HOME ASSIGNMENT 4 CRYPTOGRAPHY. UAM 2010-2011

Deadline: May 31th

Name:

Exercises

1) Write the complete addition table of $E:\ y^2 = x^3 + x + 3$ over $\mathbb{F}_5$ without using the computer.

2) Suppose that in elliptic Diffie-Hellman key exchange with $E:\ y^2 = x^3 + 1$ over $\mathbb{F}_5$ and $G = (2, 3)$ both parties send $(0, 1)$. What is the shared key?

3) We impose in the definition of elliptic curve the condition $4a^3 + 27b^2 \neq 0$. Consider for instance $E:\ y^2 = x^3 + 2x + 2$ over $\mathbb{F}_5$ that does not fulfill this condition and show that it does not give a coherent group law.

4) Consider an elliptic curve $E:\ y = x^3 + ax + b$ over $\mathbb{Q}$ at let n_2 the number of points of order exactly 2. Prove that $n_2 \neq 2$.

5) An elliptic curve E over a finite field K contains 1089 points (including the point at infinity), $E(K) = \{P_0 = O, P_1, P_2, \ldots, P_{1088}\}$. Suppose that $P_n = nP_1$ for $1 \leq n < 1088$. How many elements are there of each order?