

Lots of people working in cryptography have no deep concern with real application issues. They are trying to discover things clever enough to write papers about.

— Whitfield Diffie

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 (or use the same folder as the latex code on SMC).
- Either print out this assignment and write your answers on it, or edit the latex source on SMC and type your answers in the document. 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. 6.8.13 (Describe the steps, then use SAGE to do the numerical calculations.)

2. Read section 6.5 and give a brief summary of it. What is a squeamish ossifrage, and what does it have to do with cryptography?

3. Exercise 6.8.20

4. With $p = 11$ and $\alpha = 2$, suppose Alice chooses the secret value $x = 5$ and Bob chooses $y = 12$. Show and explain all of the steps of the Diffie-Hellman Key exchange. What value do they agree on for their key?

2. RECOMMENDED EXERCISES

These will not be graded.

- Section 6.8: # 11,