Solutions to Homework 2

Note: These answers are longer than need be for full credit.

1. NIVYILHINNIVYNBUNCMNBYKOYMNCIH

2. Because there are only 25 possible keys, the eavesdropper can just try all of them. He will know he has the right one when decryption produces a meaningful cleartext. In this example, the key is 7, and the cleartext is NEITHERABORROWERNORALENDERBE.

3. QMFYFFMQPBUKPMAHKZGUIRMOCMSZLAXPPT

4. The security of the one-time pad depends on a new key's being generated and used for each new message that is encrypted. This means that the total number of key bits needed is too large to be practical.

5. (d)

6. In order to achieve fast, low-cost distribution, the commercial distributor wants to encrypt each work only once and wants to use a symmetric-key encryption system (because symmetric-key encryption is typically faster than public-key encryption). The key d_w is much shorter than the work W itself, and thus it is feasible for the distributor to encrypt d_w each time he receives payment from a new customer and to use a (relatively slow) public-key encryption system.

7. True

8. False

9. The following examples are given in von Lohmann's article "Peer-to-peer File Sharing and Copyright Law after Napster." Other reasonable examples will also receive full credit. (1) "Community building," via network effects, and other strategies, like advertising and strategic partnerships, that depend on the existence of online communities. (2) Data collection and businesses built on customer-profiling and datamining (unless you are willing and able to monitor and control *everything* that your customers do). (3) Bundling or, more generally, aggregation of related information products and services.

10. "Capable of substantial noninfringing uses" ("the Betamax defense")

11. As von Lohmann points out, "the Betamax defense only applies until specific information identifying infringing information has been received." Therefore, a copyright owner (or his hired surrogate) could join one of Aimster's virtual private networks and gather evidence of direct infringement (perhaps by directly participating in an infringing file exchange). Once he has this evidence, the copyright owner should deliver a "cease and desist" letter to Aimster notifying it of specific infringing activity.

12. False

13. As explained in the "Openlaw DVD/DeCSS Forum FAQ List," the Senate Committee Report on the DMCA explicitly states that the reverse-engineering exemption allows circumvention of access-control technology that controls access *to a computer program*. It also states that "works generally, such as music or audiovisual works, which may be fixed or distributed in digital form" don't qualify as "computer programs" for the purposes of this exemption. Because CSS is designed to control access to audiovisual works (*i.e.*, movies), "there is a considerable doubt as to whether… reverse-engineering CSS constitutes an attempt to achieve interoperability between computer programs."

    Note by Prof. Feigenbaum: This distinction between programs and "works" that are interpreted by media-players or, more generally, between programs and data is ***not*** *mathematically meaningful.*

14. From Appendix G of *The Digital Dilemma* (p. 312):

> Unfortunately, it is far from clear that the DMCA's anticircumvention provisions will have primarily positive effects on content distributors and other interested parties. One problem is that circumvention is a bread-and-butter work practice in the cryptology and security research and development (R&D) community, yet this is precisely the technical community that content distributors are relying on to make effective technological protection measures. If this community is hindered in its ability to develop good products, is it wise to encourage owners to use these products?
>
> It is of course possible that anticircumvention laws will be interpreted by distributors not as incentives to use effective protection measures but, rather, as incentives to do just the opposite--use insufficiently tested, possibly weak protection technology, and increase reliance on the police and the courts to punish people who hack around it. This would result in some cost shifting: Instead of owners and distributors paying for good technology to protect their property, the public at large would likely pay for a greater portion of this protection through the law-enforcement system, although some of the increased costs in enforcement may be borne by the antipiracy efforts of the various information industry associations.

15. According to most copyright lawyers, fair use, in the United States, is a "defense," not a "right." Under this interpretation, for the Fair-Use Doctrine to be relevant, the following sequence of events has to take place: a copyrighted work has to be used; the copyright owner has to sue the user for infringement; both parties have to go to court, and the user has to defend himself by saying that his actions pass the Four Factors test of the Fair-Use Doctrine. Until a specific use is made and the user is charged with infringement, "fair use" does not come into play. Thus, under this interpretation, if a copyright owner can use a TPS to prevent a specific use, no one has a "right" to make this use.