HOMEWORK V

DUE: In RH 227, by 2PM, Thursday, May 3, 2012

READ:
- Presentation slides by Prof. Torsten Suel
- Presentation slides by Prof. Stuart Steele
- Presentation slides by Prof. Ramesh Karri
- Presentation slides by Prof. Helen Li

ASSIGNMENT: There are four questions

Solve all homework and exam problems as shown in class and sample solutions

1) Four students, Anna (A), Bill (B), Clara (C), and Dan (D), have each created a homepage, and each homepage contains links to some of the other students. In particular, Anna has a hyperlink to Bill, Clara, and Dan. Bill has a hyperlink to Anna and Dan, Clara has a hyperlink to Dan and Bill, and Dan has a hyperlink to Anna and to himself.

   a) Draw the graph of 4 nodes.

   b) Using the Pagerank approach on this graph of 4 nodes, write down the system of 4 equations for the significance of each page, that is, the equations defining $s(A)$, $s(B)$, $s(C)$, $s(D)$. Whose page do you think will have the highest significance value? Why?

   c) Suppose Dan removes the link to himself. Do you think this will increase or decrease his page's significance?

2) The following are requirements for a system. Are they good valid requirements:

   1) Software shall utilize a tree structure for storage requirements. Explain.

   2) The Ariane 5 Situation, while identified as a software problem, was really a system issue. True or False.

3) Consider the following simple hardware security (crypto) module:
**Step 1:** XOR input plain text with a 4-bit key

**Step 2:** Apply the substitution function

<table>
<thead>
<tr>
<th>Input (decimal)</th>
<th>Output (decimal)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

**Step 3:** Consider a permutation module as shown below

- Input bit 0 connected to output bit 2
- Input bit 1 is connected to output bit 3
- Input bit 2 connected to output bit 0
- Input bit 3 connected to output bit 1

Given plaintext of 0011 and secret key of 0000, the cipher text generated is 0110.

**Homework Question:** Design the decryption module

**Step 1:** Inverse permutation

- Input bit 2 connected to output bit 0
- Input bit 3 is connected to output bit 1
- Input bit 0 connected to output bit 2
- Input bit 1 connected to output bit 3

**Step 2:** Inverse substitution function

<table>
<thead>
<tr>
<th>Input (decimal)</th>
<th>Output (decimal)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

**Step 3:** Exclusive or with secret key

Design the decryption module using logic gates! In addition, start with cipher text 0110 and use key 0000 to see if you get plain text 0011.

4) Consider the NAND3 gate illustrated in the presentation.

Explain its operation by using a truth table and referring to the examples in the presentation.