Math 11200/20 homework 8
Due date: Monday, November 21, 2016 (Note the due date!)

Please present your solutions clearly and in an organized way. Think of it this way: if you show it to another student in this class, he/she should be able to understand it without needing to ask you questions.

In this problem set, there are some large calculations. Please do not do them by hand! Use Wolfram Alpha, for example:

- http://www.wolframalpha.com/input/?i=inverse+of+19203+mod+28943
- http://www.wolframalpha.com/input/?i=4%5E299103+mod+12839
- http://www.wolframalpha.com/input/?i=solve+9+x+%2B+3+%3D+8+mod+100
- http://www.wolframalpha.com/input/?i=eevee+curve

Problem 8.1. To use RSA, we need a way to encode things as numbers. Instead of encoding each letter separately, let's encode the entire message as a number. We use the following rule:

letter	A	B	C	D	⋯	⋯	W	X	Y	Z
encoding	11	12	13	14	⋯	⋯	33	34	35	36

(We want every letter to be associated to a 2-digit number. Note that the textbook actually does $A \to 01$, $B \to 02$, etc., which also works, but is more complicated.)

For example, "HELLO" becomes the single number `1815222225`.

(a) Encode: "BYE"
(b) Decode: `231130181929163124`

Problem 8.2. Bob tells Alice to send him a message securely via RSA. He tells Alice (and the public) the numbers

$$n = 30796045883 \qquad \text{and} \qquad e = 48611.$$

(If you don't remember what this means, see the lecture notes.)

(a) What is the encryption function?
(b) Alice wants to send the very important message "HELLO." So as before, we encode it as `1815222225`. What number does Alice send to Bob?
(c) What does Bob do to decrypt Alice's message? Please check that what he does actually does decrypt the message.

Problem 8.3. Bob is using RSA with

$$n = 956331992007843552652604425031376690367 \qquad \text{and} \qquad e = 12398737.$$

Eve the Eavesdropper observes that Alice sends him the following encrypted number:

$$136918035529722837836652077416303475217$$

What is Alice's message?