

CMSC 456: Homework 2, Fall 2005

Due at the **beginning** of class on **September 23, 2005**.

Some of the problems require thought - do not wait until the last day to start working on them! If you cannot come up with complete solutions, write down your partial solutions clearly. All sections, page numbers etc. below refer to the class textbook, *Introduction to Cryptography with Coding Theory*, **Second Edition**.

This homework is longer than usual, since the number-theoretic fundamentals studied here are very important for this course.

1. Problem 1 in Section 4.9, pages 146-147 of the textbook. **(15 points)**
2. Problem 2 in Section 3.13, page 104 of the textbook. **(10 points)**
3. Problem 5 in Section 3.13, page 104 of the textbook. **(10 points)**
4. Problem 8 in Section 3.13, page 105 of the textbook. **(5 points)**
5. Problem 11 in Section 3.13, page 105 of the textbook. **(5 points)**
6. Problem 12 in Section 3.13, page 105 of the textbook. **(5 points)**
7. Problem 26 in Section 3.13, page 108 of the textbook. **(5 points)**
8. **(For graduate students only.)** Problem 28 in Section 3.13, page 109 of the textbook. **(15 points)**