CO 487/687: Assignment #5 Due date: 3:00 pm, April 3 (Monday)

NOTE: Crowdmark links for Assignment #5 will be emailed to you before 11:00 am on March 24. If you do not receive the link, please send an email to ajmeneze@uwaterloo.ca.

1. **DSA** (10 marks)
   We recall the DSA signature scheme. The public domain parameters consist of a 3072-bit prime p, a 256-bit prime divisor q of $p-1$, and an element $g \in \mathbb{Z}_p^*$ of order q. Alice's private key is $a \in_R [1, q-1]$ and her public key is $h = g^a \bmod p$. To sign a message $M \in \{0,1\}^*$, Alice does the following:

   (i) Select a per-message secret $k \in_R [1, q-1]$.
   (ii) Compute $m = \text{SHA256}(M)$.
   (iii) Compute $r = (g^k \bmod p) \bmod q$, and check that $r \neq 0$.
   (iv) Compute $s = k^{-1}(m + ar) \bmod q$, and check that $s \neq 0$.
   (v) Alice's signature on M is (r, s).

   To verify A's signature (r, s) on M, Bob does the following:

   (i) Obtain an authentic copy of Alice's public key h.
   (ii) Check that $1 \leq r, s \leq q-1$.
   (iii) Compute $m = \text{SHA256}(M)$.
   (iv) Compute $u_1 = ms^{-1} \bmod q$ and $u_2 = rs^{-1} \bmod q$.
   (v) Compute $v = (g^{u_1} h^{u_2} \bmod p) \bmod q$.
   (vi) Accept if and only if $v = r$.

   Show how an adversary who knows a message M such that $\text{SHA256}(M) = 0$ can efficiently compute a valid signature for M.

2. **Elliptic curve computations** (10 marks)
   Consider the elliptic curve $E : Y^2 = X^3 + 2X + 6$ defined over $\mathbb{Z}_{17}$.

   (a) Find $E(\mathbb{Z}_{17})$, the set of $\mathbb{Z}_{17}$-points on E.
   (b) What is $\#E(\mathbb{Z}_{17})$? (Check: $\#E(\mathbb{Z}_{17})$ is prime.)
   (c) Find a generator of $E(\mathbb{Z}_{17})$.
   (d) Let $P = (11, 4)$, $Q = (11, 13)$, $R = (2, 1) \in E(\mathbb{Z}_{17})$. Compute the following points:
   (i) $P + Q$. (ii) $Q + R$. (iii) $2R$. (iv) $1575R$.
   (e) Determine $\log_P R$.

3. **Point multiplication** (10 marks)
   Let $E : Y^2 = X^3 + aX + b$ be an elliptic curve defined over $\mathbb{Z}_p$. Let $q = \#E(\mathbb{Z}_p)$, and suppose that q is prime. Design and analyze a polynomial-time algorithm which, on input p, a, b, q, $P \in E(\mathbb{Z}_p)$ and $m \in [1, q-1]$, outputs mP.

4. **Elliptic curve discrete logarithm problem** (10 marks)
   Let p be a prime, and let E be an elliptic curve defined over $\mathbb{Z}_p$. Let $q = \#E(\mathbb{Z}_p)$, and suppose that q is prime. Let $P, Q \in E(\mathbb{Z}_p)$ with $P, Q \neq \infty$.
   Describe Shanks's algorithm for computing $\log_P Q$, and show that the running time of the algorithm is $O(p^{1/2} \log^2 p)$ bit operations.

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 3:00 pm on April 3. 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