CS 491/591 Spring 2013 Lab 3 – 10 points

This is due as a physical turn-in at the beginning of class on Tuesday, 5 March. You will turn in a single sheet of 8.5” by 11” paper with writing/drawing on only one side. The sheet should not be stapled or folded. It should have your name on it. Your name, paragraph, and drawing should all be on one side of the paper, and the other side completely blank.

Your drawing and paragraph of explanation should design an RSA demo that you could perform, e.g., for high school students. You might be asked to do the demo for the class, but don't let that constrain your ideas about what you draw up and submit. You might want to suggest building something or using something that is not readily available in your demo, go ahead and do that and we can worry about if it's worth it or not after the class discusses your concept. Whether you end up doing your demo in class or not won't affect your grade at all. Writing a program for the demo is okay, too, but it should be visual.

You may discuss this assignment with your classmates and others at any level of detail you wish, but you should each submit something unique. You can use any online or offline resources you wish, as long as you do your own assignment.

The purpose of this assignment is to gain a more fundamental understanding of RSA. An ulterior motive of mine is to have a cool RSA demo I can show to high school students (or even younger students).

I sent out a couple of YouTube videos, one about Diffie-Hellman and one about RSA. The Diffie-Hellman one had a cool example of mixing colors of paint, and we'll go over that example with food coloring in class. We want a similarly intuitive, relatively math-free, example for RSA. I don't know what that would look like, maybe using a deck of cards, a rope wrapped around some pegs, some gears turning, or something.

Some hints to help you get started (some of them might confuse more than help, though):

- What makes RSA different from Diffie-Hellman, and therefore what should distinguish your submission from the paint demo in the YouTube video, is encryption/decryption, authentication, and non-repudiation. Diffie-Hellman is really only good for key exchange, and provides no authentication even for that.
- Modular exponentiation is what really makes RSA work, without it encrypting and decrypting would be just as expensive as factoring the product of two large primes.
- “Ring theory” and the “public and private directions” are how people who know RSA well describe their intuitions about it.
- Shor's algorithm might provide a good intuition about RSA, or might confuse high school students beyond the point of no return. I'll send out a blog post that provides an

"intuitive" explanation of quantum computing. There is some kind of duality between quantum computing and asymmetric crypto such as RSA, so quantum might be a good way to arrive at an intuition about RSA in a round-about way.

- When trying to think up the kind of open-ended thing that this assignment is about, I find that sniffing cheap, generic brand whiteboard markers puts me in the right frame of mind faster than the Expo ones.
- One idea might be a computer visualization of gears turning, with modular-exponentiation being some kind of "fast-forward" turning of a gear. For example, the gears could be large quantum numbers in terms of their circumference and then visually somehow you show how you could spin a gear really fast using powers of two.