CS 292F Elliptic Curve Cryptography
Winter Term 2017

Homework Assignment 02:

Consider the discrete logarithm problem

$$y = g^x \pmod{2017}$$

for the primitive $g = 5$ and $y = 1736$.

1. Write a simple exhaustive search code to find x and verify.
2. Find x using Shank's algorithm. Show the steps, and produce the S and T tables.
3. Find x using Pollard Rho algorithm. Show the steps, and produce the sequence.
4. Find x using Pohlig-Hellman algorithm. You can use the factorization of $2016 = 2^5 3^2 7$ to create two smaller discrete log problems, for example $2016 = 36 \cdot 56$. Show the steps.
5. Find x using the Index Calculus algorithm. Try the prime base $\{2, 3, 5\}$ and if this does not work, try $\{2, 3, 5, 7\}$. Show the steps.

Due 5pm Tuesday February 7
Either, upload an electronic copy to the Dropbox link or bring a paper copy to the class. Electronic copy of your homework can be in Text or PDF. You could also scan/pdf your handwritten work; however, do not send low-resolution or small phone-camera images.