Math 437 – Homework 7

Due 10:15am on Thursday, March 2, 2017

Please indicate any sources you used for a given problem on the solution to that problem. For example, if you worked with another student to get the solution to a problem, please indicate who. You are welcome to work together in small groups, but please try the problems on your own first and write up your own solutions.

Problem 1. Ch. 8 #7 (on page 304)

Problem 2. Ch. 8 #19 (on page 306)

Problem 3. Alice wins a trip to meet a certain celebrity, and she wants to tell Bob the good news privately. The public part of Bob's RSA key is $n = 308911$ (which factors as $541 \cdot 571$).

(a) Alice and Bob want to agree on a secret RSA exponent using Diffie-Hellman key exchange. Bob chooses $k = 13$ and $r = 13$ and sends k and $k^r (\text{mod } n)$ to Alice. He receives back $k^s \equiv 39584 (\text{mod } n)$. What secret exponent a will Alice and Bob use?

(b) Alice uses the exponent a to encrypt the zip code where she is going and sends Bob the encrypted message 164103. What is the zip code and who is she meeting?