HW 9, Due Jan 15

READ THE NOTES ON SECRET SHARING
THIS HW IS TWO PAGES LONG!!!!!!!!!!!!

1. (20 points) Zelda wants to share the secret 101001 such that if Alice and Bob both get together they can crack it, but neither one separately. Assume she uses the random-bits method and gives Alice the random sequence of bits 000000 What does she give Bob? Should she worry that she is giving away too much information?

2. (30 points) Given the points $(1, 3)$ and $(3, 4)$ we want to find a line (of the form $y = mx + b$) that goes through both points.

   (a) Assume we are operating over THE REALS. What is the line?

   (b) Assume we are operation over MOD 7. What is the line? (ALL COEFFICIENTS ARE IN $\{0, \ldots, 6\}$.)

   (c) Assume we are operation over MOD 11. What is the line? (ALL COEFFICIENTS ARE IN $\{0, \ldots, 10\}$.)

   (d) Give a composite number n such that there IS a line mod n for this problem. (ALL COEFFICIENTS ARE IN $\{0, \ldots, n-1\}$.) FIND the line mod that n.

   (e) Give a composite number n such that there IS NO line mod n for this problem. (ALL COEFFICIENTS ARE IN $\{0, \ldots, n-1\}$.)

3. (30 points) Zelda has a secret of length 7. She has 100 friends! Assume she uses the random string method (NOT the polynomial method).

   (a) She wants to allocate shares of the secret so that if any TWO of them get together they can crack it, but no ONE person can. How many strings does she send? I want an actual number.

   (b) She wants to allocate shares of the secret so that if any THREE of them get together they can crack it, but no TWO people can. How many strings does she send? I want an actual number.

   (c) She wants to allocate shares of the secret so that if any 50 of them get together they can crack it, but no 49 people can. How many strings does she send? I want an answer in terms of factorials since its rather large and might be hard to compute.

4. (20 points) Zelda has a secret of length L. She has n friends! n is even. Assume she uses the random string method. She wants to allocate shares of the secret so that if any $n/2$ of them get together they can crack it, but no $n/2 - 1$ people can. How many strings does she send? Leave the answer in terms of factorials.