TCSS543 Final Project

Elliptic Curve Cryptography

Wenjun Yang	Student ID: 1872178
Tianyi Li	Student ID: 1827924

Implementation

Detailed implementation of the five algorithms below can be found in our submission.

1. Calculate multiplications: given points a^1 and a^2 and values of d and p, computes a^3 as the product of a^1 and a^2.

2. Calculate exponentiations: given a point a, an exponent m and values of d and p, computes the exponentiation of $b = a^m$.

3. Pollard's Rho Algorithm: given input point a and b, where $b = a^m$, and values of d, p and n, calculate the discrete exponent m modulo n, and count the number of steps required for such iterations.

4. Calculate Avg Rho Steps: given a point a and values of d, p and n, generate a random exponent m modulo n by 2). Then, find the discrete exponent m modulo n using 3) and return the average number of steps required over N random discrete logarithms.

   Parameters: $p = 2^{16}-17$, $d = 154$, $n = 16339$, $a = (12, 61833)$

5. (Bonus) Calculations: finding average steps required for the following parameters.

   a). $p = 2^{18}-5$, $d = 294$, $n = 65717$, $a = (5, 261901)$

   b). $p = 2^{20}-5$, $d = 47$, $n = 262643$, $a = (3, 111745)$

   c). $p = 2^{22}-17$, $d = 314$, $n = 1049497$, $a = (4, 85081)$

Results

Different random exponent would yield slightly varied outcomes. Following results are the medians in the series of outputs.

4). Parameters: $p = 2^{16}-17$, $d = 154$, $n = 16339$, $a = (12, 61833)$

Output: **~163 steps**.

5a). Parameters: $p = 2^{18}-5$, $d = 294$, $n = 65717$, $a = (5, 261901)$

Output: **~335 steps**.

5b). Parameters: $p = 2^{20}-5$, $d = 47$, $n = 262643$, $a = (3, 111745)$

Output: **~645 steps**.

5c). Parameters: $p = 2^{22}-17$, $d = 314$, $n = 1049497$, $a = (4, 85081)$

Output: **~1322 steps**.