Problem Set 4

PAWS 2025

Nathaniel Hurst

1

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) Implement ECDH in SageMath and do some tests to show that Alice and Bob will get the same secret.

(a) Alice and Bob want to create a shared public key using the ECDH. First Alice and Bob agree on all elliptic curve E defined over $\mathbb{F}_q$ and a point $P \in E(\mathbb{F}_q)$ such that $\operatorname{ord}(P) = N$. Alice and Bob then select private keys $0 < n_a, n_b < N$ and respectively compute their public keys $A = [n_a] \cdot P$ and $B = [n_b] \cdot P$. Then Alice computes the shared key $K = [n_a] \cdot B = [n_a n_b] \cdot P$ and Bob computes the shared key $K = [n_b] \cdot A = [n_b n_a] \cdot P$. The correctness of this relies on the fact that $n_a n_b = n_b n_a$.

(b) Implemented in the file ecc_point_add.sage is addition, doubling, and scaling $[n] \cdot P$ of points on elliptic curves. Implemented in the file ECDH.sage is the Elliptic Curve Diffie-Hellman key exchange using my implementation of point addition. (You can change the parameters as needed!)

2

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, 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?

(a) The curve is in Montgomery form with $B = 1$ and $A = 486662$ and so by problem #12 we have that the curve is non-singular if and only if $B(A^2 - 4) = A^2 - 4 \neq 0$, which is true for this cure. Thus Curve 25519 is non-singular.

(b) Using Sagemath, we see that

$$\#E(\mathbb{F}_p) = 57896044618658097711785492504343953926856930875039260848015607506283634007912$$

(c) To find a point with x-coordinate 9 we can plug 9 into the curve equation to get $y^2 = 39420360$ and then use the Tonelli-Shanks algorithm to find such a y, giving us

$$(x, y) = (9, 14781619447589544791020593568409986887264606134616475288964881837755586237401)$$

(d) My implementation can be found in the file X25519.sage (uses sagemath point addition/scale functions and the Montgomery ladder). It takes about 0.014 seconds to do a key exchange, which is about the same as my ElGamal implementation in problem set 1.

3

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:

(i) $[21]P = [21]Q = (40, 0)$

(ii) $[14]P = (0, 40)$, $[14]Q = \infty$

(iii) $[6]P = (7, 37)$, $[6]Q = (7, 4)$

(b) 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.

(a) First observe that since $[21] \cdot P = [21 \cdot N] \cdot P$ we have

$$21 - 21 \cdot N \equiv 0 \pmod{42}$$

which implies that for some $k \in \mathbb{Z}$ that

$$21 - 21 \cdot N = 42k$$

Now since the right hand side is even we must have N odd, or

$$N \equiv 1 \pmod 2$$

Similarly observe that since $[14 \cdot N] \cdot P = \infty$ we have

$$14N \equiv 0 \pmod{42}$$

Then we must have $N \equiv 0 \pmod 3$, for if $N \equiv 1 \pmod 3$ then

$$0 \equiv 14 \cdot N \equiv 14 \cdot (3k+1) \equiv 42k + 14 \equiv 14 \pmod{42}$$

a contradiction, and similarly for $N \equiv 2 \pmod 3$ we have

$$0 \equiv 14 \cdot N \equiv 14 \cdot (3k+2) \equiv 42k + 28 \equiv 28 \pmod{42}$$

another contradiction. Thus

$$N \equiv 0 \pmod 3$$

Finally observe that since $(7, 37) + (7, 4) = \infty$ we have that

$$[6] \cdot P + [6 \cdot N] \cdot P = \infty$$

or $6 + 6N \equiv 0 \pmod{42}$. Then let $N = 7k + r$ for $r \in \{0, 1, 2, 3, 4, 5, 6\}$. Then we have

$$6 + 6 \cdot N \equiv 6 + 6(7k + r) \equiv 6 + 42k + 6r \equiv 6 + 6r \equiv 0 \pmod{42}$$

Now by ranging r from 0 to 6 we see that the only value which makes sense is $r = 6$. Thus

$$N \equiv 6 \pmod 7$$

Now by the Chinese Remainder Theorem (or by checking every number up to 42) we have that

$$N \equiv 27 \pmod{42}$$

(b) An implementation of the Pollard's rho algorithm for this elliptic curve can be found in the file ECDLP_pollards_rho.sage. With it I computed the discrete logarithm of the point $(0, 40) \in E(\mathbb{F}_{41})$ to the base P, giving $[14] \cdot P = (11, 15)$.

4

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 $[N]P = Q$.

(a) First we compute the baby steps (there are $\left\lceil \sqrt{19} \right\rceil = 5$ such steps)

$$P_0 = \infty \quad P_1 = P = (0, 1) \quad P_2 = [2]P = (12, 4) \quad P_3 = [3]P = (10, 3) \quad P_4 = [4]P = (1, 8)$$

Then we compute the giant steps:

$$G_0 = Q \quad G_1 = Q - [5]P = (4, 12) \quad G_2 = Q - [10]P = (12, 4)$$

Then we have the collision $G_2 = P_2$, or $Q - [10]P = [2]P$, i.e. $Q = [12]P$.

(b) We use my implementation in the file ECDLP_pollards_rho.sage to find that

$$[12]P = Q$$

5 Prove the remaining properties of Lemma 3.26 of the lecture notes.

Let $P, Q, R \in E[N]$ with $E[N] = \langle T_1, T_2 \rangle$ and suppose $P = aT_1 + bT_2$, $Q = cT_1 + dT_2$, $R = eT_1 + fT_2$. Then

$$\det(P, Q + R) = \det(aT_1 + bT_2, (c + e)T_1 + (d + f)T_2) = a(d + f) - b(c + e) =$$
$$= (ad - bc) + (af - be) = \det(aT_1 + bT_2, cT_1 + dT_2) + \det(aT_1 + bT_2, eT_1 + fT_2) =$$
$$= \det(P, Q) + \det(P, R)$$

Similarly observe that

$$\det(P, P) = \det(aT_1 + bT_2, aT_1 + bT_2) = ab - ba = 0$$

Now suppose that $\det(P, Q) = 0$ for all $P \in E[N]$. Then

$$\det(P, Q) = \det(aT_1 + bT_2, cT_1 + dT_2) = ad - bc \equiv 0 \pmod{N}$$

Now since P is arbitrary (for proving this property), choose $a = 0$ and b coprime to N, for example $b = -1 \in \mathbb{Z}/N\mathbb{Z}$ then we get $bc \equiv 0 \pmod{N}$, so $N \mid bc$, but $\gcd(N, b) = 1$, so by Euclids lemma $N \mid c$. Similarly choosing $b = 0$ and a comprime to N we can find that $N \mid d$. But since T_1, T_2 are of order N we must have that $cT_1 = \infty$ and $dT_2 = \infty$, or $Q = cT_1 + dT_2 = \infty$.

6 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 $P, Q \in E[N]$.

Observe that for all $P, Q \in E[N]$ we have

$$e_N(P + Q, P + Q) = 1$$

(since the pairing is alternating) and expanding using bilinearity we get

$$e_N(P, P)e_N(P, Q)e_N(Q, P)e_N(Q, Q) = e_N(P, Q)e_N(Q, P) = 1$$

and multiplying on the right by $e_N(Q, P)^{-1}$ gives us the desired result of

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

7

Let $e_N : E[N] \times E[N] \to \mu_N$ 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

$$\mu = e_N(T_1, T_2) \in \mu_N$$

Show that:

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

Hint: Use the properties of the Weil pairing from Proposition 3.29 in the lecture notes.

Let $P = aT_1 + bT_2$ and $Q = cT_1 + dT_2$. Then $\det(P, Q) = ad - bc$. Now observe that

$$e_N(P, Q) = e_N(aT_1 + bT_2, cT_1 + dT_2) = e_N(aT_1, dT_2)e_N(bT_2, cT_1) = e_N(T_1, T_2)^{ad} e_N(T_2, T_1)^{bc} = e_N(T_1, T_2)^{ad} \left(e_N(T_1, T_2)^{bc}\right)^{-1} = \mu^{ad}\mu^{-bc} = \mu^{ad-bc} = \mu^{\det(P,Q)}$$

where we used the fact that $e_N(aT_1, bT_2) = e_N(T_1, T_2)^{ab}$ which is seen by writing $aT_1 = T_1 + \ldots + T_1$ a times and similarly for b and expanding using bilinearity. We also used the result from problem 6 such that $e_N(P, Q) = e_N(Q, P)^{-1}$

8

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

By Lemma 3.17 we have that $\#E(\mathbb{F}_p) = p + 1$. Then we know that $N \mid p + 1$, or $p \equiv -1 \pmod N$. Then $p^2 \equiv 1 \pmod N$, or $p^2 - 1 \equiv 0 \pmod N$. That is, $N \mid p^2 - 1$, or the embedding degree is 2, which makes this curve quite insecure as it is open to attacks by the MOV algorithm and index-calculus.

9

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

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

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 $\frac{N-1}{N}$.

(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.

(a) Observe that if we write $E[N] = \langle P, R\rangle$ (we know that $E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$) we have that for any element $T \in E[N]$ of the form $T = nP + 0R = nP$ that

$$e_N(P, T) = e_N(P, nP) = e_N(P, P)^n = 1^n = 1$$

is not of order N. But for any element of the form $T = nP + kR$ where $k \neq 0$ we have that

$$e_N(P, T) = e_N(P, nP + kR) = e_N(P, nP)e_N(P, kR) = 1 \cdot e_N(P, R)^k \neq 1$$

where we used the fact that $e_N(P, R) \neq 1$ since e_N is non-degenerate. Then $e_{N(P,T)}$ is an element of the group of N −th roots of unity, and since N is prime we must have that the order of $e_N(P, T)$ is N (it must divide N, but N is prime). Hence for all elements of the form $T = nP + kR$ for $n \in \{0, ..., N-1\}$ and $k \in \{1, ..., N-1\}$ we have that $e_N(P, T)$ has order N, and there are exactly $N(N-1)$ such elements (by ranging through n and k, with N choices for n, and $N-1$ choices for k).

Then since there are N^2 elements in $E[N]$ (since $E[N] = \langle P, R \rangle$ where both P, R have order N) we have that the probability that $e_N(P, T)$ is a primitive root of unity for a point $T \in E[N]$ chosen uniformly is

$$\frac{N(N-1)}{N^2} = \frac{N-1}{N}$$

(b) Observe that in this case we can pick $R \in E[N]$ such that $R \notin \langle P \rangle$ and $e_N(P, R)$ is a primitive N −th root of unity. Then all elements of the form $T = nP + kR$ for k such that $\gcd(k, N) = 1$ are such that

$$e_N(P, T) = e_N(P, R)^k$$

is a primitive root of unity (since the order of this element is $\frac{N}{\gcd(k,N)} = N$). Then by the same reasoning in part (a) we have that there are exactly $N(\varphi(N))$ such elements, and so the proportion of points $T \in E[N]$ such that $e_N(P, T)$ is a primitive N-th root of unity is exactly

$$\frac{N(\varphi(N))}{N^2} = \frac{\varphi(N)}{N}$$

10

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

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

with parameters

$$p = 18446744073709551629 \quad P = (100, 6701093164194334038) \in E(\mathbb{F}_p)$$

with prime order $\text{ord}(P) = 18446744075714553441$.

Alice's public key is

$$A = (10301216922579099648, 17157096027455143833)$$

(a) You (Mallory) send the point

$$P_1 = (18165116349323561130, 6150811377566577555)$$

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 values 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, 1183835131033830123)
(12524092530016578390, 5123067425181934705)	(14160835454605074121, 3060569204740460707)
(4516937973540258973, 7005509288484349242)	(8040943336447228867, 13169014645599232942)
(15975665384073761733, 11032318707512935771)	(13311443695356568982, 15843145926225201761)
(15087812134455913873, 4833814421951071352)	(5030474179534288684, 4948558071821812509)
(9450845281388796607, 5731912410853213485)	(7134676168471120217, 6089059990139022202)
(5131031356309480317, 13835549974890579026)	(13275501062262900275, 10650377260320625285)

(a) Using SageMath we see that $P_1 \notin E(\mathbb{F}_p)$, and that Mallory is using the curve $y^2 = x^3 + x + 2$. With P_1 having order 20 on this curve.

(b) By checking all possible values of $[a]P_1$ and comparing them to the shared session key $K_{AB,1}$ we find that $a \equiv 5 \pmod{20}$.

(c) Proceeding as we did in part (b), we find the following relations:

Point P_i	**a ≡ ? mod ord(P_i)**
(18165116349323561130, 6150811377566577555)	$a \equiv 5 \pmod{20}$

(16395352116619970353, 6034018393034262788)	$a \equiv 56 \pmod{107}$
(12524092530016578390, 5123067425181934705)	$a \equiv 17 \pmod{41}$
(4516937973540258973, 7005509288484349242)	$a \equiv 137 \pmod{509}$
(15975665384073761733,11032318707512935771)	$a \equiv 16 \pmod{19}$
(15087812134455913873, 4833814421951071352)	$a \equiv 270 \pmod{373}$
(9450845281388796607, 5731912410853213485)	$a \equiv 16 \pmod{199}$
(5131031356309480317, 13835549974890579026)	$a \equiv 249 \pmod{739}$

Then by the Chinese Remainder Theorem we have that

$$a \equiv 43439236816954465 \pmod{46545249215375620}$$

which gives us about 300 options for a modulo the order of P. A quick check of all 300 gives us Alice's secret key:

$$a \equiv 3348151931108623485 \pmod{18446744075714553441}$$

11 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.

Assume that P has order > 3, for if not we can deduce the x coordinate of $x([3]P)$ using only $x(P)$ and $x([2]P)$. Then let $[2] = (x([2]P, y_2)$. Then observe that by Remark 3.44 in the notes that

$$x([2]P) = \frac{(3x(P)^2+a)^2}{4(x(P)^3+ax(P)+b)} - 2x(P)$$

Then $x([3]P) = x([2]P + P) = x((x[2]P, y_2) + (x(P), y_1))$ and observe by the group law with $[2]P \neq P, -P$ (order of P is greater than 3) we have

$$x((x([2]P), y_2) + (x(P), y_1)) = \frac{(y_2-y_1)^2}{(x([2]P)-x(P))^2} - x(P) - x([2]P)$$
$$= \frac{y_2^2-y_1^2+2y_1y_2}{(x([2]P)-x(P))^2} - x(P) - x([2]P) =$$
$$= \frac{x([2]P)^3+ax([2]P)+b-x(P)^3-ax(P)-b+2\sqrt{(x([2]P)^3+ax([2]P)+b)(x(P)^3+ax(P)+b)}}{(x([2]P)-x(P))^2} - x(P) - x([2]P)$$

12 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) You can look at the addition formulas for Montgomery curves (see SageMath documentation). Implement point addition and point doubling for Montgomery curves in projective coordinates in SageMath.

(d) 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?

(a) First we write $f = x^3 + Ax^2 + x - By^2$. Then $f_x = 3x^2 + 2Ax + 1$ and $f_y = -2By$. Then suppose that the curve E was singular at a point (x_0, y_0). Then $f_x = 3x_0^2 + 2Ax_0 + 1 = 0$ and $f_y = -2By_0 = 0$. From this we see that $y_0 = 0$ and so we must have the following system

$$0 = x_0^3 + Ax_0^2 + x_0$$

$$0 = 3x_0^2 + 2Ax_0 + 1$$

and by multiplying the first equation by 3, the second by x_0 (which is not zero for if it was the second equation would imply $0 = 1$) and subtracting th first from the second we get

$$0 = -Ax_0^2 - 2x_0 = -x_0(Ax_0 + 2) \implies x_0 = -\tfrac{2}{A}$$

now substituting this back into equation #2 we get

$$0 = 3\left(\tfrac{4}{A^2}\right) - 4 + 1$$

or rearranging

$$\tfrac{4}{A^2} - 1 = 0$$

or

$$A^2 - 4 = 0$$

Then $B(A^2 - 4) = 0$.

But also observe that in this step $\frac{4}{A^2} - 1 = 0$ we have a necessary condition for this system having a solution is $A^2 = 4$, or $A^2 - 4 = 0$, and in fact by following the steps as above we see that it is also sufficient. Hence E is non-singular if and only if $B(A^2 - 4) \neq 0$.

(b) and (c) Ommitted.

(d) Observe that if the x coordinate of $[2]P$ is $\frac{X_2}{Z_2}$ (as in problem #13). and $P = (x_P, y_P)$ then

$$\tfrac{X_2}{Z_2} = \tfrac{(X_1^2-1)^2}{4X_1(x_1^2+Ax_1+1)}$$

can fail when $X_1 = x_P = 0$ (as in this case it requires division by zero). Then plugging this into the curve equation we get $y_P = 0$, and so the point of possible order 2 would be $(0, 0)$.

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

$$x_3 = \frac{B(x_2y_1 - x_1y_2)^2}{x_1x_2(x_2 - x_1)^2}$$

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

$$x_3x_4 = \frac{(x_1x_2 - 1)^2}{(x_1 - x_2)^2}$$

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.)

13

(a) Let $P = (x_P, y_P) \in E(K)$ be a point on an elliptic curve given in a Montgomery model. Define

$$X_1 = x_P, Z_1 = 1, X_2 = (X_1^2 - 1)^2, Z_2 = 4X_1(X_1^2 + Ax_P + 1)$$

Given (X_n, Z_n) and (X_m, Z_m), (X_{m-n}, Z_{m-n}) define

$$X_{n+m} = Z_{m-n}(X_nX_m - Z_nZ_m)^2$$
$$Z_{n+m} = X_{m-n}(X_nZ_m - Z_nX_m)^2$$

and

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

Show that the x-coordinate of $[m]P$ is $\frac{X_m}{Z_m}$. 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.

(a) Ommitted.

(b) Since the x-coordinate of $[n]P$ is exactly $\frac{X_n}{Z_n}$, our algorithm only needs to compute thes. First convert $n = (e_Ne_{N-1}...e_0)_2$ to binary. Then $X_n = X_{(2^Ne_N + 2^{N-1}e_{N-1} + ... + 2e_1 + e_0)}$ and similarly for

Z_n. Then let $X = (x_P^2 - 1)^2$, $X_{\text{lag}} = x_P$, $Z = 4x_{P(x_P^2+Ax_P+1)}$ and $Z_{\text{lag}} = 1$, and a helper variable $R \leftarrow X$. The algorithm is as follows:

$$\text{from } i = N-1 \text{ down to } 0 \text{ do:}$$

$$\bullet \text{ if } e_i = 0 \text{ then } X \leftarrow \left(XX_{\text{lag}} - ZZ_{\text{lag}}\right)^2 \text{ and } Z \leftarrow x_P\left(X_{\text{lag}}Z - Z_{\text{lag}}R\right)^2, \text{also } R \leftarrow X_{\text{lag}}$$

$$\text{and finally } X_{\text{lag}} \leftarrow \left(X_{\text{lag}}^2 - Z_{\text{lag}}^2\right)^2 \text{ and } Z_{\text{lag}} \leftarrow 4RZ_{\text{lag}}\left(R^2 + ARZ_{\text{lag}} + Z_{\text{lag}}^2\right) \text{ and } R \leftarrow X$$

$$\bullet \text{ if } e_i = 1 \text{ then } X_{\text{lag}} \leftarrow \left(XX_{\text{lag}} - ZZ_{\text{lag}}\right)^2 \text{ and } X \leftarrow \left(X^2 - Z^2\right)^2 \text{ and finally } Z \leftarrow 4RZ(R^2 + ARZ + Z^2)$$

$$\text{output: } \frac{X_{\text{lag}}}{Z_{\text{lag}}}$$

What this algorithm is essentially doing is at each step if the bit is 0 and we currently have $X = X_{n+1}, X_{\text{lag}} = X_n$ then we reassign the values $X \leftarrow X_{2n+1}$, $X_{\text{lag}} \leftarrow X_{2n}$ (and similarly for the Z's), and if the bit is 1 we only double, assigning $X \leftarrow X_{2n+2}$ and $X_{\text{lag}} \leftarrow X_{2n+1}$. Ranging along all bits gives us the final outputs X_N, Z_N.

14

(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 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

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

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 $w = s^{-1} \bmod \ell$, then computes $u_1 = h(m) \cdot w \bmod \ell$ and $u_2 = r \cdot w \bmod \ell$, 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.

(a) Observe that

$$S = [u_1]P + [u_2]P_A = [u_1]P + [a \cdot u_2]P = [u_1 + a \cdot u_2]P = [h(m) \cdot s^{-1} + a \cdot r \cdot s^{-1}]P$$
$$= [s^{-1}(h(m) + r \cdot a)]P$$

and since $s \equiv k^{-1}(h(m) + r \cdot a) \pmod{\ell}$ we have $s^{-1} \equiv k(h(m) + r \cdot a)^{-1} \pmod{\ell}$, and so

$$[s^{-1}(h(m) + r \cdot a)]P = [k(h(m) + r \cdot a)^{-1}(h(m) + r \cdot a)]P = [k]P = R$$

Thus this wil pass as a valid signature, as $S = R$.

(b) When given k for one message, combined with the fact that (r, s) and $h(m)$ are known, we can do the computation

$$r^{-1}(k \cdot s - h(m)) \equiv r^{-1}(k \cdot (k^{-1}(h(m) + r \cdot a)) - h(m)) \equiv r^{-1}(h(m) + r \cdot a - h(m)) \equiv r^{-1}(r \cdot a) \equiv a \pmod{\ell}$$

giving us Alice's long term key a.

(c) Observe that since $r_1 = r_2$ we know that either $k_1 \equiv k_2 \pmod{\ell}$ or $k_1 \equiv -k_2 \pmod{\ell}$ (since the x coordinate matches the points $[k_1]P$ and $[k_2]P$ must be the same or inverses).

First suppose that $k_1 \equiv k_2 \pmod{\ell}$ (call it k). Then we know by definition of s_1 that

$$448 \equiv s_1 \equiv k^{-1}(h(m_1) + r \cdot a) \equiv k^{-1}(345 + 365 \cdot a) \pmod{\ell}$$

or rearranging

$$a \equiv 365^{-1}(448k - 345) \pmod{\ell}$$

Similarly from the definition of s_2 we also derive that

$$a \equiv 365^{-1}(969k - 567) \pmod{\ell}$$

and so setting them equal we can solve for $k \equiv 679 \pmod{\ell}$, allowing us to solve for

$$a \equiv 974 \pmod{\ell}$$

Now in the case where $k_1 \equiv -k_2 \pmod{\ell}$ we have the following system by definition of s_1, s_2

$$a \equiv 365^{-1}(448k_1 - 345) \pmod{\ell}$$

and

$$a \equiv 365^{-1}(-969k_1 - 567) \pmod{\ell}$$

where we used the fact that $k_2^{-1} = (-k_1)^{-1} = -k_1^{-1}$. Then we can set them equal to eachother and solve for $k_1 \equiv 185 \pmod{\ell}$, and finally use that to solve for

$$a \equiv 240 \pmod{\ell}$$

Thus we have two candidates for a, and one must be the actual value, so we have broken the system.