

Homework #1  
ISA 666 Internet Security Protocols Spring 2007

This homework is due on 02/19 by 4:30 PM. This assignment is to be done by each student individually.

- Submit your solutions in either MS Word or in PDF format. Submit your solutions to the TA at [gmuisa666@gmail.com](mailto:gmuisa666@gmail.com) with “ISA 666 HW#1” as the subject in your email. You will also need to submit a hard copy on the day the assignment is due.
- Make sure to include your name and G-number at the beginning of your homework submission.

1. Textbook Homework 2.3 (5 points)
2. Textbook Homework 3.7 (5 points)
3. Are all the 56 bits of the DES key used an equal number of times in the  $K_i$ ? If NO, state how many are unused throughout the 16 rounds. If YES, explain why that’s the case. (10 points)
4. Textbook Homework 4.5 (10 points)
5. Decode the following cipher-text, and write a detailed explanation of the process you went through to get the plaintext. If you ended up writing a program, submit it with your solution. (70 points)

```
P S E W O   T D P S U   I I M A W   E W Q I I   T U I I M
W E U I I   M E Q I W   J T W E U   I I M E Q   I E P S A
S J D
```