Algebraic Cryptography
Homework 3

Due Monday, 25 September 2017

Note: this is graduate school, so due dates for homework are somewhat flexible (within reason). I trust you to make smart decisions regarding your understanding of the material. I encourage you to do these problems before the exam, but if you are having trouble completing the write-up while studying, that is okay.

Problem 1. Exercises 1,3,5 §3 of Chapter 2 (with proofs / arguments)

Problem 2. Exercises 6,7,9 from §4 of Chapter 2 (with proofs / arguments).

Problem 3. Using the work done both on previous homeworks, prove that the RSA encryption and decryption protocols have polynomial time algorithms (in terms of the lengths of the keys). Try to provide a bound on the degree of the polynomial. Note: you do *not* need to show at this time that there is a polynomial time algorithm for RSA key generation.