Homework 7, Due Fri July 24, 2015

1. (30 points) Zelda wants to share the secret 101 such that if Alice and Bob both get together they can crack it, but neither one separately.

   (a) Assume she uses the random-bits method and gives Alice the random sequence of bits 000. What does she give Bob? Should she worry that she is giving away too much information?

   (b) Assume she is using the polynomial method with prime $p = 7$ and random $a = 2$. What does she give Alice? What does she give Bob?

   (c) Assume that Zelda, Alice, and Bob want to do verifiable secret sharing. Assume that Zelda chooses the generator $g = 3$. What additional information does Zelda give to Alice and Bob.

2. (30 points) Zelda wants to share the secret 11001 with $A_1, \ldots, A_{100}$ such that if any 2 of them get together they can crack it, but no single person can crack it.

   (a) If she uses the random-string method then how many strings will she give to each person?

   (b) If she uses the polynomial method then how many strings will she give to each person?

3. (40 points) Zelda's has a secret. She wants to give shares of it to Alice, Bob, and Carol so that all three of them can find it, but no two can. She uses the prime $p = 23$ which she tells all of them. She then tells Alice $(1, 10)$, tells Bob $(2, 5)$, tells Carol $(3, 10)$.

   (a) What polynomial did Zelda use? What is the secret?

   (b) Zelda will use $g = 4$ for Verifiable Secret Sharing. If they want to do a Verifiable Secret Sharing, what other information does Zelda send?

   (c) Alice and Bob get together. Alice LIES and tells Bob that her share is $(1, 4)$. Show how her lie will be discovered!

   (d) Look at what Zelda send ALL of Alice, Bob, and Carol so they could verify. Did she give away too much information? If so, what advice would you give Zelda for the future.