

---

## Problem Set 4

This problem set is due on *Wednesday, April 16, 2008* by 8AM. You must submit your homework to your edlab CS591d course directory. Make sure that your homework files have proper permissions set such that the course staff can read the files, but not other students. Do not make any modifications to your homework files after the due date, unless you notify the TA that you are using a late pass. You may write your solution in any program (Word, L<sup>A</sup>T<sub>E</sub>X, etc.), but you must convert your document to PDF for submission. We will accept only PDFs. Please contact the TA well ahead of the deadline if you have a question about these procedures.

This is an individual problem set. See Handout 1 (*Course Information*) for our policy on collaboration and late penalties. Mark the top of each page with your name, cs591d, the problem set number and question, and the date. Each solution must begin on a new page. Points may be deducted if your TA has problems understanding your solution. In mathematical problems, **show all your work**.

Each team member should turn in the individual problem on his or her own. For the group problems, have your team submit a *single solution*.

### Problem 4-1. Hash functions and MACs [5 pts]

*This is an individual problem.* As customary, if you receive any key insights from someone else or some other resource, you must cite that person or resource. State the names of people you consulted and the knowledge you learned from each.

#### (a) Number theoretic hash functions

Consider a function  $G$  defined as  $G(x) = g^{h(x)} \bmod p$ , where  $p$  is a large prime,  $g$  is a generator modulo  $p$ , and  $h$  is a hash function that is CR and PIR. For the purposes of this exercise, let us assume that the size of the output of  $h$  is at least twice as small the size of  $p$ . Is  $G$  PIR? Is  $G$  2PIR? Make sure to prove your answers rigorously. Is  $G$  a good hash function? Explain.

#### (b) MAC-then-Encrypt or Encrypt-then-MAC

This problem should illustrate an example of the failure of MAC-then-Encrypt authentication schemes against chosen plaintext attacks (Please see Krawczyk's *The Order of Encryption and Authentication For Protecting Communications* for a formal treatment). Consider a scheme where in order to obtain confidentiality and authentication a user first breaks his/her message  $m$  into a sequence of blocks  $m_1||m_2||\dots||m_l$  (each of the same size  $n$ ) and then attaches a MAC that is a hash of the  $\oplus$  (exclusive-or) of all the blocks of the message. The size of the output of the hash function is also  $n$ . The resulting sequence of blocks (together with the MAC attached to the end of  $m$ ) is encrypted via a symmetric block cipher in CBC mode using a randomly generated initial vector which becomes the first block of the ciphertext  $c = IV||c_1||c_2||\dots||c_l$ . For this exercise let us assume access to a *strong* cryptographic hash function. The recipient of the message must first decrypt the message and then check that the hash of the  $\oplus$  of all the blocks of the message (without the very last block) is equal to the decryption of the very last block of the ciphertext. The secret key is known only to the sender and the recipient. Design a chosen plaintext attack in which an adversary can request from the sender no more than a polynomial (in  $n$ ) number of plaintext queries in order

to obtain their encryption. An attack is successful when a new ciphertext is produced, distinct from all that were once requested from the sender, that is accepted as authentic by the recipient. Now, do the same for a scheme where the MAC is simply  $\oplus$  of all the blocks of the message (no hash functions involved).

Hint: it is helpful to start by drawing a diagram of all the processes involved in MAC formation, encryption, decryption, and authentication.

#### Problem 4-2. DoppelB(1)ock Cipher [5 pts]

*This is an individual problem.* As customary, if you receive any key insights from someone else or some other resource, you must cite that person or resource. State the names of people you consulted and the knowledge you learned from each.

A German company is attempting to make an extra strong block cipher. The company decided that composing block cipher encryption multiple times in their DoppelBock Cipher product might increase security, so they first try running a conventional block cipher encryption algorithm E twice

$$c = E_{k_1}(E_{k_2}(m))$$

with  $n$ -bit keys  $k_1$  and  $k_2$ . Thus, the total key size is  $2n$  bits. Unfortunately, a highly paid consultant explained that the new cipher is not much more secure than the original algorithm E under a chosen plaintext attack.

(a) Show how to break this scheme using a chosen plaintext attack that requires  $O(2^n)$  memory and  $O(2^n)$  encryptions/decryptions using AES.

(b) Not to give up easily, the company fired back with Mark II of the DoppelBock Cipher.

$$c = \text{AES}_{k_1}(\text{AES}_{k_2}^{-1}(\text{AES}_{k_1}(m)))$$

where  $\text{AES}_k$  means AES encryption under key  $k$  and  $\text{AES}_k^{-1}$  means AES decryption under key  $k$ .

Describe a chosen plaintext attack on this two-key version of DoppelBock when  $n = 128$ , requiring roughly  $2^{128}$  steps and storage of  $2^{128}$  encryptions under single AES encryptions.