**Reading for Lecture 5:**

1. *D is for Digital*: Chapter 10: How the Web Works, pp. 161-185. This describes web mechanisms but also includes information on cyber attacks and a section on cryptography. You should read this *before* doing the exercises below.

2. Also read: Understanding Web Site Certificates. US-CERT Security Tip (ST05-10), rev Feb 6, 2013. <https://www.us-cert.gov/ncas/tips/ST05-010> . Just one page but well written.

**Watch**:

1. Short (8.5 minute) video explaining Diffie-Hellman Key Exchange (or Key agreement):

<https://www.youtube.com/watch?v=YEBfamv-_do>

The first two minutes or so of this video are perhaps interesting history, but not too relevant. The explanation of key exchange using paint colors is great, that runs from about 2:15 to 5:00. After 5:00 the presenter explains how the paint color scheme can be implemented in mathematics. That part is also done well, and I encourage you to watch it, but don’t worry if it goes over your head. Get the concepts from the color analogy, that’s what you really need to understand.

2. Even shorter (about 2 minutes) this will introduce you to Merkle, Hellman, and Diffie.

<https://vimeo.com/23376564> as well as a very quick overview of what public key crypto is about.

**Lecture 4: Exercises**

1. Suppose I go to Turning Stone Casino and write down the sequence of results on a roulette wheel (i.e., which numbers came up). Have I written down true random numbers or pseudo random numbers?

2. Suppose I want to run a computer simulation twice to compare how well traffic flows through a network of streets using two different algorithms for controlling the stoplights. Cars will arrive at the inputs to the street network at unpredictable times, but I want the actual arrival times to be identical in both computer runs, so that the comparison of the algorithms will be fair. Do I need random or pseudorandom numbers?

3. Eventually, a pseudorandom number stream will \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

4. What is a public key certificate used for?

5. If Alice and Bob communicate using a single key and the same cryptoalgorithm, what type of cryptography are they using?

6 Public key cryptography is used today in setting up the TLS connections that display the little green lock that we all (should!) check for before entering passwords or other sensitive data over the web. But public key cryptography is only used for setting the connection up, not for encrypting the data sent over the connection. Why?

7. Suppose an attacker violates a Certificate Authority and steals the private key it uses to sign certificates. Until the theft is detected, what is the attacker able to do?

8. Where are cookies stored, and why?

9. Each browser has a different way to examine the cookies it has stored for you (I checked all of these except Internet Explorer):

**Chrome**:

Chrome: Preferences: Settings: Show Advanced Settings: Privacy: Content Settings: All Cookies and Site Data

**Firefox**:

Firefox: Preferences: Privacy: History:

- if set to “Remember History”, click “Remove individual cookies” to see a list

- if set to “Use Custom Settings for History”, click “Show Cookies” [this is the better option]

**Safari**:

Safari: Preferences: Privacy: Cookies and Website Data: click “Details” for a list

**Internet Explorer**:

Tools: Internet Options: (if menu bar hiddent, click “alt” to make it visible): General: Browsing History: Settings: and select “view objects” or “view files”

[note: I took this description from <https://kb.iu.edu/d/ajfi> but was not able to test it]

Scroll through the list of stored cookies and record:

a. Which browser did you use?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

b. What is the website for the first cookie in the list?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

c. What is the website for the last cookie in the list?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

d. About how many cookies are in the list (circle 1)

0 10 100 several hundred 1000 or more

e. Pick any cookie and look at its contents, as best you can with your browser. What can you determine about the information stored?

10. With your favorite browser, browse to [www.amazon.com](http://www.amazon.com) and look at the window displaying the URL. Now browse to canvas.lemoyne.edu and look at the window.

a. Besides the fact that the URLs are different, what else is different?

b. Discover the issuer and the expiration date of the certificate being used to secure the traffic over your connection to Canvas. The details of finding the certificate will be different depending on the browser you use, but the information should be available regardless of browser.

Certificate Authority:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Expiration Data of the Certificate:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Public Key Encryption Algorithm\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Public Key key length\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

c. Repeat the exercise for you LeMoyne e-mail account (which is provided using Gmail facilities).

Certificate Authority:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Expiration Data of the Certificate:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Public Key Encryption Algorithm\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Public Key key length\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

11. The Diffie-Hellman algorithm shown in the video is often referred to as a *key agreement* protocol rather than a *key exchange* protocol. Why?