CS555: Cryptography **Spring 2012**

Homework #5

Due date & time: 10:30am on April 5, 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 (10 pts) (a) Describe the NMAC construction and the HMAC construction. (b) Explain in your own words why NMAC offers secure MAC. (c) In what aspect does HMAC differ from NMAC?

Problem 2 (8 pts) (Katz and Lindell. Page 158. Exercise 4.17.)

Problem 3 (8 pts) (a) Give a CPA-secure encryption scheme and a secure MAC scheme such that when using them to instantiate the Encryption and Authenticate construction, the resulting construction is **secure**. (b) Give a CPA-secure encryption scheme and a secure MAC scheme such that when using them to instantiate the Encryption and Authenticate construction, the resulting construction is **insecure**.

Problem 4 (8 pts) Repeat the previous problem for the Authenticate-then-Encrypt construction.

Problem 5 (8 pts) (Katz and Lindell. Page 237. Exercise 6.2.) **Hint.** Given a one-way function g, you need to construct a function f such that $\forall n\, f(0^n) = 0^n$ and prove that f is one-way.

Problem 6 (8 pts) (Katz and Lindell. Page 238. Exercise 6.4.)

Problem 7 (10 pts) (Katz and Lindell. Page 296. Exercise 7.21.)

Problem 8 (5 pts) (Katz and Lindell. Page 295. Exercise 7.15.) **Hint.** Show that if there exists an algorithm that can solve DLG, then there exists an algorithm that can solve CDH.

Problem 9 (5 pts) (Katz and Lindell. Page 295. Exercise 7.16.)

Problem 10 (10 pts) (Katz and Lindell. Page 295. Exercise 7.18.) **Hint.** The problem given in 7.18 is not hard. Find an algorithm to compute $g^{1/x} \mod p$.

Problem 11 (10 pts) (Katz and Lindell. Page 231. Exercise 9.2.)

Problem 12 (10 pts) (Katz and Lindell. Page 231. Exercise 9.3.)