

## **CSE 651 Homework 5**

Due: Monday, May 11 by class time

### **Midterm Exam II: Friday, May 15**

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

**Closed book, closed notes**

**Calculators needed**

1. Do Problem 9.16 on page 284 of Stallings. (You may use the algorithm in Fig 9.7 or the algorithm Square-and-Multiply in class notes. They describe the same algorithm.)
2. Do b and e of Problem 9.2 on page 282 of Stallings. (Your answer must include the values of  $n$ ,  $\varphi(n)$ ,  $d$ .)
3. Do Problem 9.3 on page 282 of Stallings. Also, answer the same question with  $C = 15$ ,  $e = 5$ ,  $n = 39595$ . (Do not use the brute-force method. Hint: The question would be harder if, for instance,  $C = 11$ .)
4. Do Problem 9.4 on page 282 of Stallings.
5. Do Problem 9.6 on page 282 of Stallings.
6. Do Problem 9.8 on page 282 of Stallings.