Sample problems:

1. **Precisely how secure is it to perform Vigenere encryption twice with two separate keys, versus performing encryption once? If I insisted on performing vigenere encryption twice, what precautions should I take when choosing the keys?**

   ANS: Vigenere encryption is closed under composition, so encrypting twice is the same as encrypting once with a single key. In particular, if I have two keys of length n and m, encrypting under both keys is like encrypting under a single key of length LCM(m,n). If I insisted on encrypting twice, it would be best to ensure the key lengths are relatively prime.

2. **The letters {E,T,A,O,I,N,R,S,H,D} have a frequency greater than 1/26; the rest have a frequency less than 1/26. Together, those letters represent 74 percent of English text.**
   a. **Describe the optimal algorithm for distinguishing between a letter of English and a letter of Uniform noise.**
   b. **What is the false alarm and miss probability of this detector?**
   c. **Give an example of an English word that would constitute a miss under this detector.**

The optimal algorithm is to compare the likelihood ratio to a threshold. The 10 letters above have a likelihood ratio greater than 1; for a threshold of 1, this means that any of the above 10 letters are declared English, and the rest declared noise.

The false alarm rate of this detector is therefore 10/26, and the miss rate is 26% (26% of English text consists of unpopular letters.) A word guaranteed to cause a miss for this detector would be a word comprised solely of unpopular letters, e.g. CUP.

3. If the alphabet had 27 letters (26 and a space, for example,) how many distinct affine encryption keys would there be?

There are 27 possible shifts, and 18 possible multipliers, because a multiplier that has a factor in common with 27 is not invertible. Hence there are 18x27=486 possible keys.

4. For a given student, we want to tell if he or she graduated from Inflation University (H1) or Gauss College (H0). Either case is equally likely.

We discussed the answer to this question in class.

5. A substitution cipher has a 26-letter alphabet. A key is a table mapping every possible input letter to an output letter in the same alphabet.
a. How many different keys are there?
b. How many different keys are there such that encryption and decryption are the same, i.e. that Decrypt(x,K) = Encrypt(x,K)?

There are 26! = 403291461126605635584000000 possible shuffles of a 26 letter alphabet.

In order for encryption and decryption to be the same, we are counting the number of ways to partition the alphabet into pairs, such as we did with the Vatsyayana cipher. Here, there are $26!/(13!2^{13}) =$ 7905853580625 keys.

6. Provide two permutations f and g, such that $gfg^{-1} \neq f$.

Any two permutations where $gf \neq gf$ would work. Consider, for example, the cycle (1 2 3 4 5 6) and the swap (1 2).

7. Consider the following C function:

```
int f(int x) { return ((x^1)+1) & 0x0f; }
```

This is a permutation on the numbers from 0 to 15. Write this as a product of disjoint cycles.

Testing every value, we get (0 2 4 6 8 10 12 14). This function maps every

odd number to itself, because (x^1) increments an even number and decrements an odd number.

8. Suppose a function maps a finite set A to itself.

a. Prove that if f is an injection, then it is a bijection.

b. Show that this is not true when A is not a finite set.

If f is an injection, then f(A) has as many elements as A, since two distinct inputs map to to distinct outputs. Therefore f has to map entirely onto A.

This is not true when A is a finite set. For example, let A be the integers, and consider the function f(n)=2n.

9. Here is some Enigma-encrypted text:

CMVDMFSRXUJXQUDVRHVYGOKH

HERECOMESAVERYSPECIALBOY

This is the only possible encryption, because an Enigma machine cannot encrypt a letter to itself.

10. Explain why a one-time pad is a theoretically unbreakable form of encryption.

We haven't discussed the mathematical proof yet, but it is sufficient to point out that every possible plaintext could be recovered by decrypting a message with every possible key.