Homework 2

This assignment must be submitted **electronically** using the Yale Classes server by **5pm EST, Tuesday, February 18, 2003**. It covers readings and lectures through Thursday, February 13, 2003. Late homeworks will not be accepted.

Please be sure to type your name and e-mail address at the top of your homework assignment. In addition, please include your NetID and "hw2" in the name of your file, *e.g.*, `vr48-hw2.doc`. (Details about this appear in the instructions below.)

Instructions for submitting your homework are given below. Homework questions follow.

USING THE CLASSES SERVER

Note on security warnings:
When viewing the home page or syllabus for CS155 using the Classes server, your browser will automatically jump to the webpage for the course on the Zoo (http://zoo.cs.yale.edu/classes/cs155). Because this page resides on a different server, your browser may warn you that the page you are trying to view has both "secure and nonsecure items." You should respond "Yes" to displaying nonsecure items. Trust us, the CS155 page does not contain malicious code. But we don't use the Classes server to host the entire website, so be prepared to see this warning.

Log into the Classes server:
1. Access http://classes.yale.edu using your web browser.
2. Click on *Student Login* at the top of the second column.
3. Enter your NetID and Password in the appropriate text boxes and click *Login*.

For first-time users ONLY:
1. If this is the first time you have used the Classes server, you will now see a welcome page with your name. Check that the photo and e-mail options are correct, and scroll down to the course-selection area of the page.
2. Select courses you would like to add to your course list. To add CS155, select "Computer Science" from the *Subject* drop-down list, and type "155b" in the *Course Number* text box.
3. Click *Finished* at the bottom of the page when your are finished.
4. You will now see a page with several frames; the top and bottom frames allow you to navigate through the Classes server system, and the middle frame displays content. This is the first page you will see when you log into the Classes server in the future.

For other users, add CS155 to your course list:
1. Once you have successfully logged in, you will see a web page with several frames. In the top frame under the *Web Page, Syllabus, etc.* buttons, you will find a drop-down list. Click to view the contents of the list.
2. If "Computer Science 155b" appears in the list, you have added the course to your course list. Continue with directions on uploading your assignments below.
3. If not, in the bottom frame to the right of the *Logout* link, click the *Your Course List* link.
4. Scroll down the page to the *Add another course* section. Under *Subject*, choose "Computer Science" and type "155b" in the text box to the right.
5. Click *Update*.
6. The top frame should reload so that the drop-down list contains "Computer Science 155b."

Logging out of the Classes server:
Whenever you are finished using the Classes server, you should logout and close your browser window. To do this, click the red *Logout* link in the bottom frame. You will receive confirmation; then close your browser window.

To upload your assignment:
1. Type your assignment and save it in one of the following formats: Microsoft Word (.doc), Text (.txt), Rich Text (.rtf), PostScript (.ps), or Adobe Portable Document Format (.pdf). The filename must contain *no spaces*. Please include your NetID and "hw2" as part of the filename, and add the appropriate file extension if your are using a non-Windows machine, *e.g.*, `vr48-hw2.doc` for a Word document. If you have specific questions about a format or how to convert to one of these, please e-mail the TA at vijayr@cs.yale.edu.
2. Log into the Classes server as described above.
3. Select "Computer Science 155b" from the drop-down list of courses.
4. Click the blue *Upload* link in the top frame.
5. Enter the full path to your assignment in the text box, or click *Browse* and select the file you saved in the box that pops up.
6. Click the *Upload* button at the bottom of the page.
7. You should receive confirmation that your file was uploaded.

Changing your assignment:
1. If you wish to re-submit your homework before the deadline, you must change the filename of your assignment; *e.g.*, change `vr48-hw2.doc` to `vr48-hw2-2.doc`.
2. Follow the procedure above to upload the new file. The file will be marked with the date and time of submission. We will use the most recent file.

HOMEWORK QUESTIONS

1. *(10 points)* Do you think that the first-sale rule of copyright law is an appropriate mechanism in the digital realm? Briefly explain why or why not.

2. *(5 points)* In her February 6, 2003 lecture on Internet radio, Ms. Kunz observed that, since the passage of legislation aimed at digital-content distribution (*e.g.*, DMCA and HR5469), large-scale, for-profit, terrestrial broadcasters are doing more webcasting than they were before. To which business phenomenon covered earlier this semester is this analogous?

3. *(10 points)* Technically and legally, why is Kazaa harder to shut down than Napster? (Five points will be given for a correct answer about the technical aspect and five for a correct answer to the legal aspect.)

4. *(15 points)* Here is one basic Technical-Protection System for a content distributor:

i. Encrypt the content.
ii. Broadcast the content using a low-cost communication channel (*e.g.*, web page or broadcast television).
iii. Distribute the decryption key to paying customers (*e.g.*, to work with specific hardware or software that plays the content). Distribute the key on a higher-cost, lower-bandwidth channel.
iv. Users that pay for the decryption key can decrypt the broadcast and view the original content. Users that do not have the decryption key will be unable to decrypt the broadcast content.

(A diagram is provided on the following page.)
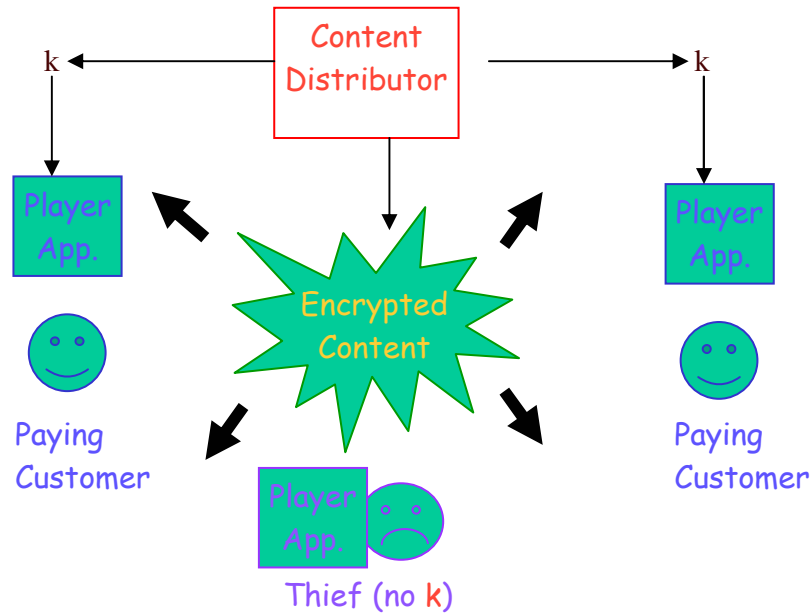
For five points each, briefly explain three technical difficulties that can arise if a content distributor uses this approach.

5. *(15 points)*

    (A) *(5 points)* HTTP, the protocol used to exchange web-page requests and web-page content, defines a sequence of steps that a client (*e.g.*, a web browser) and a server (*e.g.*, a web server) must execute to complete a web-page request. The protocol assumes that a reliable connection from the client to the server can be established. Which principles and/or protocols discussed in class make this assumption valid?

    (B) *(10 points)* In part (A), we noted that HTTP is itself not responsible for the client-server connection over the Internet; therefore, as discussed in the textbook, ordinary HTTP transmissions are vulnerable to security violations. Give two security goals that Camp discusses in the textbook. For each one, state why it might not be reached in the case of a web-page transaction (*e.g.*, viewing bank-account information), and give a possible solution to the problem.

6. *(45 points)* Recall that there are three main bodies of technique that distributors of information products use to maintain control:

    (A) Technical-Protection Services
    (B) Intellectual-Property Law
    (C) Business Models

    Hypothesis: These three approaches could be used to ensure that privacy and civil liberties are safeguarded if the Administration's Total Information Awareness program goes forward.

For 15 points each, defend or refute this hypothesis, on technical and non-technical grounds, for each of A, B, and C. You are allowed **at most** one page for each of A, B, and C.