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?

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.

   1. Describe the optimal algorithm for distinguishing between a letter of English and a letter of Uniform noise.

   2. What is the false alarm and miss probability of this detector?

   3. Give an example of an English word that would constitute a miss under this detector.

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

4. Students at Inflation University (left) and Gauss College (right) have the following grade distribution for calculus:

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.

A	B	C	D	F
2%	15%	66%	15%	2%

A	B	C	D	F
80%	10%	5%	3%	2%

(a) Describe the optimal algorithm to determine a student's college, based on his or her calculus grade. Assume a threshold $\tau = 1$.
(b) What are the false alarm and miss probabilities PF and PM ?
(c) Suppose three students are drawn from the same college with grades of D, D and A, respectively. What college do you conclude they graduated from?

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)?

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

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.

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.

9. Here is some Enigma-encrypted text:

```
CMVDMFSRXUJXQUDVRHVYGOKH
```

   Which of these four messages could the text be?

```
a) HERECOMESAVERYSPECIALBOY
b) EVERYGOODBOYDESERVESFLAN
c) BOYIHOPEMYGRADEISAWESOME
d) THISWASEASIERTHANITLOOKS
```

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