Chapter 6 of book...
Final Exam

- Thursday, August 13 at 5 PM (time of lab)
  - Most likely in Purnell 229 (I'll let you know if this is changed)
  - Final exam is cumulative
  - Responsible for all lectures and Chapters 1-6, 10 of book
    - Focus will be on lecture/book/homework material rather than labs
If there's some homework assignments that are not completed, have until next Monday to get it into me
- Understand that there has been some confusion about HTML in homework assignments...
- Open to extensions beyond that if there is still some confusion, but need to show some progress by then
Class Project

• Discussed this on Monday
  – Check slides from lecture / assignment online for more info
  – If you would like to be sure that your presentation will run on my computer, please email me presentation a day ahead of time
    • I do have PowerPoint Viewer so PowerPoint presentations should run OK
    • Also welcome to bring in your own laptop for presentation
Labs

- Labs worth 30% of overall grade
- All labs have equal weighing
- Breakdown within labs up to TA (unless specified in lab)
- TA will send me final lab grades sometime next week
  - Any questions should be directed to TA
Previously...

- Computing devices processed data into information...
- Communications devices communicated information over distances...
  - Streams of technology developed independently
Today...

- **Digital convergence**
  - Gradual merger of computing and communications into new information environment...
  - Same information exchanged among many kinds of equipment using language of computers...
Previously...

- Why has it taken so long for computing / telecommunications to come together
  - Computers are digital, most of world is analog...
What does “digital” mean?

- Digital describes any system based on discontinuous data or events...
  - In computing, refers to communications signals or information represented in two-state (binary) way using electronic or electromagnetic signals
    - Each 0 and 1 signal represents a bit...
    - Can think of this as...
      - “all or nothing...”
      - “on or off”
      - “0 or 1”
      - “full or empty”
      - “light or dark”
      - “yes or no”
    - Clearly, there are no shades of gray in a digital representation...
What does “analog” mean...?

- Analog signal is defined as “a variable signal that is continuous in time and amplitude, as opposed to a digital or discrete signal”
  - There ARE shades of gray in a analog signal...
  - Humans generally perceive the world in analog form
  - Traditionally, electronic transmission of telephone, radio, television, and cable-TV signals is analog...
Electromagnetic Spectrum

- Electromagnetic spectrum of radiation is basis for all telecommunications signals (wired and wireless)
  - Waves vary according to wavelength/frequency
    - Frequency - number of times a wave repeats in a second
    - Longer wavelength --> lesser frequency
  - Visible light is one part of the electromagnetic spectrum
    - Sun emits most of its radiation as visible light (not a surprise if you think about it...)
Electromagnetic Spectrum

- **Radio-frequency (RF) spectrum**
  - Portion of electromagnetic spectrum that carries most communications signals
  - Spectrum is allocated internationally by International Telecommunications Union (ITU) in Geneva, Switzerland
  - Spectrum allocated within United States by Federal Communications Commission (FCC) (for non-government users) and National Telecommunications and Information Administration (NTIA) (for government users)
Wave Measurements

- **Hertz**
  - Unit of frequency
  - Expressed as number of complete wave cycles per second
  - Often expressed as kilohertz/megahertz, etc...
  - Different communications signals use different ranges of frequency
    - AM radio = 535 kHz – 1.7 Mhz
    - FM radio = 88 – 108 Mhz
    - Garage door openers = about 40 Mhz
    - Cellphones = 824-849 Mhz and 869-894 Mhz

- **Bandwidth**
  - Range/band of frequencies that a transmission medium can carry in a given period of time
  - Wider bandwidth --> more frequencies can be used to transmit data = faster transmission
Radio Transmission

- Traditionally analog (not digital) and transmitted using a carrier wave
- Performed via modulation on carrier wave – carrier wave modified in some manner according to signal
- AM vs. FM radio
  - AM – amplitude modulation; conveys information over carrier wave by adjusting amplitude (“height”) of carrier wave
  - FM – frequency modulation; conveys information over carrier wave by adjusting frequency of carrier wave
Why Change Analog Signals to Digital Ones?

- Book says that digital approximations (generated from sampling wave at given times) are only approximations of analog events
  - Accept this all the time...movies/TV shows are broken into 24/30 frames per second
  - This isn't necessarily true...
    - **Nyquist–Shannon sampling theorem**: shows that an analog signal that has been sampled can be perfectly reconstructed from the samples if the sampling rate exceeds 2*B samples per second, where B is the highest frequency in the original signal.
    - Digital signals are easier to store and manipulate electronically
    - All kinds of multimedia can be changed into digital form and transmitted as data to all kinds of devices
Analog to Digital TV

• Book says that TV signals are in analog...
  – That's no longer true in US (and many other countries)...
  – Full switch to analog to digital happened in US June 12, 2009
    • First country to make full change was Luxembourg in 2006
    • Netherlands next later in 2006
    • Finland, Andorra, Sweden, Norway and Switzerland switched in 2007
    • Belgium and Germany in 2008
    • Scheduled to happen in Canada and Japan in 2011
    • UK in 2012
    • China not till 2015
  – Video about switch to digital TV:
    http://www.youtube.com/watch?v=7w34nNux4Xw
Analog to Digital TV

- Advantages of digital TV over analog TV
  - Digital channels take up less bandwidth
    - Digital broadcasters can provide more digital channels in the same space, provide high-definition television service, or provide other non-television services such as multimedia or interactivity
  - Digital also permits special services such as multiplexing (more than one program on the same channel), electronic program guides and additional languages, spoken or subtitled
    - Sale of non-television services may provide an additional revenue source
Digital “Cliff”

- Recall how digital is “all or nothing” while analog has varying shades of gray
  - Digital cliff describes sudden loss of digital signal reception
  - Analog signal fades gradually with loss of signal strength, while digital signal is either perfect or non-existent
United States 2008 wireless spectrum auction

- Analog TV operated using frequencies between 54 MHz and 806 Mhz
- Digital TV takes less bandwidth; uses frequencies between 54-698 Mhz
  - Opened up frequencies 698-806 Mhz for other uses, such as high-speed internet
  - Portion of spectrum was auctioned off by FCC; raised 19 billion dollars
  - Big “winner” was Verizon; bought a 22 MHz bandwidth block for $4.7 billion dollars
    - Google made bid; insisted on open access of spectrum
    - Planning on using spectrum for 4g wireless network; coming in 2010
Types of Wireless Communications

- **Infrared transmissions**
  - Infrared “next” to visible light on electromagnetic spectrum
  - Wavelength greater than visible light
  - Cannot be seen, but may be felt as heat
  - Infrared ports on laptops, PDAs, digital cameras, printers, and wireless mice
  - Line-of-sight communication required; must be unobstructed view between transmitter and receiver
  - Limited to short range
  - Some uses being displaced by technologies such as bluetooth
Types of Wireless Communications

- **Microwave radio**
  - Wavelength greater than infrared
  - Frequency used to operate microwave ovens
  - Used for Bluetooth; wireless digital standard used for linking cellphones, PDAs, computers, and peripherals up to 30 feet
  - Used to transmit messages between ground-based stations and satellite communications systems
    - Must have unobstructed view between transmitter and receiver
    - Over half of telephone systems today use dish microwave transmission
    - Airwaves becoming saturated with microwave signals; future needs must use other channels (such as satellite systems)
Types of Wireless Communications

● Communications satellites
  – Microwave relay stations in orbit around the earth
  – Added to avoid some limitations of microwave earth stations
  – Transmitting signal from ground station to satellite --> uplinking
  – Transmitting from satellite to ground station --> downlinking
  – Satellite systems occupy one of three zones in space
    • Geostationary earth orbit (GEO)
      – Highest level, fewer satellites needed for global coverage
      – Delay due to distance between ground and satellite; can make two-way conversations difficult
    • Medium-earth orbit (MEO)
    • Low-earth orbit (LEO)
      – Lowest level; minimal signal delay
      – More satellites needed for global coverage
Global Positioning System (GPS)

- Global Position System (GPS)
  - Consists of 24 earth-orbiting satellites transmitting timed radio signals that can be used to identify earth locations
  - Developed by US military as military navigation system
  - Opened up to “everyone” on May 1, 2000
  - GPS receiver picks up transmissions from any four satellites and uses info from then to retrieve longitude, latitude, and altitude
    - GPS uses triangulation concept to pinpoint location
    - Accurate within 3-50 feet; 10 feet is norm
  - Used for car navigation systems, tracking vehicles, locating stolen cars, orienting hikers, aiding surveying, etc.
  - Used for “Enhanced 911” to pinpoint location of cell phone making 911 call
Another Use of GPS

- Geocaching: http://www.youtube.com/watch?v=DEOdh_j6Gmw
Networks

- **Communications network**
  - System of interconnected computers, telephones, or other communications devices that can communicate with one another and share applications and data
  - Network is primarily used to share resources such as...
    - Peripheral devices
    - Programs and data
    - Databases
Types of Networks

- **Wide Area Network (WAN)**
  - Covers a wide geographic area

- **Metropolitan area network (MAN)**
  - Covers a city/suburb

- **Local area network (LAN)**
  - Connects computers and devices in limited geographic area
  - Basis for most office networks

- **Home area network (HAN)**
  - Links household digital devices including computers, printers, storage devices, VCRs, DVDs, televisions, fax machines, video game systems, home security systems

- **Personal area network (PAN)**
  - Uses short-range wireless technology to connect an individual's personal electronics (cellphone, PDA, MP3 player, notebook PC, printer)
  - Made possible with inexpensive, short-range wireless technologies (such as Bluetooth, ultra wideband, wireless USB)
Network Structures

- **Client/Server networks**
  - Remember the CNN example...
    - Clients – microcomputers that request data
    - Servers – central computers used to supply data
      - *File server* – computer stores programs and data files shared by users on LAN
      - *Database server* – stores data but not programs
      - *Print server* – controls 1+ printers; stores print-image output from microcomputers on system
      - *Web server* – contain web pages that can be viewed using a browser
      - *Mail server* – manages email

- **Peer-to-Peer networks**
  - Peer – equal standing with another
    - All microcomputers on network communicate directly without relying on server
Network Structures – Illegal Music Downloading

- **Napster – early file-sharing site**
  - Used central server; client/server network
  - Music industry sued...shut Napster down by shutting down central server
  - Napster still around today, but not like at start...

- **Other file-sharing sites: Kazaa, Limewire, Grokster, Gnutella, and Morpheus**
  - Use peer-to-peer networks
  - Can't be easily shut down
  - Recording industry now going after individual users and colleges whose networks used for illegal downloading...
Napster

- First major service that allowed easy, cheap transfer of music files
- Started by Shawn Fanning and Sean Parker
- First released in June 1999
- Peaked with 26.4 million users in February 2001
Napster – Legal Issues

- Major recording artists such as Metallica and Madonna annoyed when songs released on Napster before “official” release
- Recording companies sued Napster for contributing to copyright infringement under US Digital Millennium Copyright Act (DMCA)
  - Court found that Napster was capable of non-infringing uses, but ordered Napster to block access to copyrighted material
  - Napster unable to do this, shut down in July 2001
  - Now available in entirely different form as pay service
  - Song: Mp3 Killed the Media Star
    http://www.youtube.com/watch?v=ZdNZYBNghnY
Internet...

• Largest network by far...
  – According to Wikipedia: “The Internet is a global system of interconnected computer networks that use the standardized Internet Protocol Suite (TCP/IP). It is a network of networks that consists of millions of private and public, academic, business, and government networks of local to global scope that are linked by copper wires, fiber-optic cables, wireless connections, and other technologies.”

• Internet vs. the World Wide Web (NOT the same thing...)
  – *Internet* – global data communications system
  – *World Wide Web* – one of services communicated via the internet
    • Collection of interconnected documents and other resources
    • Linked by hyperlinks and URL
Intranets and Extranets

**Intranet**
- Organization's internal private network that uses infrastructure and standards of internet and web
- Enables employees quicker access to internal information
- Information exchanged includes employee email addresses/telephone numbers, product information, sales data, employee benefit information, lists of jobs available within organization

**Extranet**
- Private intranets that connect internal personnel and also selected outside parties
- Ford Motor company has an extranet that connects more than 15000 Ford dealers worldwide
Security on the Internet

- Already discussed email threats and computer viruses
  - These aren't the only threats...
    - Passwords should be hard to guess
    - May want to use encryption to alter data in transit to unreadable form
Passwords

- After 9/11 attacks, debt-trading firm Cantor Fitzgerald lost 700 of 1000 employees
  - Wanted to get system up and running within two days
  - Needed to know passwords of deceased employees in order to do so
  - Surviving employees recalled what they knew about employees and were able to guess the passwords
    - Shows how it is possible to guess passwords
    - Should be careful with password choice if it's important that a particular password-protected item not be accessed by others
    - Auditors and consultants are prodding companies to require that employees pick tougher (to guess) passwords and change them more frequently as part of a requirement that companies adopt adequate “internal controls” to prevent fraud (result of 2002 Sarbanes-Oxley corporate-reform act)
Encryption

- **Encryption**
  - Process of altering readable data into unreadable form to prevent unauthorized access
    - Used to protect data in transit across a network
    - Many cases exist of data in transit being intercepted
  - **Encryption process**
    - Person A sending a message to Person B
      - Person A encrypts message into cybertext
      - Person B receives the cybertext and decrypts using an encryption key

![Encryption Diagram]

- Bob
  - Hello Alice!
  - Encrypt
  - 6EB69570 08E03CE4
  - Alice’s public key

- Alice
  - Hello Alice!
  - Decrypt
  - Alice’s private key
Forms of Encryption

- Encryption key – formula for encrypting / decrypting a coded message
  - Two basic forms of encryption are private key and public key
    - Private key – same secret key used by sender and receiver to encrypt and decrypt message
    - Public key – two keys used
      - Public key made known beforehand to sender(s) and used to encrypt the message
      - Private key only known to receiver and used to decrypt the message
      - RSA algorithm used in electronic commerce protocols uses public key encryption
Alice and Bob...

One day, Alice and Bob started dating.

After their first date, Bob sent Alice a message encrypted with his public key.

HOW AM I SUPPOSED TO DECRYPT IT IF I DON'T HAVE YOUR PRIVATE KEY?

THAT'S FOR YOU TO FIND OUT.

Bob and Alice dated for years.

...but Bob never told her what the encrypted message said.

C'MON, JUST TELL ME ALREADY.

SORRY.

GRRR...

...and every night, Alice tried to decrypt the message.

DAMN.

...until, one night, Alice made a breakthrough.

Bob was sure that by the time she cracked the message,...

--- Begin Message ---
WILL YOU MARRY ME?
--- End Message ---

EUREKA!

...he will have really meant it.
National Security Agency (NSA)

- Responsible for collection and analysis of foreign communications and foreign signals intelligence
- Responsible for protecting U.S. government communications and information systems
  - Involves using state-of-the-art encryption and “breaking” encryption of foreign intelligence
  - Has been described as world's largest employer of mathematicians
  - Existence not acknowledged for years by US government; earned nickname “No Such Agency”
  - Movie scene with NSA: [http://www.youtube.com/watch?v=fJqWHDuOpc4](http://www.youtube.com/watch?v=fJqWHDuOpc4)
Homework

- Work on project
- Catch up on any previous homework assignments that you may not have completed
  - Will accept all homeworks until next Monday
    - Open to extensions beyond that, but need to show some effort by then...