Homework 2

This assignment is due in class on October 9, 2001. It covers readings and lecture notes through October 4, 2001. Late homework will not be accepted.

Write your name, email address, and date on the paper that you hand in.

One of the simplest and oldest cryptosystems is the "shift cipher." The cleartext is a text message, the key is a number k between 1 and 25, and encryption is accomplished by shifting each letter of the cleartext k places to the right (wrapping around from the end of the alphabet back to the beginning when necessary). Thus, if the key is 10, the cleartext "OneIfByLandTwoIfBySea" is mapped to the ciphertext "YxoSpLiVkxnDgySpLiCok." To decrypt, each letter is shifted k places back to the left (wrapping around the other way when needed). Cryptologic folklore has it that Julius Caesar used the shift cipher with k equal to 3; this special case is often referred to as the "Caesar cipher."

1. (5 points) What is the ciphertext produced by the shift cipher if the cleartext is "TOBEORNOTTOBETHATISTHEQUESTION" and the key is 20?

2. (10 points) The shift cipher is completely unusable in practice, because an eavesdropper who obtains a ciphertext can determine the cleartext even if he doesn't already have the key. Convince yourself of this by breaking the cipher: What is the cleartext that corresponds to the ciphertext "ULPAOLYHIVYYVDLYUVYHSLUKLYIL"?

A far more powerful result can be accomplished by implementing encryption using a "one-time pad." One variety of one-time pad uses as a key a text of the same length as the cleartext; the characters of the key are used one by one to indicate how to transform each character of the cleartext. The characters of the key could, for example, be used to indicate how far to shift each character of the cleartext. For instance, if the cleartext is "OneIfByLandOr" and the key is "CallMeIshmael," the first character of the key ("C") would indicate that "O" should be shifted right by 3 (to become "R"), the "n" shifted right by 1 (to become "o"), and so on. A key is "one-time" if it is used exactly once; the phrase "one-time pad" comes from the hard-copy pad of such keys used in the intelligence services. (The most secure keys are truly, uniformly random; hence the example of using readable text as the key is not the best practice.)

When done by computer, a one-time pad is typically implemented by selecting as a key a random sequence of 0s and 1s that is the same length in bits as the cleartext. To compute the i^{th} bit of the ciphertext, the encryption procedure takes the exclusive-or of the i^{th} bit of the cleartext and the i^{th} bit of the key. (The exclusive-or is 0 if both bits are 0 or both are 1, and it is 1 if one of the bits is 1 and the other is 0.) Decryption is done in precisely the same way. For example, encrypting the cleartext string "01100010" with the key "11001100" produces the ciphertext "10101110."

The power of a one-time pad arises from both the length of the key and the fact that it is discarded after one use. There are only 25 keys in a Roman alphabet shift cipher, but a one-time pad has 26^N keys for a cleartext of length N, obviously far too many to search in any reasonable amount of time, and if used only once there will be little ciphertext to analyze.

3. (5 points) What is the ciphertext produced by the one-time pad if the cleartext is "SLINGSANDARROWSOFOUTRAGEOUSFORTUNE" and the key is "XAWKYMLCLACSAPHSEKLAQQFJNRZTWIDUBO"?
4. (5 points) The one-time pad is provably secure. Why is it nonetheless unusable in most practical situations?

5. (5 points) Watermarking
   (a) is potentially an effective defense against large-scale, commercial piracy but not against small-scale, private-use copying
   (b) is less developed and less well understood technically than encryption
   (c) is typically expected to dissuade potential copyright infringers by making infringement detectable but not expected to make infringement technically infeasible
   (d) all of the above

6. (5 points) Recall that several proposed online content-distribution schemes incorporate both symmetric-key cryptography and public-key cryptography as follows. A digital work W such as a movie or book is encrypted by a commercial distributor, using a symmetric-key cryptosystem E_1, D_1, under a key d_w. The ciphertext $Z=E_1(W, d_w)$ is published. Each customer C must have a public-key, secret-key pair (PK_c, SK_c) for a public-key cryptosystem E_2, D_2. After the distributor receives payment from C, it sends $k_w=E_2(d_w, PK_c)$ to C; then C uses SK_c to recover $d_w=D_2(k_w, SK_c)$ and uses d_w to recover $W=D_1(Z, d_w)$. Given that every C has a known public-key PK_c, why doesn't the distributor just compute $E_2(W, PK_c)$ and send it to C after receiving payment?

Napster and Gnutella can be viewed as two extreme points on a spectrum of P2P architectures. In the Napster architecture, the task of *locating* content is done in a completely centralized fashion, by the server. (*Exchange* of content is then done by the clients, "peer-to-peer.") In the (original) Gnutella architecture, both location and exchange are done in a completely decentralized fashion; there are no "servers" as such. Computer scientists have also proposed various "hybrid" P2P architectures that can be viewed as intermediate points on this spectrum. For example, one could use a tree-structured hierarchy of servers that distributes the task of content location in much the same way that DNS distributes the task of IP-address look-up.

7. (5 points) True or False: Such a hybrid architecture could reduce the fragmentation and flooding problems that plagued the original Gnutella.
8. (5 points) True or False: The developer of such a hybrid system would not be vulnerable to charges of contributory and vicarious copyright infringement.
9. (5 points) Give an example of an Internet business strategy that the outcome of the Napster case makes it harder for P2P-technology providers to deploy.

Recall that Aimster started out purely as an instant-messaging based enabler of "virtual private networks." Later, it added Napster-like search capabilities so that the members of such a network could find material to exchange. After this search capability was added, the Recording Industry Association of America sued Aimster, claiming that the service violated copyright in much the same way that Napster had.

10. (5 points) Consider the potential defenses against a charge of contributory or vicarious infringement that von Lohmann discusses in his article "Peer-to-peer file sharing and copyright law after Napster.'' Give an example of one that would probably have been more effective for Aimster before it added search capabilities than it will be now that search capabilities have been added.
11. (10 points) Suppose that Aimster had not added search capabilities but had been sued for contributory or vicarious infringement anyway. Suppose further that Aimster used the defense that you suggested in your answer to question 9. If you were a copyright owner, how would you counter this defense, and how would you gather evidence?

12. (5 points) True or False: In order to be guilty of violating the DMCA, you have to be guilty of copyright infringement.

13. (10 points) The DMCA contains a "reverse-engineering exemption'' that permits circumvention of an access-control technology for the purpose of achieving interoperability of computer programs. Why is DeCSS probably not covered by this exemption?

14. (10 points) Some have suggested that, by making it a more serious crime to infringe a work that an owner has actively tried to protect than it is to infringe a work that the owner has merely asserted ownership of, the DMCA provides an incentive for owners of valuable copyright material to protect their property with effective TPSs. Why might this backfire?

15. (10 points) What is the (possibly fatal) weakness in the following argument? "The DMCA's prohibition on trafficking in circumvention tools must be unconstitutional. Content distributors could use protection technology to distribute material in such a way that it cannot be accessed for the purposes of quotation, criticism, and parody. I have a right to make these and other 'fair uses' of copyright material, and thus I have an implied right to make, sell, or buy a tool that enables me to circumvent such a distributor's TPS.''