PAWS 2025: MATHEMATICAL CRYPTOGRAPHY
PROBLEM SET 4

GIACOMO BORIN, JOLIJN COTTAAR, ELI ORVIS, GABRIELLE SCULLARD

The goal for the exercises in Problem Set 4 is to give you practice with ECDLP and attacks on it. The problems are divided into three parts: beginner, intermediate, and advanced.

(1) (Beginner) Now that we know the group structure of elliptic curves, we can discuss Elliptic Curve Diffie Hellman.
  (a) Describe Elliptic Curve Diffie Hellman (ECDH), i.e., give the scheme of the key exchange method that does Diffie Hellman on an elliptic curve.
  (b) (sage) Implement ECDH in SageMath and do some tests to show that Alice and Bob will get the same secret.

(2) (Beginner, sage) Consider the elliptic curve (Curve25519) defined by the equation

$$y^2 = x^3 + 486662x^2 + x$$

over the prime field $\mathbb{F}_p$ where

$$p = 2^{255} - 19.$$

Using SageMath (see here for references on how to input a curve not in Short Weierstrass form), do the following:
  (a) Show that the curve is non-singular.
  (b) Compute the number of points on the curve over $\mathbb{F}_p$.
  (c) Find a point with x-coordinate $x = 9$ and use it as a base point for the Diffie-Hellman key exchange.
  (d) Time your implementation as you did for Exercise 7 in Problem Set 1. How does it compare to your previous implementation?

(3) (Beginner) Consider the elliptic curve $E : y^2 = x^3 + 1$ over $\mathbb{F}_{41}$. $E(\mathbb{F}_{41})$ is cyclic of order $42 = 2 \cdot 3 \cdot 7$ and generated by $P = (11, 15)$.
  (a) Let $Q = (25, 13)$. Compute $N \pmod{42}$ such that $[N]P = Q$, using the following computations to compute N mod 2,3, and 7.
    - $[21]P = [21]Q = (40, 0)$
    - $[14]P = (0, 40)$, $[14]Q = \infty$
    - $[6]P = (7, 37)$, $[6]Q = (7, 4)$
  (b) (sage) Write code which solves the ECDLP in $E(\mathbb{F}_{41})$, with base point $P = (11, 15)$. Randomly generate some points $Q = [N]P$ in $E(\mathbb{F}_{41})$ to check that your code works.

(4) (Beginner, sage) Let E be the elliptic curve $E : y^2 = x^3 - 3x + 1$ defined over $\mathbb{F}_{13}$. $E(\mathbb{F}_{13})$ is cyclic of order 19 and generated by $(0, 1)$. Let $Q = (4, 1) \in E(\mathbb{F}_{13})$.
  (a) Use Baby-Step Giant-Step to compute N such that $[N]P = Q$.
  (b) Use the adaptation of Pollard's Rho algorithm to elliptic curves (as described in Section 3.2.1) to compute N such that $[N]P = Q$.

(5) (Intermediate) Prove the remaining properties of Lemma 3.24 of the lecture notes.

(6) (Beginner) Let $e_N : E[N] \times E[N] \to \mu_N$ be a pairing satisfying the properties from Proposition 3.27 of the lecture notes. Show that:

$$e_N(P, Q) = e_N(Q, P)^{-1},$$

for all $P, Q \in E[N]$.

(7) (Intermediate) Let $e_N : E[N] \times E[N] \to \mu_{\mathbf{N}}$ be the Weil pairing, and $\det : E[N] \times E[N] \to \mathbb{Z}/N\mathbb{Z}$ be the determinant pairing with respect to some basis (T_1, T_2). Further denote

$$\mu = e_N(T_1, T_2) \in \mu_{\mathbf{N}}.$$

Show that:

$$e_N(P, Q) = \mu^{\det(P,Q)} \quad \text{for all } P, Q] in E[N].$$

Hint: Use the properties of the Weil pairing from Proposition 3.27 in the lecture notes.

(8) (Intermediate) Let $E : y^2 = x^3 + 1$ over $\mathbb{F}_p$ for some $p \equiv 2 \mod 3$. Consider some point $P \in E(\mathbb{F}_p)$ of order $\mathrm{ord}(P) = N$. Determine the embedding degree of N in $\mathbb{F}_p$.
Hint: Use Lemma 3.17 of the lecture notes.

(9) (Intermediate) Let $P \in E[N]$ a point of order N on an elliptic curve over a finite field $\mathbb{F}_p$ with $p \nmid N$.
 (a) First assume that N is prime. show that:

$$\#\{T \in E[N] | \mathrm{ord}(g) = N \text{ where } g = e_N(P, T)\} = N(N-1),$$

 and conclude that the probability that $e_N(P, T)$ is a primitive root of unity for a point $T \in E[N]$ chosen uniformly at random is $(N-1)/N$.
 (b) Now let $N \in \mathbb{Z}$ be an arbitrary positive integer. Compute the proportion of points $T \in E[N]$ so that $e_N(P, T)$ is a primitive N-th root of unity.

(10) (Intermediate, sage) In this exercise, you are Mallory and your goal is to recover Alice's key using the invalid curve attack. You are using the elliptic curve

$$E : y^2 = x^3 + x + 25, \quad \text{over } \mathbb{F}_p$$

with parameters $p = 18446744073709551629$ and $P = (100, 6701093164194334038) \in E(\mathbb{F}_p)$ with prime order $ord(P) = 18446744070571455341$.

Alice's public key is $A = (10301126922579099648, 1715709602745514383 3)$
 (a) You (Mallory) send the point $P1 = (18165116349323561130, 6150811377566577555)$. Check that $P_1 \notin E(\mathbb{F}_p)$. Find the (unique) parameter b_1 so that P_1 is on the curve $E_1 : y^2 = x^3 + x + b_1$. What is the order of P_1? Compute all possible values for $[a]P_1$ (without computing the secret key a).
 (b) By checking all possible values for $[a]P_1$, you find that Alice computed the "shared" session key $K_{AB,1} = (18446744073709551626, 5458368549901343073)$. What can you conclude about the value of a?
 (c) You continue sending more maliciously generated public keys. The points P_i sent by you and the value of Alice's corresponding session keys $K_{AB,i}$ are collected in the table below. What is Alice's secret key?

Point P_i	shared key $K_{AB,i}$
$(18165116349323561130, 6150811377566577555)$	$(18446744073709551626, 5458368549901343073)$
$(16395352116619970353, 6034018393034262788)$	$(16718172481871216672, 11838351310338 30123)$
$(12524092530016578390, 5123067425181934705)$	$(14160835454605074121, 3060569204740460707)$
$(4516937973540258973, 7005509288484349242)$	$(8040943336447228867, 13169014645599232942)$
$(15975665384073761733, 11032318707512935771)$	$(13311443695356568982, 15843145926225201761)$
$(7142461303424024564, 6616795770963544980)$	$(15087812134455913873, 4833814421951071352)$
$(15087812134455913873, 4833814421951071352)$	$(5030474179534288684, 4948558071821812509)$
$(9450845281388796607, 5731912410853213485)$	$(7134676168471120217, 6089059990139022202)$
$(5131031356309480317, 13835549974890579026)$	$(13275501062262900275, 10650377260320625285)$

(11) (Intermediate) Let $y^2 = x^3 + ax + b$ be an elliptic curve. Find a formula that computes $x([3]P)$ from $x(P)$ and the curve constants a, b.

(12) (Intermediate) Let K be a field with characteristic different from 2. Let $A, B \in K$ and $B \neq 0$. Then an elliptic curve given by the equation

$$E : By^2 = x^3 + Ax^2 + x$$

is said to be in *Montgomery form*. Curves in Montgomery form are particularly useful for efficient implementations of elliptic curve cryptography, in particular when working in projective coordinates.

(a) Show that a curve E in Montgomery form is non-singular if and only if $B(A^2 - 4) \neq 0$.
(b) Show that there is a unique point at infinity on the Montgomery model of an elliptic curve. Show that this point is not singular, and is always defined over the base field K.
(c) (sage) You can look at the addition formulas for Montgomery curves here [1]. Implement point addition and point doubling for Montgomery curves in projective coordinates in SageMath.
(d) Bonus question: when do these formulas fail, i.e., when do they require a division by zero? Compare this with the Short Weierstrass model case? Can you find a point of (conjectured) order 2 on a Montgomery curve?

(13) (Advanced) Let E be an elliptic curve in Montgomery form given by the equation $By^2 = x^3 + Ax^2 + x$ over a field K with characteristic different from 2. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E such that $x_1 \neq x_2$ and $x_1 x_2 \neq 0$. Then $P_1 + P_2 = (x_3, y_3)$ where

$$x_3 = \frac{B(x_2 y_1 - x_1 y_2)^2}{x_1 x_2 (x_2 - x_1)^2}.$$

Writing $P_1 - P_2 = (x_4, y_4)$ one finds

$$x_3 x_4 = \frac{(x_1 x_2 - 1)^2}{(x_1 - x_2)^2}.$$

For the case $P_2 = P_1$ we have $[2](x_1, y_1) = (x_3, y_3)$ where

$$x_3 = \frac{(x_1^2 - 1)^2}{4x_1(x_1^2 + Ax_1 + 1)}.$$

(This is Lemma 9.12.5 in Mathematics of Public Key Cryptography by Steven Galbraith.)

(a) Let $P = (x_P, y_P) \in E(K)$ be a point on an elliptic curve given in a Montgomery model. Define $X_1 = x_P$, $Z_1 = 1$, $X_2 = (X_1^2 - 1)^2$, $Z_2 = 4x_1(x_1^2 + Ax_1 + 1)$. Given (X_n, Z_n), (X_m, Z_m),

[1] `https://hyperelliptic.org/EFD/g1p/auto-montgom.html`

(X_{m-n}, Z_{m-n}) define

$$X_{n+m} = Z_{m-n}(X_n X_m - Z_n Z_m)^2$$
$$Z_{n+m} = X_{m-n}(X_n Z_m - X_m Z_n)^2$$

and

$$X_{2n} = (X_n^2 - Z_n^2)^2$$
$$Z_{2n} = 4X_n Z_n(X_n^2 + AX_n Z_n + Z_n^2).$$

Show that the x-coordinate of $[m]P$ is X_m/Z_m. In other words, show that these recursive formulas correctly compute the x-coordinate of multiples of the point $[m]P$. Note that, since these are recursive formulas, you can do a proof by induction on the addition formulas.

(b) Write a "double and add" algorithm to compute the x-coordinate of $[n]P$ using the projective Montgomery addition formula.

(14) (Advanced) (From material by Tanja Lange) The Elliptic Curve Digital Signature Algorithm works as follows: The system parameters are an elliptic curve E over a finite field $\mathbb{F}_p$, a point $P \in E(\mathbb{F}_p)$ on the curve, the number of points $n = |E(\mathbb{F}_p)|$, and the order ℓ of P. Furthermore a hash function h is given along with a way to interpret $h(m)$ as an integer.

Alice creates a public key by selecting an integer $1 < a < \ell$ and computing $P_A = [a]P$; a is Alice's long-term secret and P_A is her public key.

To sign a message m, Alice first computes $h(m)$, then picks a random integer $1 < k < \ell$ and computes $R = [k]P$. Let r be the x coordinate of R considered as an integer and then reduced modulo ℓ; for primes p you can assume that each field element of $\mathbb{F}_p$ is represented by an integer in $[0, p-1]$ and that this integer is then reduced modulo ℓ. If $r = 0$ Alice repeats the process with a different choice of k. Finally, she calculates

$$s = k^{-1}(h(m) + r \cdot a) \mod \ell.$$

If $s = 0$ she starts over with a different choice of k.

The signature is the pair (r, s).

To verify a signature (r, s) on a message m by user Alice with public key P_A, Bob first computes $h(m)$, then computes $w \equiv s^{-1} \mod \ell$, then computes $u_1 \equiv h(m) \cdot w \mod \ell$ and $u_2 \equiv r \cdot w \mod \ell$ and finally computes

$$S = [u_1]P + [u_2]P_A.$$

Bob accepts the signature as valid if the x coordinate of$S$ matches r when computed modulo ℓ.

(a) Show that a signature generated by Alice will pass as a valid signature by showing that $S = R$.

(b) Show how to obtain Alice's long-term secret a when given the random value k for one signature (r, s) on some message m.

(c) You find two signatures made by Alice. You know that she is using an elliptic curve over $\mathbb{F}_{1009}$ and that the order of the base point is $\ell = 1013$. The signatures are for $h(m_1) = 345$ and $h(m_2) = 567$ and are given by $(r_1, s_1) = (365, 448)$ and $(r_2, s_2) = (365, 969)$. Compute (a candidate for) Alice's long-term secret a based on these signatures, i.e. break the system.