

# Arab Academy for Science, Technology, and Maritime Transport

## College of Computing and Information Technology

### IS703 Information Systems Security

### CS716 Data Security

Spring 2013

#### Homework 3 (Total of 40 pts) Due on Sunday May 12<sup>th</sup> 2013

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

**Q1. (5 pts)** Solve problem 9.2 (parts *d* and *e*) from the textbook (page 282).

**Q2. (10 pts)** In your own words, summarize *The Security of RSA* subsection starting on page 285 in your textbook.

**Q3. (5 pts)** Solve problem 10.1 from the textbook (page 324).

**Q4. (5 pts)** Solve problem 10.2 from the textbook (page 324).

**Q5. (15 pts)** We covered in class the *Diffie-Hellman key exchange* for two parties. Research the *Diffie-Hellman key exchange for more than two-parties*. Provide a summary of your findings (possible extensions you can find), detailing one such extension in your own words. Include in you report any references you consult.