Homework for Part II (by Prof. Lin)

Deadline: 2012/11/13

Note: Please hand in this homework to OPLab 503D (Building One) by the deadline. Or hand to TA before class.

Homework: 8.11, 9.2, 10.1, 10.15 and 14.1

Reference solutions:

8.10

Only multiples of p have a factor in common with p^n, when p is prime. There are just p^{n-1} of these $\leq p^n$, so $\phi(p^n) = p^n - p^{n-1}$.

9.4

By trial and error, we determine that $p = 59$ and $q = 61$. Hence $\phi(n) = 58 \times 60 = 3480$. Then, using the extended Euclidean algorithm, we find that the multiplicative inverse of 31 modulo $\phi(n)$ is 3031.

10.2

A. By reviewing, for all $i = 1, \ldots, 12$, the value 7^i mod 13, we see that all the values 1,…,12 are generated by this sequence, and 7^{12} mod 13 = 1 mod 13, so 7 is a primitive root of 13.

B. By experimenting with different values for i, we get that 7^3 mod 13 = 5, so Alice's secret key is $X_A = 3$.

C. Using the private secret key used by Alice in the previous section, we can determine that the shared secret key is

$$K = (Y_B)^{X_A} \bmod 13 = 12^3 \bmod 13 = 12$$

10.14

We follow the rules of addition described in Section 10.3. To compute 2G = (2, 7) + (2, 7), we first compute

$$\lambda = (3 \times 2^2 + 1)/(2 \times 7) \bmod 11$$
$$= 13/14 \bmod 11 = 2/3 \bmod 11 = 8$$

Then we have

$$x_3 = 8^2 - 2 - 2 \bmod 11 = 5$$
$$y_3 = 8(2 - 5) - 7 \bmod 11 = 2$$
$$2G = (5, 2)$$

Similarly, 3G = 2G + G, and so on. The result:

2G = (5, 2)	3G = (8, 3)	4G = (10, 2)	5G = (3, 6)
6G = (7, 9)	7G = (7, 2)	8G = (3, 5)	9G = (10, 9)
10G = (8, 8)	11G = (5, 9)	12G = (2, 4)	13G = (2, 7)