CS 100: The Internet

Chris Kauffman

Week 9-2
### Midterm Grade Breakdown

<table>
<thead>
<tr>
<th>Cut</th>
<th>Grade</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>F</td>
<td>8</td>
</tr>
<tr>
<td>70</td>
<td>C</td>
<td>4</td>
</tr>
<tr>
<td>80</td>
<td>B</td>
<td>14</td>
</tr>
<tr>
<td>90</td>
<td>A</td>
<td>17</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>43</td>
</tr>
</tbody>
</table>

Mean 83.24  
Median 88.14

### Midterm Survey

- Results posted online
- Review quickly
- Issues to address:
  - Grading
  - Difficulty
HW5: Overview

Two Parts

Problems 1-3  Practice a little encryption
Problems 4-5  Get your personal web page made and on the web

Problem 4-5

- Upload stuff to your Mason web space
- Must use some new and interesting tools
  - PuTTY on windows, Terminal on Mac, SFTP on both
- Thursday walk through some of the steps together (bring computers)
- Visit HW 5 section on uploading to mason and read
How does the Internet work?

- A lot of wires
- An older analogous system
- An interesting set of problems
Backbone Example: Sprint
The Backbone Under the Sea

Attributed to B.S.Halpern (T.Hengl; D.Groll)

Source
Python Can Read Web Stuff

The `urllib.request` package is very useful for this

```python
from urllib.request import *

url = "http://www.google.com"  # Where to connect
connection = urlopen(url)      # connect to google
bytes = connection.read()      # read whole page
text = bytes.decode("UTF-8")   # decode to text
print(text)                    # print

url = "http://www.cs.gmu.edu/~kauffman/jazz-albums.txt"
# Merge several steps
jazz = urlopen(url).read().decode("UTF-8")
print(jazz)
```
A Puzzle: Secure Internet Communication

- Encryption schemes like Caesar, Vigenere, and DES are based on shared secrets
- Same secret key to encrypt and decrypt a message
- Have you ever ordered something from Apple or Amazon?
- Sent your credit card number to them?
- Have you ever told them your secret key?
- Does this seem like a problem?
- How does one communicate securely with someone else on the internet?
An Answer

**Lock Boxes**: One secret thing (key), One public thing (lock)

- **Public Key Encryption**: seems magical, just number theory
- Also known as **asymmetric encryption**
- **RSA**: First and most prevalent public key method
Exercise: Quick Review

- What is a good analogy for how the internet works?
- Why are encryption techniques like Caesar Cipher not so good for internet commerce?
- What kind of encryption technique is good for internet commerce?
Ping!

- ping: command to check speed of packet delivery
- Available on Windows cmd.exe and Mac Terminal
- Just type `ping google.com` or `ping mason.gmu.edu`

```
lila [ckauffm2-hw2] % ping google.com
PING google.com (74.125.228.100) 56(84) bytes of data.
64 bytes from iad23s08-in-f4.1e100.net (74.125.228.100): icmp_seq=1 ttl=51 time=3.83 ms
64 bytes from iad23s08-in-f4.1e100.net (74.125.228.100): icmp_seq=2 ttl=51 time=4.13 ms
64 bytes from iad23s08-in-f4.1e100.net (74.125.228.100): icmp_seq=3 ttl=51 time=3.80 ms
```

- Wait what? I wanted Google, not
  iad23s08-in-f8.1e100.net
- Oh, I see how it is
Tracing The Trip

tracert (windows) or traceroute (mac/unix)

- Shows the path packets take through the network

lila [ckauffm2-hw2] % traceroute google.com
traceroute to google.com (74.125.228.104), 30 hops max, 60 byte packets
  1  129.174.120.1 (129.174.120.1) 0.402 ms 0.459 ms 0.504 ms
  2  * * *
  3  129.174.255.205 (129.174.255.205) 0.890 ms 0.877 ms 0.915 ms
... 12 above-google.iad10.us.above.net (64.125.12.82) 4.098 ms 3.987 ms 4.079 ms
  13  209.85.252.80 (209.85.252.80) 10.021 ms 10.010 ms 4.064 ms
  15  iad23s08-in-f8.1e100.net (74.125.228.104) 3.697 ms 3.687 ms 3.988 ms

Who Lives at that Address?

- The American Registry for Internet Numbers
- Allows one to look up who owns an IP address
- Let’s look up who is between us and Google
Goal: Get some Text on the Internet

- Download Sublime Text Editor if you haven’t
- Write a short text file like
  More online text to clog the tubes up.
- Save the file as test.txt
- Use SFTP to upload the file to mason.gmu.edu
  - Putty for Windows
  - Termina/sftp for Mac
Putting Stuff on the Internet

You can put stuff on the internet
▶ Not on Facebook, Twitter, Tumblr, Flickr, etc
▶ On your own personal web page
▶ For HW 5, will need to do just that
▶ Instructions here

Goals Today

▶ Download Sublime 2 Text Editor
▶ Download SFTP software (if needed)
▶ Create a simple text file
▶ Put it on the Mason Web Server for all the Internet to see
Creating Text File

- Open Sublime Text Editor
- Describe in a 2-3 sentences how the internet works
- Save this file to an easy location (desktop or CS 100 folder)
- Name it how-the-internet-works.txt
General process to put stuff on the web

1. Have an account on a server: mason.gmu.edu (all of you do)
2. Know your username and password on server: NetID and pass for GMU
3. Log into the server using a secure FTP connection
   - Mac OS X: Terminal + sftp command
   - Windows: Download Putty and install, use PSFT (putty home)
4. Issue commands to set up a web directory on the server
5. Create files on your local computer
6. Transfer files from your local computer to the web folder on the server

More detailed explanations are on HW 5 specification
Text files are great, such as this one:
http://mason.gmu.edu/~ckauffm2/jazz-albums.txt
But most of us prefer HTML:
http://mason.gmu.edu/~ckauffm2/index.html