

*Cryptography succeeds when its no longer the weakest link.*

— Ron Rivest

---

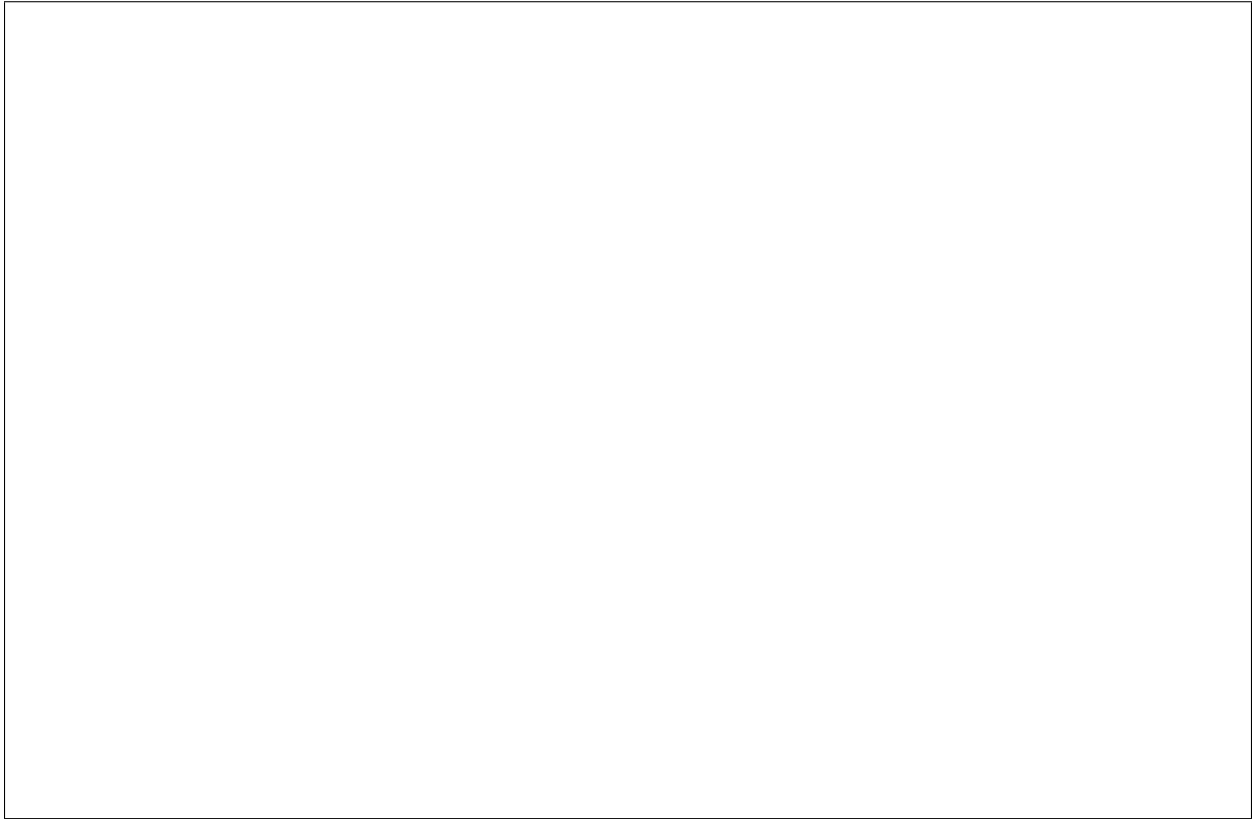
### GUIDELINES

- 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.
- 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.

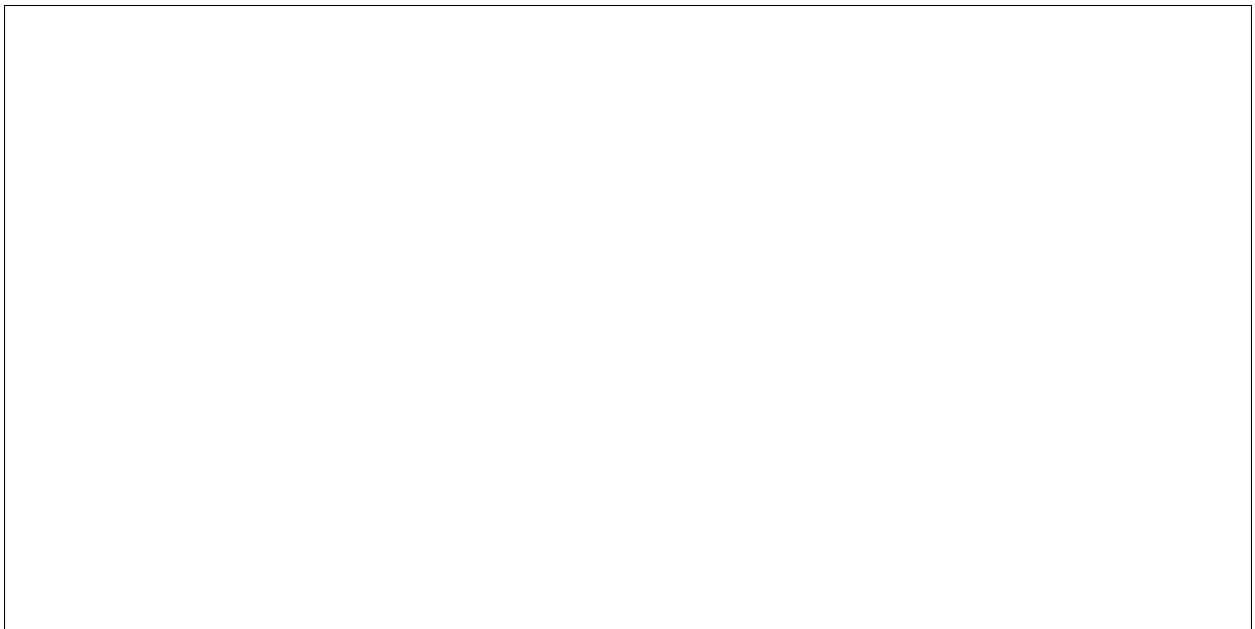
### 1. GRADED PROBLEMS

1. Use the Euclidean Algorithm to find the gcd of 250 and 1023.

2. Use the Euclidean algorithm to find integers  $x$  and  $y$  such that  $33x + 113y = 1$ . What is  $33^{-1} \pmod{113}$ ? Show all of your steps!



3. Use modular exponentiation to compute  $5^{268} \pmod{34}$ . Make sure to show your steps.



4. Alice wants to send a message to Bob using the 3-pass protocol. She decides to use the prime  $p = 43$ , and picks her key,  $a = 5$ . Bob picks his key,  $b = 25$ .
- (a) What are Alice and Bob's decryption keys? Find them using Euclid's algorithm.

- (b) Alice wants to send the message  $m = 3$ . Find the values of each of the messages that Alice and Bob send back and forth. Does Bob recover Alice's plaintext at the end?

## 2. RECOMMENDED EXERCISES

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

- Section 3.13: # 1,4,18