CO 487/687: Assignment #3 Due date: March 1 (Wednesday)

NOTE: Crowdmark links for Assignment #3 will be emailed to you before 11:00 am on February 17. If you do not receive the link, please send an email to ajmeneze@uwaterloo.ca.

1. **Hash functions** (5+5 marks)

   (a) Let $G : \{0,1\}^{2n} \to \{0,1\}^n$ and $H : \{0,1\}^{2n} \to \{0,1\}^n$ be two hash functions. Define the function $F : \{0,1\}^{2n} \to \{0,1\}^n$ by $F(x) = H(G(x), G(x))$. (Here, the comma "," denotes concatenation.) Prove that if G and H are collision resistant, then F is also collision resistant.

   (b) Suppose that $f : \{0,1\}^{n+r} \to \{0,1\}^n$ is a compression function that is preimage resistant. Define $H : \{0,1\}^{2(n+r)} \to \{0,1\}^n$ as follows. Given $x \in \{0,1\}^{2(n+r)}$, write

   $$x = x_L \| x_R \quad \text{where} \quad x_L, x_R \in \{0,1\}^{n+r}.$$

   Then define

   $$H(x) = f(x_L \oplus x_R).$$

   Prove that H is not 2nd preimage resistant.

2. **MAC schemes** (10 marks)
   Consider the following MAC scheme for authenticating fixed-length messages from $\{0,1\}^{256}$. For each i, $1 \le i \le 128$, let S_i be a fixed subset of $\{1, 2, 3, \ldots, 255, 256\}$. The key space is $\{0,1\}^{128}$. To authenticate a message m with key k, one first forms the 128-bit string $b = b_1 b_2 \cdots b_{128}$ where b_i is the sum modulo 2 of the bits of m indexed by the elements of S_i, and then AES-encrypts b with key k. The resulting ciphertext c is the tag on m.
   Show how a passive adversary who is given a single valid message/tag pair can easily produce new valid message/tag pairs. (Note: By a "passive" adversary we mean one who does not have access to a MACing oracle.)
   (Hint: Describe the MAC generation algorithm using matrix multiplication over the integers modulo 2.)

3. **MAC schemes derived from block ciphers** (10 marks)
   Let E denote the family of encryption functions for a block cipher where plaintext blocks, ciphertext blocks, and keys are each 128 bits in length. Let $H : \{0,1\}^* \to \{0,1\}^{128}$ be a hash function. Assume that plaintext messages m all have bitlengths that are multiples of 128; we write $m = (m_1, m_2, \ldots, m_t)$, where each m_i is an 128-bit block and t is the length of m in blocks.
   Consider the following four MAC schemes each with 128-bit secret key k.

   (i) $\text{MAC}_k(m) = c_t$, where $c_0 = 0$, and $c_i = c_{i-1} \oplus m_i \oplus E_k(m_i)$ for $1 \le i \le t$.

   (ii) The sender selects $c_0 \in_R \{0,1\}^{128}$ and computes $\text{MAC}_k(c_0, m) = c_t$, where $c_1 = E_k(c_0 \oplus m_1)$, and $c_i = c_{i-1} \oplus E_k(m_{i-1} \oplus m_i)$ for $2 \le i \le t$. The sender transmits (m, c_0, c_t). The receiver recomputes $\text{MAC}_k(c_0, m)$ and compares it with c_t.

   (iii) $\text{MAC}_k(m) = E_k(H(m))$.

   (iv) The sender selects $c_0 \in_R \{0,1\}^{128}$ and computes $\text{MAC}_k(c_0, m) = h$, where $c_i = E_k(m_i \oplus c_{i-1})$ for $1 \le i \le t$ and $h = H(c_t)$. The sender transmits (m, c_0, h). The receiver recomputes $\text{MAC}_k(c_0, m)$ and compares it with h.

Are any of these MAC schemes secure? (Justify your answer.)
(It will help to review the definition of a secure MAC scheme.)

4. **Algorithm analysis** (10 marks)
   Describe an efficient algorithm which, on input $n \in \mathbb{N}$, determines whether n has an integer cube root; that is, your algorithm should determine if there exists an integer $a \in \mathbb{N}$ such that $n = a^3$. ($\mathbb{N}$ is the set of natural numbers.) Using big-O notation, give an upper bound on the number of bit operations your algorithm takes.

5. **RSA computations** (5 marks)
   Alice chooses $n = 1271$ and $e = 131$ for use in the basic RSA public-key encryption scheme.

   (a) Find Alice's private key d.

   (b) Encrypt the message $m = 3$ for Alice. (Use the repeated-square-and-multiply algorithm to perform the modular exponentiation.)

   (Please do not use Maple for this problem, except possibly to do the modular multiplications. The purpose of this exercise is to make sure that you understand how to perform the basic RSA operations. Please show the main steps in your calculations.)

You should make an effort to solve all the problems on your own. You are also welcome to collaborate on assignments with other students presently enrolled in CO 487. However, *solutions must be written up by yourself.* If you do collaborate, please *acknowledge your collaborators* in the write-up for each problem. *If you obtain a solution with help from a book, research paper, a web site, or elsewhere, please acknowledge your source.* You are *not* permitted to solicit help from online bulletin boards, chat groups, newsgroups, or solutions from previous offerings of the course.

The assignment should be submitted via Crowdmark before 11:00 am on March 1. Late assignments will not be accepted except in *very* special circumstances (usually a documented illness of a serious nature). High workloads because of midterms and assignments in other courses will *not* qualify as a special circumstance.

Office hours:
Alfred Menezes (MC 5026): Monday 3:00-5:00 pm, Friday 1:00-3:00pm
Ted Eaton (MC 5481): Tuesday 10:30-11:30 am
Gabriel Gauthier-Shalom (MC 5113): Thursday 3:00-4:00 pm
Philip Lafrance (MC 5497): Tuesday 12:30-1:30 pm
Christopher Leonardi (MC 5494): Tuesday 2:00-3:00 pm
Cathy Wang (MC 6313): Thursday 2:00-3:00 pm