Test 2. Due 05/11/06 9:00pm

This test is take home. It must be your own individual work. You may, however, consult your textbooks and notes. Any other form of acquiring help, such as discussing exam problems with others and consulting other textbooks or web sites, is a clear violation of the honor code. Note that providing information to others that leads to solutions is also a violation of the honor code.

Show your work and justify all your answers. You will be graded not only on the correctness of your answer, but also on the clarity you express it. Be neat and be concise. Points will be deducted from any irrelevant answer and wrong answer. Thus, if you don’t understand the problem, the chances of losing points would increase if you write more. For example, if your solution contains one part that is a correct answer to the problem, one part that is irrelevant, and one part that is wrong, then you may still end up with 0 point for your answer, depending on how bad your irrelevant part and the wrong part are. This policy is to discourage you from writing sloppy answers.

You are required to do just four problems of your own choice. You will earn extra points if you do all five problems.

Submit your test using the following command on Mercury:

submit wang 561test2 <your test>

<table>
<thead>
<tr>
<th>Problem</th>
<th>Points</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>125</td>
<td></td>
</tr>
</tbody>
</table>

I have abided by the Academic Honor Code on this test.

Name: ___________________________ Signature: ___________________________ Date: ___________________________

Dr. J. Wang
1. (25 points) Someone chose $e = 2$ as the public key in RSA. Is it safe? Justify your answer.

2. (25 points) Alice used DSS to sign documents, but her random number $k_A$ was stolen, what could happen? Justify your answer.

3. (25 points) Why is $\text{Auth}_{C,TGS}$ needed in Step 3 in Kerberos? Justify your answer.

4. (25 points) Figure 1 shows a screen-subnet firewall system, where its DMZ contains three servers. IP address of each device is shown in the figure. Construct ACL rules so that clients from outside can get access to the servers in DMZ, but not to any device inside the Intranet and the inside router.

![Screened-subnet firewall system](image)

**Figure 1.** Screened-subnet firewall system.

5. Someone constructed a program $D$ that takes a program $P$ as input and claimed that it can check whether $P$ contains viruses: If yes, $D(P)$ outputs TRUE; otherwise, outputs FALSE. The subroutine `infect-executable` in the following program first scans memory, seeking an executable file, and then duplicates itself to that file. Can $D(P)$ return TRUE? Justify your answer.

   1. program $P := \{$
   2. \hspace{1em} ... \hspace{1em}$
   3. \hspace{1em} main-program := \{ \hspace{1em}$
   4. \hspace{2em} if $D(P)$ then goto next; \hspace{2em}$
   5. \hspace{2em} else infect-executable; \hspace{2em}$
   6. \hspace{1em} } \hspace{1em}$
   7. \hspace{1em} next: ... \hspace{1em}$
   8. \hspace{1em} } \hspace{1em}$

Dr. J. Wang  
Test 2