CO 487/687: Assignment #5 Due date: April 4 (Wednesday), 11:59 pm

---

NOTE: You will be emailed a Crowdmark link for submitting the assignment on March 23. If you do not receive the link, please send an email to ajmeneze@uwaterloo.ca.

1. **Elliptic curve computations** (10 marks)
   Consider the elliptic curve $E : Y^2 = X^3 + 10X + 16$ defined over $\mathbb{Z}_{17}$.

   (a) Find $E(\mathbb{Z}_{17})$, the set of $\mathbb{Z}_{17}$-rational points on E.

   Solution, all the '=' sign are modulo by 17 $0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 16, 5^2 = 8, 6^2 = 2, 7^2 = 15, 8^2 = 13, 9^2 = 13, 10^2 = 15, 11^2 = 2, 12^2 = 8, 13^2 = 16, 14^2 = 9, 15^2 = 4, 16^2 = 1$
   Let $x = 0, y^2 = 16, y = \pm 4 = 4, 13$ The same for $x = 1, 2, 3, \ldots 16$ All the rational points are $\{\infty, (0,4), (0,13), (4,1), (4,16), (5,2), (5,15)(7,2), (7,15), (8,8), (8,9), (9,6), (9,11)\}$

   (b) What is $\#E(\mathbb{Z}_{17})$? (Check: $\#E(\mathbb{Z}_{17})$ is prime.)

   Solution Its 13 and its a prime.

   (c) Find a generator of $E(\mathbb{Z}_{17})$.

   Solution Any point except ∞ is a generator as the $\#E(\mathbb{Z}_{17})$ is prime.

   (d) Let $P = (5,2)$, $Q = (9,11)$, $R = (9,6) \in E(\mathbb{Z}_{17})$. Compute the following points:
   (i) $P + Q$.
   $\lambda = \frac{11-2}{9-5} = 9 \cdot 4^{-1} = 9 \cdot 13 = -2$
   $x = (-2)^2 - 9 - 5 = 7, y = -((-2) \cdot (7-5) + 2) = 2$, Thus, $P + Q = (7,2)$
   (ii) $Q + R$.
   Since $Q = -R$, $Q + R = \infty$
   (iii) $2R$.
   $\lambda = \frac{3 \cdot 9^2 + 10}{6 \cdot 2} = (-2) \cdot 10 = -3$
   $x = (-3)^2 - 9 \cdot 2 = 8$
   $y = -((-3) \cdot (8-9) + 6) = 8$
   $2R = (8,8)$
   (iv) $2018R$.
   $2018R = (2018 \bmod 13)R = 3R = (4,1)$

   (e) Determine $\log_P R$.

   Solution $2P = (7,15), 3P = (9,6)$ Thus, $\log_P R = 3$

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

Solution Write m in binary representation as $m_i, i = 0, 1, 2, \ldots, \lfloor \log m \rfloor$

Algorithm 1 Double and Add

1: $X \leftarrow P, Q \leftarrow \infty$
2: **for** i from 0 to $\lfloor \log m \rfloor$ **do**
3: $\quad Q \leftarrow m_i X + Q$
4: $\quad X \leftarrow 2X$
5: **end for**
6: **Output** Q

Analysis The For loop gets executed $\lfloor \log m \rfloor$ times and each loop only contains constant computation, namely line 3 and 4. So the total runtime is $O(\lfloor \log m \rfloor \cdot \mathit{Constant}) \sim O(\log m)$ which is polynomial in terms of the length of m.

3. **Elliptic curve signature scheme** (10 marks)
Let p be a prime, and let E be an elliptic curve defined over $\mathbb{Z}_p$ with $\#E(\mathbb{Z}_p) = n$ (a prime). Let P be a generator of $E(\mathbb{Z}_p)$, and let H be a cryptographic hash function. Alice selects a private key $a \in_R [1, n-1]$, and computes her public key $A = aP$. She signs a message $m \in \{0,1\}^*$ as follows:

i) Select $k \in_R [1, n-1]$ and compute $R = kP$.
ii) Compute $e = H(m, R)$.
iii) Compute $s = (ae + k) \bmod n$.
iv) Alice's signature on m is (s, e).

(a) Describe a reasonable procedure for verifying Alice's signature (s, e) on a message m. Justify the *correctness* of your verification algorithm. (You do not have to justify the *security* of the signature scheme.)

Solution Compute $R' = sP - eA, e' = H(m, R')$. If $e' = e$ ACCEPT, otherwise REJECT.

$$H(m, R') = H(m, sP - eA) = H(m, (s - ea)P) = H(m, kP) = H(m, R) = e$$

(b) Suppose that Alice uses the same k to sign two different messages m_1 and m_2. Show how an adversary who knows these messages and their signatures can efficiently (and with high probability) determine Alice's private key.

Solution Since $R = (s - ea)P = sP - eA$, for two message signature pairs with the same k, $s_1P - e_1A = R_1 = kP = R_2 = s_2P - e_2A$

$$s_1P - e_1A = (s_1 - e_1a)P = (s_2 - e_2a)P = s_2P - e_2A$$

We have $s_1 - e_1a = s_2 - e_2a$ as P is a generator so k is unique.

$$a = (s_1 - s_2)(e_1 - e_2)^{-1}$$

As long as e_1 and e_2 are different (Since p is a prime, the inverse of $(e_1 - e_2)$ always exists as long as they are not equal), anyone can compute the private key. Assume H is collision resistant, then with high probability $e_1 \neq e_2$ as otherwise one could've found a collision $(m_1, R), (m_2, R)$.

4. **Elliptic curve hash function** (10 marks)
Let p be a 256-bit prime, and let E be an elliptic curve defined over $\mathbb{Z}_p$ with $\#E(\mathbb{Z}_p) = n$ a prime. Let $P, Q \in_R E(\mathbb{Z}_p)$ be points, neither of which is the point at infinity. Define the function $H : [0, n-1] \times [0, n-1] \longrightarrow E(\mathbb{Z}_p)$ by $H((a, b)) = aP + bQ$. That is, messages are pairs (a, b) of integers in the interval $[0, n-1]$, and the hash of such a message is the elliptic curve point $aP + bQ$. Prove, under a reasonable computational assumption, that H is collision resistant.

Solution Assume DL in Elliptic Curve is computationally infeasible, H is collision-resistant. Suppose H is not collision-resistant. Then one can efficiently finds $(a_1, b_1), (a_2, b_2)$ with either $a_1 \neq a_2$ or $b_2 \neq b_2$ as otherwise the plaintext would be the same, such that

$$a_1 P + b_1 Q = a_2 P + b_2 Q$$

WLOG, $a_1 \neq a_2$.

$$P = (a_1 - a_2)^{-1}(b_2 - b_1)Q$$

So one can compute $\log_P Q = (a_1 - a_2)^{-1}(b_2 - b_1)$

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 487/687. 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 **11:59 pm on April 4**. Late assignments will not be accepted except in *very* special circumstances (usually a documented illness of a serious nature). A high workload because of midterm tests and assignments in other courses will *not* qualify as a special circumstance.

Instructor and TA office hours:

Monday:	1:00 pm – 2:00 pm	Alessandra Graf (MC 5029)
	3:00 pm – 5:30 pm	Alfred Menezes (MC 5026)
Tuesday:	10:30 am – 11:30 am	Priya Soundararajan (MC 5466)
	11:30 am – 12:30 pm	Sam Jaques (QNC 4114)
	1:00 pm – 2:00 pm	Luis Ruiz-Lopez (MC 5486)
	3:00 pm – 4:00 pm	Elena Bakos Lang (MC 5474)
Thursday:	2:00 pm – 3:00 pm	Chris Leonardi (MC 5494)
Friday:	1:00 pm – 3:00 pm	Alfred Menezes (MC 5026)
