Problem 1 The Internet is, slowly, transitioning from the version of the TCP/IP protocol suite currently in use—IPv4—to a new version, IPv6.

Unlike IPv4 IP addresses, which are 32 bits long (e.g., 192.168.10.1), IPv6 IP addresses are 128 bits long (e.g., 2001:1890:1112:0001:0000:0000:0000:0020).

(a) Consider random-scanning Internet worms. These worms spread by choosing a random IP address, connecting to any host answering to that address, and attempting to infect it.

Is the random-scanning strategy feasible if the Internet switches from IPv4 to IPv6? Why or why not?

*Hint:* Consider the density of Internet-connected machines in the IP address space.

(b) On the IPv6 Internet, what are some specific ways that a worm, executing on a compromised computer, can discover IP addresses of other hosts to try to infect?

*Hint:* Consider sources of IP address on the infected computer itself and on the local-area network to which it is connected.

(c) Suppose the worm targets Web servers running some application (say, bulletin board software written in PHP). Can Google searches help the worm find potential targets? How?

Problem 2 The most commonly used keyed lock is a pin tumbler lock, shown in Figure [1].

This type of lock features \( k \) pin stacks (typically 4 to 7, with the lock in the figure having 6), each cut at one of \( n \) possible depths (typically 4 to 10), which are held in the plug by springs.

A key has bitings at a certain depth for each pin stack. When the key is inserted into the keyway, its bitings push each pin stack up by a certain amounts. The correct key will cause each to be pushed so that its cut aligns with the shear line that separates the plug from the shell, allowing the plug to rotate, as shown in Figure [2].

In many institutional settings a master-keying system is used, where each of several locks (say, one for each room in a dorm) has a different change key, but all share a single master key. This is most commonly implemented by including two cuts in each
Figure 1: On the left, the lock face. On the right, a cutaway view showing six pin stacks and (horizontal) shear line. The pin stacks keep the plug from rotating within the shell and opening the door.

Figure 2: On the left, a cutaway view showing the correct key inserted in the lock. Note that the cuts in the pin stacks are aligned with the shear line. This allows the plug to rotate, as shown on the right.

Figure 3: On the left, a cutaway view of a master-keyed lock. Note that each pin stack has two cuts. On the right, the lock with the change (non-master) key inserted. One set of cuts is at the shear line; the other cut for each stack is either above or below.
pin stack, one for the change key, the other for the master key, as shown in Figure 3. The locks will each have different change cuts, but all share the same master cuts, so the same master key will open all of them. The change key and the master key never share a cut: in each pin stack there is one cut for the change key, and another at a different depth (either above or below) for the master key.

a. Suppose that a lock is keyed with the change key at 11111 (five pins, all at depth 1), and the master key at 44444 (five pins again, all at depth 4 this time). Will a key cut at 11411 open the lock? Explain.

b. Suppose you have access to a master-keyed lock, a change key that opens it, but not the master key. In addition, you have a supply of blanks that can be filed down to specific bitings of your choice. Explain how to use the observation from part a. to recover the master key.

As a function of \( k \) and \( n \), how many blanks will you need? How many tries in the lock?

c. Suppose you have access to the change keys for many locks all keyed for the same master key (but, again, no access to the master key). For example, suppose that you measure the biting on the keys given to all the residents in a dorm. Explain how you can (with high probability) recover the master key without any blanks — and even without access to any of the locks!