1. Consider a process (A) that generates one of the following characters every second: A-Z, a-z, 0-9, $, or %.
    a.

Characters	Probability of one of the characters
0-9	1/16
A-Z	1/(8*26)
a-z, $, %	1/(4*28)

What is the Entropy of this system? You can do it by hand or use a spreadsheet or code. Please describe or show your work.

    b. If each character above is equally likely, what's the Entropy?
    c. Now, consider process B that generates two characters uniformly randomly every two seconds to generate a two-character message, e.g. ZY or CC. What's the entropy of each two character message? What's its relationship to your answer in part b and why?

2. Consider a physical door lock with a 16 character key pad (0-9 and A-F). The lock stores a single 4 character password which a user must enter to unlock the door. Alice is in charge of generating passwords and programming the lock. Bob wishes to guess the password, but has no information other than the general mechanism Alice uses to generate the passwords.
   Calculate Bob's Expected Uncertainty (Entropy) in the password given Alice's following approaches.
    a. Alice is numerophobic so she chooses uniformly random letters only…. no numbers.
    b. Alice chooses each character by pulling the characters out of a hat and then replacing the characters before drawing another. (Cryptographically random)
    c. Alice flips a fair coin 4 times to generate a number between 0 and 15. We will call this number, s. The first character is the hexadecimal representation of s. The second character is hexadecimal representation of (2s +1) mod 16. The third is the hexdecimal representation of (3s+ 2) mod 16 and the fourth is (s+15) mod 16.
    d. Alice chooses four character l33t speak words at random that are representable using 0-9 and A-F … see http://www.datagenetics.com/blog/march42013/index.html for a list of such words.
    e. (This one you cannot directly calculate.) Alice chooses words as in d, but instead of by uniform chance, she picks familiar words to her. What happens to the resulting entropy in comparison to d) and b).

3. A system has a 3 ring security model similar to that discussed in class. Ring 0 is used for a hypervisor, HV, managing virtual machines, Ring 1 is used for the O/S kernel of any of the virtual machines running, and Ring 2 is used by applications running in those virtual machines.

Assume you have AppA running on Linux in VmA and AppB running on BSD on VmB on the above system. AppB and AppA have opened a network socket between them and have can use system calls to read from and write from the socket, readSock() and writeSock().

a) AppA perfoms a writeSock() system call. What happens in terms of the system call interface and the ring values?

b) What must happen for the data to be transferred between VMs? (in terms of rings)

c) Assume AppB is waiting for data having called readSock(). What does the BSD kernel have to do to get the data to AppB.