Due: Wednesday, December 2.

This assignment is worth 10% of final grade

1. Some hard computational problem are easy in special cases. For example, consider the following "graph colouring problem": Given a graph $G = (V, E)$, and an integer k, determine if the vertices V of the graph can be coloured using at most k colours in such a way that if vertices u and v are given the same colour, the (u, v) is not an edge (i.e. (u, v) is not in E). If the graph can be so coloured then find such a colouring of the vertices.

   (a) Show how you can view exam timetabling as a graph coloring problem; that is, the goal is to schedule (if possible) exams in a fixed numnber of time slots such that no student has two (or more) exams at the same time. That is, indicate, what are the vertices and what are the edges.

   (b) In general (that is, for all graphs) we do not know a good method for graph colouring and indeed even for $k = 3$, it is an NP-hard complete problem to determine if a graph has a 3 colouring. On the other hand, it is easy to find a 2 coloruing if one exists. Describe how you could determine if a graph $G = (V, E)$ could be coloured with just 2 colours.

   (c) For the timetabling problem, what features of the graph might make it easy to help find a solution. Describe any "reasonable approach" a University might use if a solution cannot be found.

2. Suppose you want to choose a sequence of (say) 100 decimal digits to be used as a private key (in a cryptographic protocol) or an initial seed (for say a pseudo random generator). How would you choose such a sequence? Can you think of some physical observation or soucre of information that can be used for this purpose?

3. Let $p = 7, q = 23$ and let $N = p \cdot q = 161$. Choose an initial seed x_0 as in the previous question (or use your 7 or 8 digit ID mod 161 from assignment 1). Generate the sequence $x_0, x_1, \ldots$ using $x_i = x_{i-1}^2 mod N$ until some number x_i is repeated; that is, $x_i = x_j$ for some $j < i$. What is the value of $j - i$? Having written down $x_0, \ldots x_i$ for the i such that x_i is the first repeated number, see if you can reproduce this sequence of numbers after not looking at it for at least an hour. Describe how good your memory was. That is, how much of the sequence were you able to remember withour error or how few errors did you make in trying to remember the sequence.