Homework 32, due November 29

(1) (Problem 1, Page 303) Suppose you have a secret, namely 5. You want to set up a system where four persons A, B, C, D are given shares of the secret in such a way that any two of them can determine the secret, but no one alone can determine the secret. Describe how this can be done. In particular, list the actual pieces of information (i.e., numbers) that you could give to each person to accomplish this.

(2) (Page 304, problem 8) There are four people in a room, exactly one of whom is a foreign agent. The other three people have been given pairs of numbers corresponding to a Shamir secret sharing scheme in which any two people can determine the secret. The foreign agent has randomly chosen a pair. The people and pairs are as follows. All numbers are modulo 11.

$$\text{Alice} : (1, 4)\ \text{Bob} : (3, 7)\ \text{Charles} : (5, 1)\ \text{Donald} : (7, 2)$$

Determine who the foreign agent is and what the message is.

(3) Alice and Bob want to use quantum key distribution to generate a shared 128-bit AES key. Assuming no one is eavesdropping or interfering in their protocol, roughly how many bits should Alice send to Bob so they have a good chance of sharing 128 bits?