CS555: Cryptography **Spring 2012**

Homework #3

Due date & time: 10:30am on February 28, 2012. Hand in at the beginning of class (preferred), or email to the TA (jiang97@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 was due, then you have used one extra day. If you exhaust your three late days, any late homework won't be graded.

Additional Instructions: The submitted homework must be typed. Using Latex is recommended, but not required.

Problem 1 (9 pts) For a finite abelian group, one can completely specify the group by writing down the group operation table.

- (4 pts) (a) Write down group operation tables for the following finite abelian groups: $(\mathbb{Z}_5, +)$, $(\mathbb{Z}_5^*, \times)$
- (2 pts) (b) Show that the group operation table for every finite abelian group is a Latin square; that is, each element of the group appears exactly once in each row and column.
- (3 pts) (c) Below is an addition table for an abelian group that consists of the elements $\{a, b, c, d\}$; however, some entries are missing. Fill in the missing entries.

+	a	b	c	d
a	a			
b	b	a		
c			a	
d				

Hint: Use part (b) above. Try to determine the identity element first. Use the fact that if $ab = ac$, then $b = c$.

Problem 2 (5 pts) Let $G := \{x \in \mathbb{R} : x > 1\}$, and define $a \star b := ab - a - b + 2$ for all $a, b \in \mathbb{R}$. Show that:

- (a) G is closed under $\star$;
- (b) the set G under the operation $\star$ forms an abelian group.

Problem 3 (5 pts) Solve the following using the Chinese Remainder Theorem:

$$\begin{cases} x = 4 & \mod 5 \\ x = 3 & \mod 7 \\ x = 2 & \mod 11 \end{cases}$$

Write out the intermediate steps.

Problem 4 (6 pts) (Katz and Lindell. Page 294. Exercise 7.1)

Problem 5 (5 pts) (Katz and Lindell. Page 294. Exercise 7.5)

Problem 6 (5 pts) (Katz and Lindell. Page 294. Exercise 7.8)

Problem 7 (5 pts) (Katz and Lindell. Page 190. Exercise 5.4.)

Problem 8 (5 pts) (Katz and Lindell. Page 190. Exercise 5.5.)

Problem 9 (10 pts) (Katz and Lindell. Page 190. Exercise 5.12.)

Problem 10 (10 pts) (Katz and Lindell. Page 108. Exercise 3.16.)

Problem 11 (15 pts) (Katz and Lindell. Page 108. Exercise 3.20.)

Problem 12 (10 pts) (Katz and Lindell. Page 109. Exercise 3.21.)

Problem 13 (10 pts) (Katz and Lindell. Page 109. Exercise 3.22.)