CS 161 – Computer Security
Instructor: Tygar
22 September 2014

Homework 3

Notes

- Homework 3 is due on 29 September 2015 at 3PM.
- Please work on this homework individually – no collaboration allowed.
- Please submit this homework in PDF format.
- It is possible to answer all questions relatively briefly. Please limit your answer to each question to a page at most.
- Submit this homework using Gradescope.

Please start the answer to each question on a new page

For the following questions, please consider the elliptic curve : $y^2 = x^3 + 4x + 3$. You may use any computational tools you wish (except receiving help from another human) for the following questions. Please list any computational tools you use.

However, we recommend attempting as much of this problem set by hand as possible: you will likely have midterm questions which require you to compute similar values by hand.

1. List the points of the $E \bmod p$ for $p = 3, 5, 7, 11, 13$.
2. For each of the above cases compute the trace of Frobenius $t_p = p + 1 - (\#\text{ of points in } E)$ and verify that $|t_p| < 2\sqrt{p}$.
3. Write the addition table for $E \bmod 7$.