Math 502
Solution to Problem 3

Tuesday, April 29, 2008

Problem No. 3

A message is waiting for you at the url

`http://math.albany.edu/~hammond/maple/pvc` .

The El Gamal key for decoding it as 950. What is the content of the message?

Response

First retrieve the resource behind the url. Upon examining it, one finds an elliptic curve $e4313$, which is $y^2 = x^3 + 43x + 13$, a prime, which is 1283, and a list consisting of 34 pairs of points in the affine plane. The vector should be construed as the El Gamal encryption of 34 points on the given elliptic curve with coordinates in the field $\mathbf{Z}/1283\mathbf{Z}$.

To recover the sequence of points one computes the point x represented by a pair of points $[y, z]$ according to the formula

$$x \;=\; z - 950y$$

relative to the arithmetic of points on the curve.

In *Maple*

```
read ellc:
read pvc:
affelleq(e4313);
                                  2    3
                                 Y  = X  + 43 X + 13
numell(e4313,theprime);
                                        1319
dec := w -> addell(e4313,w[2],powell(e4313,-950,w[1],theprime),theprime):
pv := map(dec,pvc);
  pv := [[801, 1020], [975, 23], [1143, 1151], [1151, 248], [1085, 1244],
         [1013, 352], [1215, 1254], [443, 1178], [321, 486], [834, 756],
         [975, 23], [1032, 409], [1013, 352], [443, 1178], [321, 486],
         [821, 515], [1112, 1115], [1151, 248], [1013, 352], [1093, 45],
         [975, 23], [1143, 1151], [1215, 1254], [443, 1178], [321, 486],
         [975, 23], [1101, 251], [1001, 331], [321, 486], [841, 285],
         [1041, 866], [1215, 1254], [1093, 45], [1013, 352]]
```

The variable *pv* is the list of 34 points on the curve corresponding to the original encrypted list of 34 pairs of points on the curve.

The package `ellc` contains functions *encell* and *decell* for, respectively, encoding values as points on the curve and recovering values from points on the curve. These procedures are not regarded as cryptographic. For this exercise recovery is the only step required. The function *decell* takes 3 arguments: point, prime (for the field), and number of "tries". For this exercise the number of tries is 10.

```
v := map(decell,pv,theprime,10);
  v := [80, 97, 114, 115, 108, 101, 121, 44, 32, 83, 97, 103, 101, 44, 32,
        82, 111, 115, 101, 109, 97, 114, 121, 44, 32, 97, 110, 100, 32, 84,
        104, 121, 109, 101]
convert(v,bytes);
                      "Parsley, Sage, Rosemary, and Thyme"
```