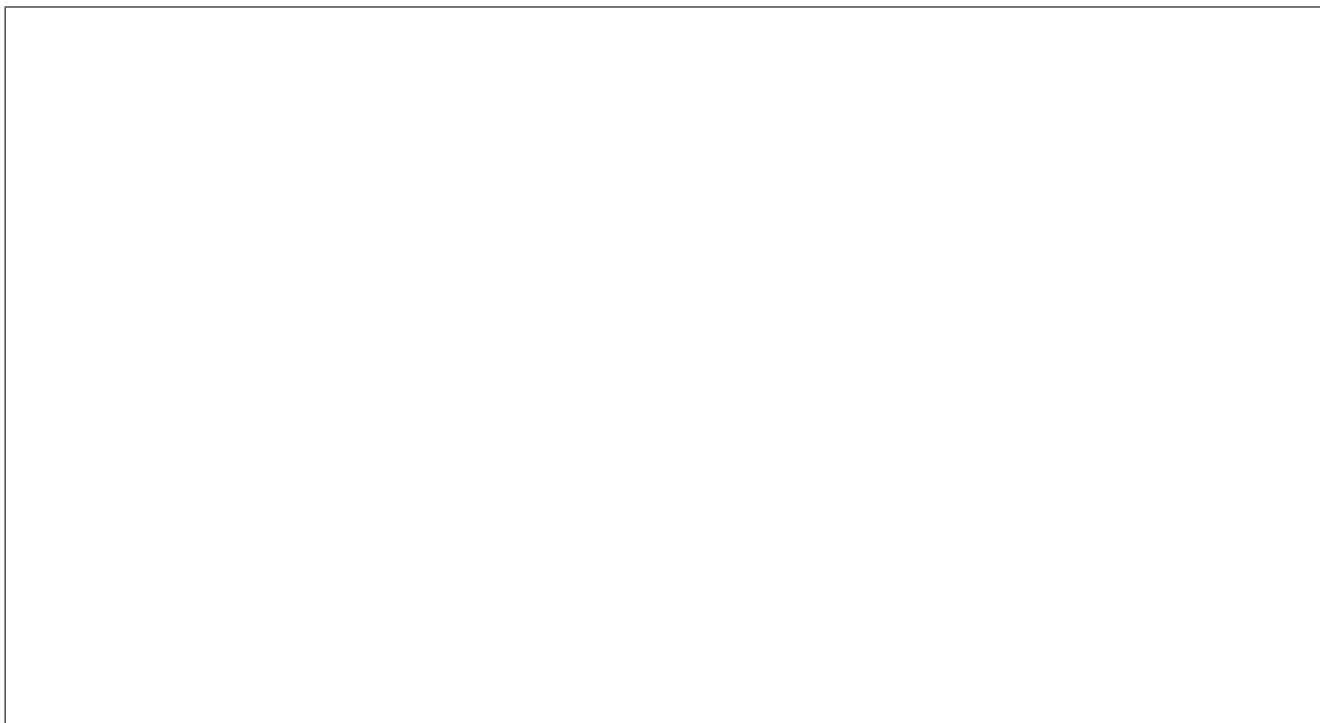
3. Use modular exponentiation to compute $4^{268} \pmod{25}$. Make sure to show your steps.



4. Let F_n be the n -th Fibonacci number, where $F_1 = 1$, $F_2 = 1$, and for $i > 2$

$$F_i = F_{i-1} + F_{i-2}.$$

(a) What is $\gcd(F_9, F_8)$? How many steps of Euclid's algorithm are needed?



- (b) For any $n > 2$ what is $\gcd(F_n, F_{n-1})$? How many steps does it take? Prove your answer. (Induction may be helpful...)

2. RECOMMENDED EXERCISES

These will not be graded but are recommended if you need more practice.

- Section 3.13: # 1, 4, 18