Announcements

● Final Exam scheduled for Monday December 12, 2011 (8:30AM-11:30AM)

● Lab 5 late deadline has been extended to 11:59pm today, Good luck!
Agenda

- Review Cryptography
- Review TCP, Congestion Control
- Review Practice Final (Time Permitting)
- Questions?
- Final Remarks
Symmetric Encryption

- The crucial point is that there is a **shared** private key
  - Must be known to both parties, and **only** known by two parties

- Why?

- Because it's **symmetric**
K is important

- Different types of security guarantees
  - information theoretic
  - computational

- A completely random key provides us with information theoretic security ($p(M|C)$ is uniform)

- A shorter pseudo random key leads to computational security ($p(M|C)$ may be 0 for all $M$ except one)
  - But we rely on it being a lot of work to guess and check

- Why not completely random?
  - Because it requires $|K| = |M|$, impractical to share
Stream Ciphers

- Generate pseudo-random stream of bits from short key
- Encrypt/decrypt by XORing with stream as if one-time pad
- But NOT one-time PAD! (People who claim so are frauds!)
- In practice, many stream ciphers uses have run into problems
Block Ciphers

- Used in PGP (secure email), SSL (securing TCP), as well as IPsec

- Message to be encrypted processed in blocks of k bits
  - One-to-one mapping from clear-text to cipher block
  - Generalizes to $2^k!$ possible mappings for given k, resulting in cryptographic security

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>110</td>
</tr>
<tr>
<td>001</td>
<td>111</td>
</tr>
<tr>
<td>010</td>
<td>101</td>
</tr>
<tr>
<td>011</td>
<td>100</td>
</tr>
<tr>
<td>100</td>
<td>011</td>
</tr>
<tr>
<td>101</td>
<td>010</td>
</tr>
<tr>
<td>110</td>
<td>000</td>
</tr>
<tr>
<td>111</td>
<td>001</td>
</tr>
</tbody>
</table>

Plaintext: 010110001111

Encrypted text: 101000111001

Input Blocks: 010, 110, 001, 111

Output Blocks: 101, 000, 111, 001
Block Ciphers (contd)

- How to we resolve the fact that if block is repeated in plaintext, ciphertext will be repeated? (secrecy compromised)

- Cipher-Block chaining!
Integrity

- Message Authentication Codes (abbreviated as MAC, distinct from media access control, i.e., link layer)
- Alice and Bob have a shared secret key/authentication key
Integrity (contd.)

• We require a **cryptographic** hash function, H
  ○ One for which it is **computationally infeasible** to find any two different messages \(x\) and \(y\) such that \(H(x) = H(y)\)

• How do we distribute the shared authentication key?
  ○ Public key cryptography (e.g., RSA)
TCP Congestion Control
Practice Final

● Questions?

● **Disclaimer:** Please note that the practice final is meant as a preparation tool to help you think about different material presented during the quarter. It is not necessarily an indication of the exact coverage of materials or length of actual final exam.
Questions?
Final Remarks

● It's three hours (3>1.25)

● You already have 5/100 if you attended Jon Peterson's guest lecture!

● You already know what it looks like (very similar in format to the midterm)
  ○ A mix of short answers, some multiple choice, some true/false

● Questions are not necessarily in order of difficulty

● Congratulations on making it to the end! You have learned a very valuable set of networking principles and implementation experience that will serve you well!