Problem Set 5

1. **Secret Sharing Practice**
   On the class webpage, we've set up a secret number, shared between everybody in the class in such a way that 3 students need to cooperate to figure out the secret. So, go to the class webpage, and enter your 8-digit student ID number to obtain your secret. Then, **find 3 other CS70 students** to work on this problem with. The secret is encoded modulo 97.

   (a) (6 pts) Work together with your group to figure out the secret, using the secret shares of 3 of the group members.

   (b) (2 pts) Use the 4th group member's share to *check* that the polynomial you obtained in part (a) is correct (show this on your homework).

   Remember to write up your work independently. List the other members of your group on your homework.

   You may also work in groups of 5 people; in that case, discard one of the secret shares. We encourage you to talk to people after lecture, during the lecture break, or in your discussion section to find a group. You can also try posting on the course newsgroup, `ucb.class.cs70`. If you can't find a group, email your TA to be matched up.

2. **How many secrets?** (4 pts)

   A secret sharing scheme is k-secure if and only if any group of k or fewer people has probability at most $1/q$ of recovering the secret, where q is the number of possible choices for the secret (this means that the best strategy such a group has is to guess the secret at random). In the typical secret sharing scheme, the secret is $P(0)$, the value of a certain degree k polynomial (that we construct) at 0. Suppose that, instead, the secret is $P(0), P(1)$ (the values at both 0 and 1). Of course, we also change the algorithm by handing out $P(2), \ldots, P(n+1)$ to the n people instead of handing out $P(1), \ldots, P(n)$. Is this scheme still k-secure? Prove your answer.

3. **Secret Sharing**

   (a) (4 pts) Suppose that the teaching staff of a course involves three professors and two TAs. The solutions to the next homework are encrypted by an encryption key shared by all five. The three professors together should be able to access the solutions, or any one TA with one professor, or both TAs. Suggest a secret-sharing scheme that achieves this. (*Hint:* Try weights.)

   (b) (4 pts) Suppose now that the class is taught by three professors, each with *her* own two TAs. Any two professors can access the data, as long as one TA from each is also present. Now what?

4. **Error Correcting Code**

   In this question we will go through an example of error-correcting codes. Since we will do this by hand, the message we will send is going to be short, consisting of $n = 3$ numbers, each modulo 5, and the number of errors will be $k = 1$.

   (a) (2 pts) First, construct the message. Let $a_0 = 4$ and $a_1 = 3$, $a_2 = 2$; then use the polynomial interpolation formula to construct a polynomial $P(x)$ of degree 2 (remember that all arithmetic is mod 5) so that $P(0) = a_0$, $P(1) = a_1$, and $P(2) = a_2$; then extend the message to length $N + 2k$ by adding $P(3)$ and $P(4)$. What is the polynomial $P(x)$ and what are $P(3)$ and $P(4)$?

(b) (5 pts) Suppose the message is corrupted by changing $P(0)$ to 0. Use the Berlekamp-Welsh method to find a polynomial $g(x)$ of degree 2 that passes through 4 of the 5 points. Show all your work.

5. **Feedback** (8 pts for answering all questions; no partial credit)
Please be brutally honest. If you would rather remain anonymous, you may give your answers on a separate sheet of paper and turn it in without stapling it to your homework. Label that sheet of paper with your name in the top right corner. The readers will tear off your name after verifying you turned in a survey, and give the separate-page responses to us in a separate stack.

1) The pace of the course is (list all that apply):
   a) Speed of light (very fast)
   b) A bit too fast
   c) Close to my pace
   d) A bit too slow
   e) Way too slow
   f) I sleep in the lectures
2) The pace of discussion in sections is (list all that apply):
   a) Speed of light (very fast)
   b) A bit too fast
   c) Close to my pace
   d) A bit too slow
   e) Way too slow
   f) I sleep in the sections, too
3) How challeging do you find the material covered in class?
   a) Rocket science
   b) Fairly challenging
   c) Just right
   d) Easier than I'd like
   e) I did this in kindergarden
4) Office hours are:
   a) Very helpful
   b) Useful at times
   c) Pointless
   d) What office hours?
5) The homeworks are:
   a) Akin to mediæval methods of torture
   b) Challenging, but help understand the material
   c) Challenging but useless
   d) Of reasonable difficulty
   e) Could be more difficult
6) The example problems used in discussions are:
   a) Akin to mediæval methods of torture
   b) Challenging, but help understand the material
   c) Challenging but useless
   d) Of reasonable difficulty

   e) Could be more difficult

7) The lecture notes are (list all that apply):
   a) The sole way I learn anything in CS70
   b) Occasionally helpful
   c) Too verbose
   d) Too terse
   e) Unreadably complicated
   f) Useless
8) What section do you usually go to, if any?
9) Whose office hours do you usually go to, if any?
10) Give two suggestions for making the sections/office hours more helpful.
11) Give two suggestions for making the lectures better.
12) Give a suggestion for making the lecture notes better.

Please feel free to add any other comments you might have on any part of the course. Thank you.