Problem Set 13

Due: 9:00 a.m. on Wednesday, April 20

Instructions: Carefully read Sections 6.3 and 6.4 of the textbook. Submit your solutions to the following problems. Be sure to adhere to the expectations outlined on the sheet *Guidelines for Problem Sets*. Submit your solutions in-class or to Dr. Cooper's mailbox in the Department of Mathematics.

Exercises: From pages 361–371 of the textbook.

1. Section 6.3 #6.8, page 362
2. Let E be the elliptic curve with defining equation $y^2 = x^3 + 23x + 13$ over $\mathbb{F}_{83}$. Let $P = (24, 14) \in E(\mathbb{F}_{83})$. Use the Double-and-Add Algorithm to find $19P$.
3. Alice and Bob agree to use elliptic Diffie-Hellman key exchange with the prime $p = 2671$, elliptic curve $E : y^2 = x^3 + 171x + 853$ and point $P = (1980, 431) \in E(\mathbb{F}_{2671})$.
   (a) Alice sends Bob the point $Q_A = (2110, 543)$. Bob decides to use the secret multiplier $n_B = 9$. What point should Bob send to Alice? What is their secret shared value?
   (b) Alice and Bob decide to exchange a new piece of secret information, but this time Alice sends Bob only the x-coordinate $x_A = 2$ of her point Q_A. Bob decides to use the secret multiplier $n_B = 3$. What single number modulo p should Bob send to Alice? What is their secret shared value?
4. Section 6.4 #6.17(a), page 364

Note: You may use Maxima for tedious computations. If you do so, then please still show sufficient work. The following commands may be helpful:

- to find $a \pmod{n}$ type the command $\mathrm{mod}(a, n)$;
- to find the greatest common divisor of two positive integers a and b type the command $\gcd(a, b)$;
- to find the prime factorization of a positive integer n type the command $\mathrm{factor}(n)$;
- to find the inverse of n modulo m (where $\gcd(n, m) = 1$), type the command $\mathrm{inv\_mod}(n, m)$.