OLD FINAL AND EXTRA PROBLEMS as Study Guide

1. The Wisian's have an alphabet of 14 letters.
   (a) How many shift ciphers can the Wisian's use?
   (b) How many affine ciphers can the Wisian's use?

2. For each of the following ways that Alice and Bob can exchange messages in secret (1) describe how the cipher works. (2) given a argument that it is UNCRACKABLE!, (3) describe how to crack it, Clarity is VERY IMPORTANT in this problem!!!!!!!!!!!!!!!!!
   (a) General Substitution Cipher.
   (b) Matrix Cipher with a 10000×10000 matrix. (Warning: You can't just say **By Linear Algebra**.)

3. (READ the entire problem before working on it.) A prime p is called *zell* if $\frac{p-1}{30}$ is prime.
   (a) Give an **efficient** algorithm that will, given a zell prime, and a number g, test if g is a generator (It cannot be brute force.)
   (b) The algorithm you gave above had to take the power of g 6 times. Give an algorithm that takes a power of g LESS than 6 times.
   (c) Use that algorithm on $p = 43$ to find our if 2 is a generator and if 3 is a generator.

4. Zelda has a secret! It is a string of DIGITS, so a string of elements from $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Zelda is NOT going to convert it to binary. She wants to give shares to Alice, Bob, Carol, Donna such that
   - If Alice and Bob get together they can discover the secret.
   - If Bob, Carol, Donna get together they can discover the secret.

   Give a protocol to do this. NOTE that the secret is NOT a sequence of bits, but a sequence of digits.

5. TRUE, FALSE, or UNKNOWN TO SCIENCE. EXPLAIN your answer and be COHERENT, CLEAR, CONCISE. Let s be a secret of length L where $L \geq 50$. Zelda has 100 friends $\{A_1, \ldots, A_{100}\}$. There exists a secret sharing scheme for 10 people, so that if any five of them get together than they can find s, but if 4 get together the know NOTHING about the s, AND A_1 gets a string of length $L-1$ AND $A_2, \ldots, A_{100}$ get strings of length 2^L.

6. Zelda wants to use the polynomial method for secret sharing. She wants to work with polynomials over the rationals. Why is this a terrible idea?