Introduction to Number Theory

Spring 2016

Homework # 7
Last Updated: March 24, 2016
Due Date: Thursday April 7th.

I recommend that you review the material from the first 18 chapters of the book. When we return from spring break, we won't be directly following the book. But the closest material is from Chapters 35 and 36.

FRINT Chapter 16:

(1) 16.1 (Note: the purpose of this exercise is to emphasize that it's very easy to compute $a^k \mod m$, even if k is really large. You can do this exercise comfortably on a four-function calculator)

FRINT Chapter 17:

(2) 17.1
(3) 17.2
(4) 17.5

FRINT Chapter 18:

(5) 18.1
(6) 18.2

Extra Credit Exercises:

(7) In this exercise, you will actually send me a securely encrypted message. In principle, this should not be too hard. But in practice, it can be a bit hard. We break this exercise into multiple parts. If you encounter trouble, feel free to email me.
   (a) *To send me a message, you need my public key. You can find my key on public keyservers associated to the name "davidlowryduda".* Find and save my public key by looking at the MIT keyserver, pgp.mit.edu. (If you want to make sure you have the right key, the associated keyid begins "BF7F0291".)
   The key you now have is associated to the gpg encryption protocol, which is one of the better-known protocols. In order to use my key to send me a message, you need to figure out how to use gpg. I recommend that you follow a tutorial on gpg for your operating system.
   (b) Decide on a message you want to send me. One idea might be to write something about your favorite aspect of the course so far. Or perhaps about what you've done over spring break.
   (c) Encrypt your message using my public key, and send it to me. I will respond to say if everything went smoothly.

(8) In this exercise, you will create a public key, send it to me, and figure out how to decrypt a message.
   (a) Follow a tutorial on creating a gpg public key, and send me your public key.
   I will then send you a message encrypted with your public key.
   (b) Decrypt the message.
   The message will contain a question.
   (c) Send me an email response to the question in my message, so that I know that you have successfully decrypted a message.