Sample of challenges in home assignment 4 — Cryptography. UAM 2010-2011

1) Write the calculations to get a nontrivial factor of 4221089 using $E:\ y^2 = x^3 + x + 7$ and the starting point $P = (1,3) \in E$. <u>Note:</u> The program typed in class was specialized for $y^2 = x^3 + ax + 1$ and $P = (0,1)$ but you can still use the function for adding points.

2) Guess the secret message $\begin{array}{|c|c|c|c|c|c|c|}\hline \mathtt{L}_1 & \mathtt{L}_2 & \mathtt{L}_3 & \quad & \mathtt{L}_4 & \mathtt{L}_5 & \mathtt{L}_6 \\ \hline\end{array}$ where $\mathtt{L}_i$ is a letter with `ord(L`$_i$`)=Ai` knowing that the output of the program

```
E = EllipticCurve(GF(6091541), [0,5622139])
G = E([3353686,4066380])
Ppub = E([5894715,2653441])
k = floor( 10^6*random() )
print k*G, E([256^2*A1+256*A2+A3,256^2*A4+256*A5+A6]) + k*Ppub
```

has been:

```
(3452962 :  2418876 :  1) (1041155 :  5388088 :  1)
```