Arab Academy for Science, Technology, and Maritime Transport

College of Computing and Information Technology

IS703 Information Systems Security

Spring 2012

Homework 2 (Total of 50 pts)
Due on Wednesday April 25th 2012

Please send through email a softcopy of your homework (Always keep a copy of the homework you hand in). Page numbers and problem numbers refer to the 4th edition of the course textbook.

Q1. **(10 pts)** Solve problem 3.9 from the textbook.

Q2. **(10 pts)** In your own words, describe a possible attack on *double DES* which makes it not recommended as a DES replacement.

Q3. **(10 pts)** Solve problem 6.6 on page 196 from the textbook.

Q4. (10 pts) In your own words, and referring to Ch5 in the textbook, summarize how AES works while comparing it to DES. Your summary should not exceed 4 pages.

Q5. **(10 pts)** Solve problem 7.3 on page 228 from the textbook.