The University of Sydney
Math3925 Public Key Cryptography

Semester 2 **Solutions for Assignment 3** 2003

1. Let E be the elliptic curve $E/\mathbb{F}_{1723}$

$$y^2 = x^3 + 568x + 1350,$$

with $E(\mathbb{F}_{1723})$ of order $2^2 \cdot 443$, let $P = (524, 1413)$ be a generator for the subgroup of prime order 443, and let $Q = (1694, 125)$ be another point of order 443.

a. Determine the abelian invariants of E, and find elements G_1 and G_2 which generate $E(\mathbb{F}_{1723})$ such that both $\log_{G_1}(P)$ and $\log_{G_2}(P)$ equal 2.

b. Compute the discrete logarithm $\log_P(Q)$ using the baby-step, giant-step algorithm.

c. Compute the discrete logarithm $\log_P(Q)$ using a Pollard ρ algorithm, giving the sequence $P_i = n_i P + m_i Q$ in a table with the exponent sequence (n_i, m_i), and the function f such that $P_{i+1} = f(P_i)$ you used to generate your sequence.

Solution

a. The group is either cyclic of order $4 \cdot 443$ or is isomorphic to $\mathbb{Z}/2Z \times \mathbb{Z}/886\mathbb{Z}$. For such G_1 and G_2 to exist, $886G_i = 443P = \mathcal{O}$, so the group exponent is 886, so the latter is correct. In order to find such elements we first note that $Q_0 = 222P$ satisfies $2 \cdot 222P = 444P = P$. Then, by choosing random points and raising them to the power 443, we determine two independent 2-torsion points Q_1 and Q_2. Now $G_1 = Q_0 + Q_1$ and $G_2 = Q_0 + Q_2$ generate the 2-torsion subgroup, give $2G_1 = P$, and thus also generate the cyclic subgroup of order 443.

b. We first form the baby steps $P, 2P, 3P, \ldots, 41P$, then the sequence of giant steps from $Q, Q + 42P, Q + 84P, \ldots$. In this case we find a match

$$Q + 8 \cdot 42P = 37P,$$

whence $Q = (37 - 8 \cdot 42)P = -299P$ so $\log_P(Q) = -299 \bmod 443 = 144$.

c. The following `Magma` code implements a simple Pollard ρ algorithm, in this case we find a trivial match $3P + 323Q = 6P + 626Q = \mathcal{O}$, hence (again)

$$Q = -323^{-1}3P = -299P = 144P.$$

```
E := EllipticCurve([FiniteField(1723)|568,1350]);
P := E![524,1413]; Q := E![1694,125];

function PollardStep(Pi,ni,mi)
    xi := Integers()!Pi[1];
    if xi le 30 then
return Pi+P, ni+1, mi;
    elif xi le 60 then
return 2*Pi, 2*ni, 2*mi;
    else
return Pi+Q, ni, mi+1;
    end if;
end function;

P1i := P; n1i := 1; m1i := 0;
P2i, n2i, m2i := PollardStep(P1i,n1i,m1i);
repeat
    P1i, n1i, m1i := PollardStep(P1i,n1i,m1i);
    P2i, n2i, m2i := PollardStep(P2i,n2i,m2i);
    P2i, n2i, m2i := PollardStep(P2i,n2i,m2i);
until P1i eq P2i;
```

2. Let (E, P, Q, n, h) be an elliptic curve ElGamal public key, defined by

$$E : y^2 = x^3 + x + 46138835891$$

over the field $\mathbb{F}_p$ where $p = 57093632599$, with points

$$P = (30878623636, 18908393885)$$
$$Q = (35764107892, 37899251204)$$

such that $nP = O$ and $nh = |E(\mathbb{F}_p)|$, where $n = 57093496807$ and $h = 1$. Given an encrypted message (R, S), where

$$R = (39054828257, 56592547930)$$
$$S = (52681797901, 1351188767)$$

find the secret message M.

N.B. An elliptic curve ElGamal public key specifies an elliptic curve E over $\mathbb{F}_q$, a generator P of a prime order cyclic subgroup of order n, a multiple $Q = [x](P)$, and the order of the cokernel $E(\mathbb{F}_q)/\langle P \rangle$.

Solution We first solve the discrete logarithm $x = 49250313024$. Then

$$M := S - xR = (4181957872, 50461884172).$$

3. Let $N = 73018750355491$ be the product of two primes p and q. Find an elliptic curve E over $\mathbb{Z}/N\mathbb{Z}$, an integer m and the x-coordinate of a point P, such that $mP = (x : y : z)$ where $\mathrm{GCD}(N, z) = p$, and hence factor N. After factoring N, determine the group structure of $E(\mathbb{Z}/N\mathbb{Z})$.

Solution The elliptic curve $E : y^2 = x^3 + x + 1$ over $\mathbb{Z}/N\mathbb{Z}$ gives

$$E(\mathbb{Z}/N\mathbb{Z}) \cong E(\mathbb{Z}/p\mathbb{Z}) \times E(\mathbb{Z}/q\mathbb{Z}).$$

Beginning with $P = (0, 1) = (0 : 1 : 1)$, raised to powers of primes up to 200, we find an point $Q = (x : y : z)$ with $\mathrm{GCD}(z, N) = p$. With this factorization, we find the group orders

$$|E(\mathbb{Z}/p\mathbb{Z})| = 2^6 \cdot 17 \cdot 23 \cdot 191, \text{ and } |E(\mathbb{Z}/q\mathbb{Z})| = 2^3 \cdot 7 \cdot 272903,$$

explaining why $Q = \mathcal{O} \in E(\mathbb{Z}/p\mathbb{Z})$ but $Q \neq \mathcal{O} \in E(\mathbb{Z}/q\mathbb{Z})$. To find the group structure of $E(\mathbb{Z}/N\mathbb{Z})$ we only need to know the groups structure of each quotient, which is determined by an analysis of the 2-torsion subgroup.