CPSC 155b: Solutions to Homework Assignment 2

1. Possible reasons includes the following. More discussion of this issue can be found in Chapter 5 and Appendix E of **The Digital Dilemma**.

   - Key management is difficult.
   - Effective public-key infrastructure is not yet fully developed and widely deployed.
   - Many governments, most notably that of the United States, place restrictions on the export of encryption-enabled products that can be difficult and costly to comply with.
   - If the digital content in question is “consumed” on ordinary, general-purpose computers, then a potential pirate who is determined enough can always program a computer to capture the content at the “rendering” stage (*e.g.*, when it displayed on the screen or played on the audio port), even if the application developer has taken great care to keep the content in encrypted form before and after this stage.

2. Possible answers include the following.

   - Special-purpose appliances are more expensive to design, manufacture, deploy, and upgrade than software applications that run on general-purpose computers.
   - Consumers can only use such appliances for one purpose and hence may be reluctant to buy them. On the other hand, consumers who have bought them may feel more locked in and reluctant to replace them.
   - Pirates have a harder job with special-purpose appliances. In particular, successful pirate devices such as cable-t.v. descramblers have to be manufactured and marketed. They cannot be distributed over the Internet and installed with a mere mouse click the way pirated software or pirated content can.
   - Sound encryption-based content management is easier to design if the designers can make use of special-purpose hardware and tamper-resistant memory.
   - US companies do not have nearly as dominant a position in the consumer-electronics industry as they do in the application-software industry.

3. (a) Application Layer
   (b) Digital Signatures
   (c) Watermarking
   (d) Cryptographic envelopes
   (e) IP layer
   (f) Encryption

4. Possible answers include:

- The number of parties involved in a B2B content business is much smaller than the number involved in a B2C content business. This makes key management (technically) easier.

** The fact that the number of parties is relatively small also means that non-technical forces discourage theft. Consider the newspaper production-staff member who receives an encrypted stock photograph over the Internet. His job is to decrypt it and use it in the print run. If he tries to resell it or improperly modifies it before using it, he runs a significant risk of damaging his employer's reputation, of damaging his employer's business relationship with one of its suppliers, and of losing his job and not being able to find another one in the newspaper production field.

- Often the content in a B2B scenario does not have mass-market appeal. This eliminates the motivation for a large number of pirates.
- The parties in a B2B scenario are more likely to be able to afford a high-quality TPS and a well-trained system-administration staff.