

CSE 651 Homework 5

Due: Wednesday, May 12 by class time (10:30 am)

Midterm Exam II: Monday, May 17

Scope: Public-key cryptography and RSA, including the math used in RSA.

Open book, open notes

1. Do Problem 9.16 of Stallings. (You may use the algorithm in Fig 9.7/9.8 or the algorithm Square-and-Multiply in class notes. They describe the same algorithm.)
2. Do b and e of Problem 9.2 of Stallings. (Your answer must include the values of n , $\varphi(n)$, d .)
3. Do Problem 9.3 of Stallings. (Do not use the brute-force method.)
4. Do Problem 9.4 of Stallings.
5. Do Problem 9.6 of Stallings.
6. Do Problem 9.8 of Stallings.