CS555: Cryptography **Spring 2012**

Homework #4

Due date & time: 10:30am on March 22, 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 (6 pts) Let $(\mathbb{G}, \cdot)$ be a finite group, and $g \in G$. Show that $\langle g \rangle$ is a subgroup of $\mathbb{G}$. Here $\langle g \rangle$ denote the set $\{g, g^2, g^3, \cdots\}$.

Problem 2 (6 pts) Prove that if a finite group of order t has at least one generator g, i.e., the group can be written as $\{g, g^2, \cdots, g^t\}$, then the group has exactly $\phi(t)$ generators, where ϕ is Euler's totient function.

Hint: Prove that g^j is a generator if and only if $\gcd(j, t) = 1$.

Problem 3 (6 pts) Find all sub-groups of the group $(Z_{15}, +)$. Find all sub-groups of the group $(Z^*_{15}, \times)$.

Hint: A sub-group must have the closure property. Thus if a subgroup contains an element g, it must contain $\langle g \rangle$.

Problem 4 (6 pts) (Katz and Lindell. Page 294. Exercise 7.10.)

Hint. The Chinese Remainder Theorem says that if $x \equiv c (\mathrm{mod} \;\; p)$ and $x \equiv y (\mathrm{mod} \;\; q)$, then $x \equiv y (\mathrm{mod} \;\; pq)$. The result proven in Exercise 7.8 may also be helpful.

Problem 5 (6 pts) (Katz and Lindell. Page 295. Exercise 7.13.)

Problem 6 (10 pts) Merkle hash trees.

Merkle suggested a parallelizable method for constructing hash functions out of compression functions. Let f be a compression function that takes two 512 bit blocks and outputs one 512 bit block. To hash a message x one uses the following tree construction. The message is first divided into N blocks, then starting from the beginning, apply f to every pair of adjacent blocks, resulting in $\lceil N/2 \rceil$ blocks. Repeat until one gets one block a, then apply f to $a||$msg-len and get the hash value.

For example, suppose the message has 3100 bits; it thus has 7 blocks, with the last block padded with 484 0's. Let the 7 blocks be $x_0, x_1, \cdots, x_6$. One first compute $c_0 = f(x_0, x_1)$, $c_1 = f(x_2, x_3)$, $c_2 = f(x_4, x_5)$, $c_3 = x_6$. One then compute $b_0 = f(c_0, c_1)$, $b_1 = f(c_2, c_3)$. One then compute $a_0 = f(b_0, b_1)$. The hash value of the message x is $f(a_0, \text{msg-len})$, where msg-len is the binary representation of 3100, padded with 0's.

Prove that if one can find a collision for the resulting hash function then one can find collisions for the compression function.

Hint: The proof is similar to that of the Merkle-Damgard construction.

Problem 7 (15 pts) Constructing hash functions from block ciphers.

Consider the Davies and Price construction of a hash function from a block cipher $\mathcal{E}$. A message x is divided into fixed-size blocks $x_1, x_2, \cdots, x_k$.

$$H_0 = \text{Initial Vector}$$
$$H_i = \mathcal{E}_{x_i}[H_{i-1}] \oplus H_{i-1} \text{ for } 1 \leq i \leq k$$
$$H_k \text{ is the hash value.}$$

We use $h_y(x)$ to denote the hash value of message x when using y as the initial vector. For example, given two message blocks x_1, x_2, then

$$h_y(x_1) = \mathcal{E}_{x_1}[y] \oplus y$$
$$h_y(x_1||x_2) = h_{h_y(x_1)}(x_2) = \mathcal{E}_{x_2}[h_y(x_1)] \oplus h_y(x_1).$$

In this problem, we assume that AES with 128 bit keys is used as $\mathcal{E}$. Therefore, each message block has 128 bits and the initial vector and the hash value have 128 bits.

a. (5 pts) Describe an algorithm that runs in time $O(2^{128}$ and can generates an initial vector y and an infinite sequence of messages $x^1, x^2, x^3, \cdots$ such that $h_y(x^1) = h_y(x^2) = h_y(x^3) = \cdots$.
Hint: find a message block x_1 and a block y such that $h_y(x_1) = y$.

b. (10 pts) Describe a variation of the above attack with expected running time $O(2^{64})$ to attack the hash function when the initial vector value is fixed to a value y_0. The attack algorithm, when given y_0, finds an infinite sequence of messages $x^1, x^2, x^3, \cdots$ such that $h_{y_0}(x^1) = h_{y_0}(x^2) = h_{y_0}(x^3) = \cdots$.
Hint: find two message blocks x_1 and x_2 and a block y such that $h_{y_0}(x_1) = y = h_y(x_2)$.

Problem 8 (15 pts) (Katz and Lindell. Page 155. Exercise 4.4.)

Problem 9 (10 pts) (Katz and Lindell. Page 155. Exercise 4.6.) Here we are asking whether when Construction 4.3 is still a secure fixed-length MAC when one uses a weak PRF. If your answer is yes, give a proof sketch. If your answer is no, give a counter example; that is, you give a weak PRF, and then given an algorithm that can perform forgery.

Problem 10 (10 pts) (Katz and Lindell. Page 155. Exercise 4.9.)

Problem 11 (10 pts) (Katz and Lindell. Page 157. Exercise 4.12.) If your answer is yes, prove it. If your answer is no, give a counter example.