Homework Assignment # 9

Due Date: Monday, November 15

The file "ellc_add.c" which can be found on our web page contains a C function which performs addition on an elliptic curve together with a sample program. The function will be very useful for the programming problems of this assignment.

0. Read the article "Selecting Cryptographic Key Sizes" by Lenstra and Verheul, presented at the 3rd Workshop on Elliptic Curve Cryptosystems, November 1–3, 1999, Waterloo, Canada. This article will create quite a bit of discussion in the public-key community, as the authors claim that RSA with 1024 bits is roughly security equivalent to elliptic curve cryptosystems with 135 bits, whereas most other tables (such as the one provided in the lecture) always claimed that elliptic curves require about 160 bits for that level of security.

1. Show that the condition $4a^3 + 27b^2 \neq 0 \bmod p$ is fulfilled for the curve

$$y^2 \equiv x^3 + x + 6 \bmod 11 \qquad (1)$$

2. Perform the additions

   (a) $(2,7) + (5,2)$

   (b) $(3,6) + (3,6)$

   in the group of the curve (1). Use only a pocket calculator. You should use the program only for verification of your results.

3. Write a program which generates a list of all 13 elements in the group of points of the elliptic curve (1) from the primitive element $\delta = (5,2)$. The list should look as follows:

```
d = (5,2)
2d = ...
...
13d = ...
14d = ...
```

   Your program should generate the output `O = point of infinity` if the result of an addition is the point of infinity. Verify that $14\delta = \delta$.

4. Verify that $\delta, 2\delta, 3\delta$ are actually points on the curve.

5. (Easy) In the group of points of the specific curve (1) all elements are primitive. Why? (Hints: How many elements are in the group? What are the possible orders?) Please note that this is a great exception. In general it is not true that all elements of an elliptic curve are primitive.

6. In practice, a and k are both in the range of $p \approx 2^{150} \cdots 2^{250}$. Obviously computing $\beta = a \cdot \alpha$ and $y_0 = k \cdot \alpha$ can not be done in a straightforward manner, i.e. we can not perform a (or k) additions of the form $\alpha + \alpha + \alpha + \cdots + \alpha$.

   Luckily, the square-and-multiply algorithm can directly be adopted to the problem here. The new "double-and-add" algorithm relies entirely on the two operations doubling and addition.

   (a) Provide a pseudo-code description of the new algorithm similar to the one we introduced in the lecture for the operation $a \cdot \alpha$. Assume there is a function `ellc_add` and a function `ellc_double` which performs adding and doubling of points, respectively.

   (b) Illustrate how the algorithm works for $a = 19$ and for $a = 160$. Do *not* perform elliptic curve operations, but keep α a variable.

   (c) How many (i) point additions and (ii) point doublings are required on average for one "multiplication"? Assume that all integers have $n = \lceil \log_2 p \rceil$ bits.

   (d) Assume that all integers have $n = 160$ bits, i.e., p is a 160 bit prime. Assume one group operation (addition or doubling) requires 20 μsec. What is the time for one double-and-add operation? What is the data throughput in bits/sec if the Menezes-Vanstone encryption scheme is being used?

7. Let E be the elliptic curve $y^2 = x^3 + x + 13$ defined over Z_{31}. It can be shown that $\#E = 34$ and that $(9, 10)$ is an element of order 34 in E. The Menezes-Vanstone Cryptosystem defined on E will have as its plaintext pairs (s, t), where $s, t \in Z_{31}^{\star}$. Suppose Bob's secret "exponent" is $a = 25$.

   (a) Compute $\beta = a\alpha$.

   (b) Decrypt the following string of ciphertext:

   $$((4,9),28,7),((19,28),9,13),((5,22),20,17),((25,16),12,27)$$

   (c) Assuming that each plaintext represents two alphabetic characters, convert the plaintext into an English word. Here we will use the correspondence

   $$A \leftrightarrow 1, \ldots, Z \leftrightarrow 26$$

   since 0 is not allowed in a plaintext pair.

8. (**Mathematical problem, 20 extra points**) Derive the formula for addition on elliptic curves. That is, given the coordinates for P and Q, find the coordinates for $R = (x_3, y_3)$.

   Hint: First, find the equation of a line through the two points. Insert this equation in the elliptic curve equation. At some point you have to find the roots of a cubic polynomial $x^3 + a_2x^2 + a_1x + a_0$. If the three roots are denoted by x_0, x_1, x_2 you can use the fact that $x_0 + x_1 + x_2 = -a_2$.