OPERATING SYSTEMS 2009 Exercise 5

1. Often asterisks instead of letters are shown in a field where you enter a password. The alternative to this is to not show anything at all (then a potential hacker, who can see the screen, will not know the length of the password). Assuming passwords consisting only of the lower-case letters 'a' to 'z' of length 5 to 8 characters, how much safer is it to not show anything on the screen? (2p)

2. Let's assume we can crack a system using 56-bit encryption keys in one hour today. Which year will we then be able to crack a system using 2048-bit keys in one hour, assuming processing capacity is doubled every half year? (2p)

3. Describe step-by-step which data structures and data blocks need to be accessed in order to read the first block in a file, given its name. Assume nothing is stored in cache memory, and that the file can be found in the root folder of the file system.
   a) Describe it for a FAT-based file system
   b) Describe it for an i-node based file system.

4. In a file system where the clusters (blocks) are kept track of using a file allocation table (FAT), we can choose the cluster size for the system. Of which size should the clusters be, in order for the space lost due to internal fragmentation to be less than the space that the file allocation table occupies, when the disk is full? We assume that the median file size is 8kB, and that the FAT-table elements are 32 bits. (2p)

5. Write - in your favorite programming language – an implementation of the elevator algorithm, which for a given sequence of requested cylinder read operations, schedules these read operations. The program should also calculate the total number of disk arm movements. Show the results for the sequence {12, 44, 89, 33, 51, 22, 73, 28}.