CS355: Cryptography **Fall 2005**

Homework #1

Due date & time: 10:30am on September 9, 2005. Hand in at the beginning of class (preferred), or email to the TA (wangq@purdue.edu) by the due time.

Late Policy: You have three extra days in total for all your homeworks. Any portion of a day used counts as one day; that is, you have to use integer number of late days each time. If you emailed your homework to the TA by 10:30am the day after it is due, then you have used one extra day. If you exhaust your three late days, any late homework won't be graded.

Additional Instructions: (1) The textbook is **Second Edition** of *Introduction to Cryptography with Coding Theory* by Trappe and Washington. (2) The submitted homework must be typed. Using Latex is recommended, but not required. (3) You must write out the intermediate steps of your computation. Just giving the final answer will get little partial credit.

Problem 1 (5 pts) Exercise 1 in Section 3.13 of the textbook.

Problem 2 (10 pts) Exercise 3 in Section 3.13 of the textbook.

Problem 3 (5 pts) Exercise 4 in Section 3.13 of the textbook.

Problem 4 (15 pts) Exercise 6 in Section 3.13 of the textbook. You must give justification for your answer.

Problem 5 (5 pts) Exercise 8 in Section 3.13 of the textbook.

Problem 6 (10 pts) Exercise 10 in Section 3.13 of the textbook.

Problem 7 (10 pts) Exercise 4 in Section 2.13 of the textbook.

Problem 8 (5 pts) Exercise 7 in Section 2.13 of the textbook.

Problem 9 (10 pts) Use the problem description in Exercise 11 in Section 2.13 of the textbook, answer the following questions.

- **a.** Calculate the index of coincidence of the language in the problem.
- **b.** Calculate the exact value of the index of coincidence of the ciphertext ("ABCDBABBBAC").
- **c.** Determine the most probable key, and argue that why it is the most probably key.

Problem 10 (5 pts) Exercise 23 in Section 2.13 of the textbook.

Problem 11 (5 pts) Show that if $\gcd(a, b) = 1$ and $a|n$ and $b|n$, then $ab|n$.

Problem 12 (15 pts) For positive integer n, let $\mathcal{D}(n)$ denote the set of positive divisors of n. For two positive integers n_1, n_2 such that $\gcd(n_1, n_2) = 1$, show that $\mathcal{D}(n_1) \times \mathcal{D}(n_2)$ is in one-to-one correspondence with $\mathcal{D}(n_1 \cdot n_2)$, via the map that sends the element (d_1, d_2) in $\mathcal{D}(n_1) \times \mathcal{D}(n_2)$ to the number $d_1 \cdot d_2$. That is, you need to show that the map is a bijection from $\mathcal{D}(n_1) \times \mathcal{D}(n_2)$ to $\mathcal{D}(n_1 \cdot n_2)$.

Optional Problem (0 pt) (a) Roughly how long did you spent on this homework? (b) Among the topics that have been covered in the class, which one or ones (if any) you have found to be most difficult?