Admin:
- Midterm test (in class)
- Th Feb 28
- Assignment 1 (Due Today)
- Due Feb 14 (two weeks)
- Assignment 2
- Mar 14 (double check)
- Assignment 3
- April 4 (double check)
- Scribe Notes: Jason Kemp

Block Cipher:
$C = E_{k}(m)$
$M = D_{k}(c)$

Psuedo-Random Permutations

Does Not Happen

Can Encrypt any Message ($2^b$)

Cant Decrypt

Block Cipher is deterministic

Every C is possible

AES:

AES 128 (128 bit key, 192/256 are also defined)

Video Clip
http://www.youtube.com/watch?v=mlzxpkdXP58
Modes Of Operation

ECB: (electronic code book)
1) Lets you encrypt messages longer than a block
2) Improve security

<table>
<thead>
<tr>
<th>Encryption</th>
<th>IV</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>$M_1$</td>
<td>$K$</td>
<td>$C$</td>
</tr>
<tr>
<td>$M_2$</td>
<td>$K$</td>
<td>$C$</td>
</tr>
<tr>
<td>$M_3$</td>
<td>$K$</td>
<td>$C$</td>
</tr>
</tbody>
</table>

Zero Padding

Initialization Vector
- Random, |IV| = |m| = |c|
- Random with each encryption
- Generate it after the message to be encrypted is supplied

Decrypt
- Reversible, with IV

Counter Mode (CIR/CM)

PRP, (PRP, PRP++, ... <= PRG)

Security Definition:

<table>
<thead>
<tr>
<th>Security</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stream Cipher</td>
<td>Lowest</td>
</tr>
<tr>
<td>Block Cipher + ECB</td>
<td>Lowest</td>
</tr>
<tr>
<td>Block + CBC</td>
<td>Medium</td>
</tr>
<tr>
<td>Block + CTR</td>
<td>Medium</td>
</tr>
<tr>
<td>Block with MAC (future lecture)</td>
<td>Highest</td>
</tr>
</tbody>
</table>

One time Security:
Background
- Given c, can you find m? (should not be possible)
- Given c, can you find k? (should not be possible)
- Given c, some info about m, can you find k? (should not be possible)
- Given c, m, find k, then decrypt future c's? (should not be possible)
  * in one time, future encryptions will be different
Security Game:
- (one time Security)
- Participants
  - Adversary
  - Oracle (black box encryption function
    □ Has a key, but can’t recover it
    □ Can supply inputs and get outputs
    □ “lunchtime attacks” (feed in plaintext, and receive ciphertext)

1) Adversary chooses any two messages: m₀, m₁
2) Give (m₀, m₁) to oracle (oracle has chosen a key previously)
3) Oracle flips a coin b ← {0, 1}
   i. Encrypts mᵦ: cᵦ = Enc(k)(mᵦ)
4) Oracle gives the adversary cᵦ
5) Adversary guesses value of b

Naively guess: Pr[Correct] = 1/2
Adv = |1/2 - Pr[Correct]|
- No advantage
A crypto system is secure if any adversary’s advantage is negligible (really small, 1/poly(L))
Negl(L) ≪ 1/poly(L)