**CS355: Cryptography** **Fall 2005**

# Homework #5

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

This is the last homework for this course. There are 150 points worth of problems. You are strongly encouraged to start early.

The Late Policy and Additional Instructions for HW1 still apply.

*Discrete Log and El Gamal Encryption*

**Problem 1 (5 pts)** Exercise 6 in Section 7.6 of the textbook. (Page 215)

> **Hint:** The notation $L_2(3) = 69$ means that $2^{69} \equiv 3 (\mathrm{mod}\ 101)$. You may use the results in Exercise 5 without proving them.

**Problem 2 (5 pts)** Exercise 7 in Section 7.6 of the textbook. (Page 215)

**Problem 3 (10 pts)** Exercise 10 in Section 7.6 of the textbook. (Page 216)

**Problem 4 (5 pts)** Exercise 11 in Section 7.6 of the textbook. (Page 216)

*Hash Functions and Message Authentication Code*

**Problem 5 (10 pts)** Exercise 1 in Section 8.8 of the textbook. (Page 239)

> **Hint:** Consider which of the three security properties can be attacked.

**Problem 6 (10 pts)** Let $h$ be a hash function defined as follows. For any message $m$, divides it into blocks of 160 bites $M = M_1||M_2||\cdots||M_\ell$; then $h(M) = M_1 \oplus M_2 \oplus \cdots \oplus M_\ell$, where $\oplus$ denotes bit-by-bit XOR. Is $h$ one-way? Is $h$ strongly collision resistant? Why or why not?

**Problem 7 (10 pts)** Suppose that $f : \{0,1\}^n \rightarrow \{0,1\}^n$ is a one-way bijection. Define a compression function $h : \{0,1\}^{2n} \rightarrow \{0,1\}^n$ as follows. Given $x \in \{0,1\}^{2n}$, write $x = x_1||x_2$, where $x_1, x_2 \in \{0,1\}^n$. The define $h(x) = f(x' \oplus x'')$. Prove that $h$ is *not* second preimage resistant.

**Problem 8 (10 pts)** Let $h : \{0,1\}^* \rightarrow \{0,1\}^m$ be a hash function constructed by iterating a collision resistant compression function using the iterative construction. Show that defining $MAC_k(M) = h(k||M)$ results in an insecure MAC. That is, show that given a valid text/MAC pair $(M, H)$ one can efficiently construct another valid text/MAC pair $(M', H')$ without knowing the key $k$.

More on the back. Turn Over.

*Digital Signatures*

**Problem 9 (5 pts)** Exercise 1 in Section 9.6 of the textbook. (Page 252)

**Problem 10 (15 pts)** Exercise 4 in Section 9.6 of the textbook. (Page 253)

**Problem 11 (10 pts)** Exercise 6 in Section 9.6 of the textbook. (Page 253)

**Problem 12 (10 pts)** Assume that Alice signs two messages using El Gamal, and for both messages she uses the same $k$. Show how an attacker can totally break the signature scheme (recover the signing key), without solving an instance of the Discrete Log Problem.

*Zero Knowledge Proofs*

**Problem 13 (15 pts)** Exercise 2 in Section 14.3 of the textbook. (Page 321–322)

Do part (a) and part (b). Do not do part (c); instead, explain why is this protocol Zero Knowledge?

**Problem 14 (15 pts)** Exercise 5 in Section 14.3 of the textbook. (Page 323–324)

In addition to finishing the protocol, also explain why is this protocol a proof of knowledge, and why is this protocol Zero Knowledge.

**Problem 15 (15 pts)** Exercise 6 in Section 14.3 of the textbook. (Page 324)