University College London
Department of Computer Science

Cryptanalysis Lab 07

J. P. Bootle, N. Courtois

March 7, 2019

jonathan.bootle.14@ucl.ac.uk
Version 2.0

1. Polynomials and Interpolation

Lagrange interpolation polynomial

The purpose here is to determine the unique polynomial of degree n, P_n which verifies

$$P_n(x_i) = f(x_i), \quad \forall i = 0, \ldots, n.$$

The polynomial which meets this equality is Lagrange interpolation polynomial

$$P_n(x) = \sum_{k=0}^{n} l_k(x) f(x_k)$$

where l_k are polynomials of degree n that form a basis of $\mathcal{P}_n$

$$l_k(x) = \prod_{i=0 \; i \neq k}^{n} \frac{x - x_i}{x_k - x_i} = \frac{x - x_0}{x_k - x_0} \cdots \frac{x - x_{k-1}}{x_k - x_{k-1}} \frac{x - x_{k+1}}{x_k - x_{k+1}} \cdots \frac{x - x_n}{x_k - x_n}$$

Using Lagrange formula find a polynomial such that:

```
P(1) = 0
P(2) =  -3
P(3) =  10
P(4) =  81
```

2. Polynomials and Interpolation

Show that it is IMPOSSIBLE to find a polynomial with integer coefficients such that:

```
P(1) = 5
P(2) = 5
P(3) = 5
P(4) = 5
P(5) = 8
```

Hint: if x is a root of a polynomial then it can be divided by $(x-a)$. Factorization of polynomials with real/rational/integer coefficients is unique.

3. Elliptic Curve Diffie-Hellman

Click on the green letter in front of each sub-question (e.g. (a)) to see a solution. Click on the green square at the end of the solution to go back to the questions.

EXERCISE 1. In this exercise, you will use Sage and share a Diffie-Hellman Key with a partner, using points on an elliptic curve. To create an elliptic curve E defined by $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$, use `E = EllipticCurve(GF(p),[a,b])`.

(a) Create an elliptic curve E defined by $y^2 = x^3 + 70x + 355$, over the finite field of size 1031.

(b) The command `n = E.cardinality()` sets n to be the number of points on the curve. What is the value of n? What properties should n have in order to be suitable for Diffie-Hellman?

(c) Typing `E.gens()` gives a set of points which generate all the points on the elliptic curve. In this case, there is only one generator, and `P = E.gens()[0]` sets P to be a group generator for this curve. If $P = (x : y : z)$, then your partner can get P by typing `P = E(x,y,z)`.

(d) Choose a random integer a such that $0 \leq a < n$. Your partner should choose b similarly.

(e) Use Sage to find the elliptic curve point $A = a^*P$, and give this to your partner. For example, if $A = (x : y : z)$ then your partner can type `A = E(x,y,z)` to get A.

Your partner should compute $B = b^*P$ and give this to you in the same way.

(f) Use Sage to find $a^*B = (ab)^*P$. Your partner will also find $(ab)^*P$ via b^*A. The point $(ab)^*P$ is your shared secret key. Check that you and your partner computed the same answer.

4. Elliptic Curve Factorisation Algorithm

Click on the green letter in front of each sub-question (e.g. (a)) to see a solution. Click on the green square at the end of the solution to go back to the questions.

EXERCISE 2. In this exercise, you will use Sage to explore how integers are factored using elliptic curves.

(a) To create an elliptic curve Ep defined by $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$, use `E = EllipticCurve(GF(p),[a,b])`. Create an elliptic curve Ep defined by $y^2 = x^3 + x + 4$, over the finite field of size 11.

(b) To create a curve EN defined by $y^2 = x^3 + ax + b$ over $\mathbb{Z}_N$, use `E = EllipticCurve(Integers(N),[a,b])`. Create a curve EN defined by $y^2 = x^3 + x + 4$, over the ring of integers modulo 438713.

(c) Type $PN = EN(100584, 115601)$ to create the corresponding point on EN. Similarly, type $Pp = Ep(100584, 115601)$ to create the same point, reduced modulo 11, on Ep. Type `Pp` to view the point modulo 11. The point should be expressed as $(x : y : 1)$. The point at infinity is $(0 : 1 : 0)$.

(d) Type `Ep.cardinality()` to find out the number of elliptic curve points modulo 11. What is the number of points? Type `a*Pp` to compute multiples of the point Pp. What is the order of Pp in the elliptic curve group Ep?

(e) Set $QN = 8 * PN$ and use SAGE to compute QN. Now, try to compute $9 * PN = QN + PN$. What happens? Compute the difference between the x coordinates of PN and QN, and compute the greatest common divisor of this with N. Look at the formulae for adding elliptic curve points. Does this explain the error?

(f) Set $N = 20077$. Consider the curve E defined by the equation $y^2 = x^3 + x + 5$. Assume that N has a prime factor p with $\mid E(\mathbb{Z}_p) \mid$ being 5-powersmooth. Given that $P = (427, 466)$ is a point on $E(\mathbb{Z}_N)$, factor N.

Solutions to Exercises

Exercise 1(a) Use `E = EllipticCurve(GF(1031),[70,355])` to produce the correct elliptic curve. □

Exercise 1(b) You should get $n = 1009$. For secure Diffie-Hellman key exchange, we ideally want n to be large and prime so that the Discrete Logarithm problem is hard in the elliptic curve group. □

Exercise 1(c) An example generator is the point $P = (5 : 393 : 1)$. It doesn't matter which generator you use, as long as you and your partner are using the same generator. □

Exercise 1(d) You can use `a = randint(0,1009)` to get a. □

Exercise 1(e) The point a^*P is computed in Sage exactly as written here: `a*P`. □

Exercise 1(f) Get b^*P from your partner. □

Exercise 2(a) Use `Ep = EllipticCurve(GF(11),[1,4])` to produce the correct elliptic curve. □

Exercise 2(b) Use `EN = EllipticCurve(Integers(438713),[1,4])` to produce the correct curve. □

Exercise 2(d) There are 9 points on the elliptic curve Ep defined modulo 11. The order of a group element divides the order of the group, 9, and Pp is not the point at infinity, so we only have to check whether $3 * Pp$ is equal to the point at infinity or not. However, $3 * Pp = (3 : 1 : 1)$, so 3 is not the order of Pp. Therefore, the order of Pp is 9. □

Exercise 2(e) You can use `a = randint(0,1009)` to get a. □