Optional Study Problems #2

CMSC/Math 456
Instructor: Daniel Gottesman

These problems from the textbook Katz & Lindell will help you study for the final and understand the class topics better. They are not necessarily representative of problems you might see on the test. These problems are for material from the second half of the class. See the earlier mid-term practice problems file for problems from the first half of the class.

The problems are ungraded and completely optional. Do only the ones that you feel will help you the most. Do not turn them in. I have classified them in two sets: A modest number of "recommended problems" for each topic, and some additional "honorable mentions" of problems I feel are also helpful in case you feel you need more practice. The total number of problems listed here is quite large. Focus on the ones for which you feel the least confident about the material.

These problems are from the 3rd edition of the book. If you have an older edition, I am not sure if all the problem numbers will match.

General: Here is an exercise you can do: Come up with one or two problems that you think would be appropriate mid-term questions. Give them to your friends to solve, and have them do the same.

RSA

- Recommended Problems: 12.15, 12.16, 12.20
- Honorable Mention: 12.17

Message Authentication Codes and CCA Security:

- Recommended Problems: 4.1, 4.6, 4.15, 5.3, 5.9
- Honorable Mention: 4.4, 4.5, 5.4, 5.7, 5.8

Hash Functions:

- Recommended Problems: 6.6, 6.12
- Honorable Mention: 6.11, 6.13, 6.14, 6.15

Digital Signatures, Certificate Authorities, and TLS:

- Recommended Problems: 13.2, 13.5, 13.9
- Honorable Mention: 13.4, 13.8