Computer Security: Problem

- **The Problem: Billions in Losses**
  - Outright theft
  - Online scams
  - Viruses / Worms
    - Actual damage
    - Actions to avoid damage
  - Denial of Service
  - Etc.

- **Possible Traps (Public Systems !!!)**
  - Trojan Horse
  - Onlooker
  - Cameras
Computer Security: Defenses

- **Passwords**
  - Using Secure Passwords
  - Keeping them Secure

- **Encryption**
  - Simple (Classical Encryption – Pre-Computer)
  - Strong (Modern – Computer Based)

- **Good Practices**
  - Like all fields, doing something stupid ...

- **Tradeoffs**
  - Is the cure worse than the disease?

- **Long Live Common Sense!**
Good Passwords and Cracking

- Briefcase (style) Combination Locks
  - Brute force methods: Try all combinations
    1. Number of wheels
    2. Number of position per wheel
    3. Time per trial
    4. How long does it take?

- Contrast to BRUTE brute force method (Always Consider!)

- Password on a computer
  - + More possibilities per “wheel”
  - + More “wheels” (often up to user)
  - - Computer based cracking faster!
  - - Dictionary attacks

- Picking a good UNIX password
Classical Encryption

- When passwords fail, encryption can be fallback
  - Also provides extra level of difficulty
- Security vs. Privacy
- Many levels of encryption sophistication:
  - Go through some of them
- Single Alphabetic Substitution
  - Caesar: L FDPH, L VDZ, L FRQTXHUH
  - Magic decoder ring?
  - Cryptoquote
- Cracking single alphabetic substitution
  - Character frequency -- ETAONIRSH
  - (Length of text)
# Classical Encryption: Single Alphabet

IFOJ LKFJN DCE LNPNC XNDJL DVF

FOJ IDMRNJL UJFOVRM IFJMR FC

MRSL KFCMSCNCM, D CNQ CDMSFC,

KFCKNSPNE SC BSUNJMX, DCE

ENESKDMNE MF MRN GJFGFLSMSFC

MRDM DBB ANC DJN KJNDMNE NHODB.

-- D BSCKFBC

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1</td>
<td>H</td>
<td>1</td>
<td>O</td>
</tr>
<tr>
<td>B</td>
<td>6</td>
<td>I</td>
<td>3</td>
<td>P</td>
</tr>
<tr>
<td>C</td>
<td>16</td>
<td>J</td>
<td>11</td>
<td>Q</td>
</tr>
<tr>
<td>D</td>
<td>14</td>
<td>K</td>
<td>7</td>
<td>R</td>
</tr>
<tr>
<td>E</td>
<td>7</td>
<td>L</td>
<td>6</td>
<td>S</td>
</tr>
<tr>
<td>F</td>
<td>15</td>
<td>M</td>
<td>15</td>
<td>T</td>
</tr>
<tr>
<td>G</td>
<td>2</td>
<td>N</td>
<td>18</td>
<td>U</td>
</tr>
</tbody>
</table>
Classical Encryption

- Polyalphabetic Substitution
  - The Vignere Cypher
  - The Babbit Solution
    - How many alphabets used?
      - digraph frequency “th”
    - Several Single-Alphabet problems

- Cypher Reuse!
  - Bigger pool of data
  - Patterns become obvious

- One Time Pads
  - Can be Absolutely Secure
  - Computers and Random Number Generators ?!
Classical Encryption

- The Key Exchange Problem
  - Threats
  - Using your “secure” channel
  - A padlock analogy
  - Diffie, Hellman, and Merkle solution