Arab Academy for Science, Technology, and Maritime Transport

College of Computing and Information Technology

IS703 Information Systems Security

CS716 Data Security

Spring 2014

Homework 2 (Total of 60 pts)
Due in class on Tuesday May 20th 2014

Please provide a softcopy of your homework (Always keep a copy of the homework you hand in). Page numbers refer to the 5th edition of the course textbook.

Q1. **(10 pts)** Solve problem 3.8 from the textbook.

Q2. **(5 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 review questions 6.4 and 6.5 on page 215 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 14.1 on page 441 from the textbook.

Q6. (5 pts) Solve problem 9.2 (parts *d* and *e*) from the textbook (page 282).

Q7. (10 pts) In your own words, summarize *The Security of RSA* subsection starting on page 285 in your textbook.