CO 487/687: Assignment #4 Due date: March 22 (Wednesday)

NOTE: Crowdmark links for Assignment #4 will be emailed to you before 11:00 am on March 10. If you do not receive the link, please send an email to ajmeneze@uwaterloo.ca.

1. **Estimating the security level of RSA** (10 marks)
   Recall that the *Number Field Sieve* algorithm for factoring RSA moduli n has running time

   $$O(e^{(1.923+o(1))(\log_e n)^{1/3}(\log_e \log_e n)^{2/3}}) \text{ bit operations.}$$

   This running time expression can be simplified to

   $$e^{1.923(\log_e n)^{1/3}(\log_e \log_e n)^{2/3}} \text{ bit operations}$$

   by ignoring the $o(1)$ term in the exponent and the hidden constant in the $O(\cdot)$ expression.

   (a) Using the simplified running time, estimate the security level of RSA when used with a 1024-bit modulus, a 2048-bit modulus, and a 3072-bit modulus. (Recall that a "security level" of k bits means that the running time of the fastest attack known for solving a computational problem or breaking a cryptographic scheme has running time approximately 2^k.)

   (b) Suppose that a new integer factorization algorithm is discovered with running time

   $$e^{1.923(\log_e n)^{1/4}(\log_e \log_e n)^{3/4}} \text{ bit operations.}$$

   Estimate the security level of RSA with a 1024-bit modulus, a 2048-bit modulus, and a 3072-bit modulus.

   (c) In light of the new integer factorization algorithm in (b), what should the bitlength of n be in order to achieve a 128-bit security level?

2. **RSA signatures** (10 marks)
   Consider the variant of the basic RSA signature scheme in which no hash function is used. That is, to sign a message m, where $0 \leq m \leq n-1$, Alice computes $s = m^d \bmod n$ and sends (m, s) to Bob. (Here, (n, e) is Alice's RSA public key, and d is Alice's RSA private key.) To verify, Bob computes $m' = s^e \bmod n$ and checks that $m' = m$.

   (a) Show that this signature scheme is existentially forgeable under a key-only attack.

   (b) Show that this signature scheme can be *totally broken* under a chosen-message attack. In this attack, the adversary is given an arbitrary message $m \in [0, n-1]$ and a signing oracle. The adversary's can obtain the signature of any messages of its choosing from the oracle except for m itself. Its goal is to determine the signature of m.

3. **Exposed messages for RSA** (10 marks)
   Let (n, e) be an RSA public key, where $n = pq$, and e is an integer with $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$. It is known that the number of plaintexts $m \in [0, n-1]$ satisfying $m^e \equiv m \pmod{n}$ is

   $$[1 + \gcd(e-1, p-1)] \cdot [1 + \gcd(e-1, q-1)].$$

   Such a plaintext message m is called *exposed* since its RSA ciphertext is equal to m itself.

   (a) Let $e = \frac{\phi(n)}{2} + 1$. Prove that all n plaintext messages $m \in [0, n-1]$ are exposed.

(b) Let $n = 64349$ be an RSA modulus. Determine all values of e, $1 < e < \phi(n)$, $\gcd(e, \phi(n)) = 1$, for which $m^e \equiv m \pmod{n}$ for all $m \in [0, n-1]$.

4. **Offline electronic cash** (10 marks)
   Explain why *salts* are used in the offline cash protocol (slides 269-273).

5. **Discrete logarithms** (10 marks)
   $g = 64$ is known to be an element of order 131 in $\mathbb{Z}_{787}^*$. Use Shanks's algorithm to find $\log_g 388$. (Show the main steps of your work.)

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 22. 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