Tips and Tricks for HW8

● Your UCSC account should look something like this:
  - Some files...
  - Other files...
  - public_html/
    - index.html
    - DEMO1/
      - index.html
      - demo1.pde
      - processing.js
    - DEMO2/
      - index.html
      - demo2.pde
      - processing.js
• Make a webpage demo
  – FileZilla for SFTP
    • sftp.ic.ucsc.edu
    • people.ucsc.edu/~nwhitehe
  – TextWrangler for editing
Secrets and Encryption
If you could only speak in numbers, how would you send a message to your friend?

Get into pairs with one person playing red and the other playing blue. Make sure you are both clear on who is red and who is blue.

If you cannot find a pair, double up in an existing pair (e.g. two reds and one blue).
Devise Your Encoding

• Spend a couple minutes agreeing on a system for communicating using numbers
  – Must work for any message with A-Z letters
  – Must not take a very long time to encode and decode
  – You can write down notes
For *REDS* eyes only

- All *BLUEs* close your eyes
  - No cheating!
For REDS eyes only

- DO NOT SAY THE MESSAGE!!!
- DO NOT SAY LETTERS AS YOU ENCODE!!!
- The secret message is:
  - "I LOVE PEAS"
- Write the secret message down
- Start encoding it
  - Don't let your partner see it!
For **BLUES** eyes only

- All *REDS* close your eyes
  - No cheating!
For **BLUES** eyes only

- DO NOT SAY THE MESSAGE!!!
- DO NOT SAY LETTERS AS YOU ENCODE!!!
- The secret message is:
  - "I LOVE CATS"
- Write the secret message down
- Start encoding it
  - Don't let your partner see it
• Finish encoding your secret message
  – Recopy to blank paper if needed
• Exchange secret messages with your partner
  – Don't give them the original message...

• Once you have an encoded message, decode it
  – *Don't say it out loud!*
What was the message?

What was the secret message from your partner?

<table>
<thead>
<tr>
<th>Blue</th>
<th>Red</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. SQUEAMISH</td>
<td>OSSIFRAGE</td>
</tr>
<tr>
<td>B. SUPER BOWL</td>
<td>A BIG BANANA</td>
</tr>
<tr>
<td>C. TO BE OR NOT</td>
<td>GOOD QUESTION</td>
</tr>
<tr>
<td>D. I LOVE PEAS</td>
<td>I LOVE CATS</td>
</tr>
<tr>
<td>E. TOO MANY</td>
<td>SECRETS</td>
</tr>
</tbody>
</table>
Think of your favorite TV show. Encode the name using your encoding scheme.

Once you are done, exchange encoded messages with your partner and begin decoding.

Don't say messages out loud!
A. My partner chose a good TV show and correctly encoded the name
B. My partner chose a good TV show but made some mistakes in the encoding
C. My partner chose a terrible TV show but correctly encoded the name
D. My partner chose a terrible TV show and even made some mistakes in the encoding
E. I was unable to decode my partner's message
Intercepted Messages

• Grab an encoded message from a nearby group
  – Yes, steal their message!
• Try to decode it as a group
A. We successfully decoded our target's message and they chose a good TV show
B. We successfully decoded our target's message and they have terrible taste
C. We were unable to decode the message but we have a good guess for what it was
D. We were unable to decode the message and have no clue what it was
Keyed Encoding

- **Unencoded**
  - 1=A 2=B 3=C 4=D ... 26=Z

- **Keyed**
  - 1=S 2=E 3=C 4=R 5=I 6=T 7=K 8=Y ... 26=P

- **Notes:**
  - You must use every letter exactly once
  - Write out tables both ways
    - number → letter
    - letter → number
Encode a message

- Both of you share same secret tables
- Think of your favorite location/place
- Encode your favorite place using tables
- Make your message in the form:
  - 'THE BEST PLACE IS …'
- When done, exchange with partner
  - Decode their favorite place
  - When you think you know it, verify it with your partner by showing your paper
  - DON'T SAY MESSAGES OUT LOUD!
A. My partner correctly encoded a location and I decoded it.
B. My partner made some mistakes in the encoding.
C. I made some mistakes in the decoding.
D. The message was successfully decoded but made no sense.
E. I was unable to decode my partner's message.
Intercepted Messages (2)

• Grab a keyed encoded message from a nearby group
  – Yes, steal their message!
• Try to decode it as a group
Success/Failure?

- Were you able to crack their code?
- What information do you know?
  - How does it help you?
Untrusted Transmission

- 4 volunteers
  - Alice
  - Bob
  - Carol/Charlie
  - Mallet/Mallory

- 'Alice wants to send a message to Bob'
  - Carol/Charlie is a normal participant
  - Mallet/Mallory is a malicious participant
• Alice and Bob get together ahead of time, both get a copy of key (sparkly)

• Protocol
  – Alice locks with sparkly key
  – Sends locked package across untrusted network
  – Bob gets locked package
  – Bob unlocks with sparkly key
Why is it secure?

• Why is this protocol secure?
  
  A. Only Alice and Bob have copies of the key that opens the message
  B. There is only one key that opens the message
  C. The working key is transmitted along with the message
  D. Mallet/Mallory never touches the message
No Key Exchange

- If Alice and Bob had to get together to exchange keys, why not just hand off the package then?
- What if they just met online?
Double Lock Protocol

- Protocol:
  - Alice locks with sparkly key lock *(singly locked)*
  - Alice sends to Bob
  - Bob locks with teal key lock *(double locked)*
  - Bob sends back to Alice
  - Alice unlocks sparkly key lock *(singly locked)*
  - Alice sends back to Bob
  - Bob unlocks teal key lock *(unlocked)*
Why is it secure?

What makes the double-lock protocol secure against tampering by Mallet/Mallory?

A. The attacker never touches the message
B. The attacker only has one key that they can unlock
C. The attacker only has possession of the message when it is locked with at least one lock
D. The attacker only has possession of the message when it is locked with one lock
Not actually a secure protocol!

• This protocol is better than nothing
  – But it is not secure
• Why is it not secure?
  – How can Mallet/Mallory trick Alice?
Man-in-the-Middle

- Man-in-the-middle attack
  - Mallet/Mallory pretends to be Bob
  - Can do anything Bob could do
  - No way to distinguish Bob and malicious parties
What was the flaw in the scrambled alphabet table code you used last time?

A. The sender and receiver both knew the key
B. The same letter always went to the same number
C. The start of the original message was known
D. B & C
E. There was no flaw
Enigma

- http://www.youtube.com/watch?v=G2_Q9FoD-oQ
Public Key Encryption

• A way for anyone to send a secret message to Alice/Bob

• Only Alice/Bob can open the message once it's locked

• How would you do it with locks and keys?
• Public directory of open locks
  – Choose the lock for Alice, click it on your message
  – Now only Alice can unlock
  – Just need to trust directory names are correct

• Alice sends a message to Bob
  – Alice finds Bob's public lock from the directory
  – Alice clicks lock on her message
  – Alice sends locked message to Bob
  – Bob unlocks, gets message

• This is *public key encryption*
A message to Bob says, 'I love you, do you love me? From Alice'

- How could Mallet/Mallory fool Bob?
- How can you fix it?
Public Key Signatures

• Public directory of keys
  – Anyone can grab a key from the directory for a given name (public keys)
  – Only the named person has a special lock that matches the key
    • Lock requires special private key to close
    • Lock opens with public key

• To sign a message:
  – Alice writes message, puts in box
  – Alice locks her secret lock onto box using private key
  – Anyone can now unlock message with Alice's public key
  – Verifies that message was locked by Alice
  – But only Alice can lock using her private key
• Shared key encryption
  - Turn messages into data that only makes sense if the recipient has the key
  - Sender and receiver use same key to scramble/unscramble the message

• Public key encryption
  - Everyone has public/private keys
  - Encrypt with public key of recipient to send them a message (only they can decrypt message)
  - Sign messages with private key (anyone can verify the signature with public key)

• Designing good protocols is tricky!
  - Lots of ways to trick people (man-in-the-middle example)
What good is a digital signature?

A. Only the owner of the private key can sign messages that verify with the matching public key

B. Anyone can sign messages using the public key, only the owner of the private key can read them

C. Only the owner of the public key can sign messages that verify with the matching private key

D. Digital signatures can't be copied
Crypto Currencies
Bitcoins are like hats...

- http://www.youtube.com/watch?v=E_9R45RLNR0
What are Bitcoins?

- https://docs.google.com/presentation/d/1f4k32ZNzNbxxGxROX5o-Jn1x3htzYDL3UMhmfe4965E/present#slide=id.gfa7bd1c0_00

Introduction to Bitcoin
How does it work?

- Based on public/private keys
  - encryption, digital signatures
- Users request to send money to another address
  - sign request
  - post request, everyone else sees it, verify it is ok
  - once >50% of network sees it, it goes through
  - everyone keeps track of every transaction
    - verify digital signatures
    - check for double spending
    - check that sender actually has the money
    - pseudo-nonymous digital records
Stealing Bitcoins

• How could you steal someone's bitcoins?
  A. Copy files off their computer (their keys)
  B. Promise to send them something if they give you bitcoins (and never send it)
  C. Hack into their online bank
  D. Steal their physical wallet (containing keys printed on paper)
  E. All of the above
Mt. Gox

- One guy's website
  - Intended for Magic the Gathering card dealing
Largest Exchange in Trouble


Bitcoin exchange Mt. Gox goes dark in blow to virtual currency

BY RAIRIDH VILLAR, SOPHIE KNIGHT AND BRETT WOLF
TOKYO/ST LOUIS Tue Feb 25, 2014 8:47pm EST

106 COMMENTS | Tweet 480 | Share 123 | Share this 8+1 99 | Email | Print
Silk Road


- frosty@frosty in his digital footprint
Alternative Crypto Currencies

Major

**Bitcoin (BTC)**
- [http://bitcoin.org/](http://bitcoin.org/)
- **blocks every 10 min**
- **coin supply** 21 million coins will be available
- **difficulty adjustment** 2016 blocks
- **hashing algorithm** SHA256d
- **Initial Reward** 50 coins per block
- **Market Cap:** $144,000,000 (Jan 5th, 2013)
- **Launch Date:** January 3rd, 2009

**Namecoin (NMC)**
- [https://en.bitcoin.it/wiki/Namecoin](https://en.bitcoin.it/wiki/Namecoin)
- (merged mined with BTC)
- [https://github.com/vincecd/namecoin](https://github.com/vincecd/namecoin)
- [http://namecoin.info/](http://namecoin.info/)
- **blocks every 10 min**
- **coin supply** 21 million coins will be available
- **difficulty adjustment** 2016 blocks
- **hashing algorithm** SHA256d
- **Initial Reward** 50 coins per block
- **Market Cap:** ??? BTC
- **Launch Date:** April 18, 2011

**Litecoin (LTC)**
- [http://litecoin.org/](http://litecoin.org/)
- **blocks every 2.5 min**
- **coin supply** 84 million coins will be available
- **difficulty adjustment** 2016 blocks
- **hashing algorithm** scrypt
- **Initial Reward** 50 coins per block
- **Market Cap:** 150,000 BTC
- **Launch Date:** October 2011

**Dogecoin (Dogec)**
- **blocks every 1 min**
- **coin supply** 99 Billion coins will be available and 5 Billion added every year.
- **hashing algorithm** scrypt
- **Initial Reward** 1,000,000 - 3 (Random) coins per block
Dogecoin

- http://dogecoin.com/

dogecoin is an open source peer-to-peer cryptocurrency, favored by Shiba Inus worldwide.

START USING DOGECOIN TODAY:
Dogecoin

- http://www.youtube.com/watch?v=3wL1xNHq90k
Dogecoin

- Just a joke, right???
  - Actually most used cryptocurrency (# transactions)
  - One of largest currencies by implied market cap
  - Fastest adopted currency... ever
  - Paper bills, strong crypto, good parameters...
Paper Wallets

• You can print your own money!
• Don't let anyone see the private key
  – Snooper can steal present and future balances
  – Do you trust...
    • Your OS
    • Your printer
    • Your printer driver
    • Your roommates with Google Glass
Web Search Quiz!
"The search tools that help us find needles in the digital haystack have become the lenses through which we view the digital landscape. Businesses and governments use them to distort our picture of reality."

A. True

B. False
Google responds efficiently to queries by going out and searching the web in real-time.

A. True

B. False
• Which steps happen in the background?
  A. Gather information & Keep copies
  B. Gather information & Keep copies & Build an index
  C. Understand the query
  D. Determine relevance of each result & Determine ranking of results
• Google indexes what percentage of web pages?
A. 100% Almost everything
B. About 50% on average but some days 30% and some days 100%
C. Less than 5%
D. Best estimates are 30%
• How often do pages get indexed?

A. Every page is indexed every day

B. It depends on the page, some pages like whitehouse.gov are indexed many times a day, others rarely

C. Google watches how often pages change

D. B & C

E. None of the above
• Web pages typically represent the present but could be a few days out of date.

A. True

B. False
Dole Kemp 96 Web Site Enter Here

The Dole Kemp 96 Web Site is Presented for Educational Purposes by 4President.org

The Clinton Gore 96 Web Site is Archived Here
Web search is free and democratic. Every web page has an equal chance of being indexed and coming out the top of the list.

A. True

B. False
How are search results funded? Who pays?

A. Users pay a subscription fee
B. Web sites pay to be indexed
C. The government pays using taxes
D. Advertisers pay to place ads next to results.
E. B & D
• Why is search so attractive to advertisers?

A. Advertisements can be targeted more precisely using your digital footprint.

B. Advertisers only pay when you click on their ad.

C. Millions of people use search every day.

D. All of the above
End