## Homework for Part II (by Prof. Lin)

Deadline: 2011/11/13
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 $\mathrm{p}^{\mathrm{n}-1}$ of these $\leq \mathrm{p}^{\mathrm{n}}$, so $\phi\left(\mathrm{p}^{\mathrm{n}}\right)=\mathrm{p}^{\mathrm{n}}-\mathrm{p}^{\mathrm{n}-1}$.

## 9.4

By trail 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 $7^{i} \bmod 13$, we see that all the values $1, \ldots, 12$ are generated by this sequence, and $7^{12} \bmod 13=1 \bmod 13$, so 7 is a primitive root of 13 .
B. By experimenting with different values for $i$, we get that $7^{3} \bmod 13=5$, 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

$$
K=\left(Y_{B}\right)^{X_{A}} \bmod 13=12^{3} \bmod 13=12
$$

### 10.14

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

$$
\begin{aligned}
\lambda & =\left(3 \times 2^{2}+1\right) /(2 \times 7) \bmod 11 \\
& =13 / 14 \bmod 11=2 / 3 \bmod 11=8
\end{aligned}
$$

Then we have

$$
\begin{aligned}
& x_{3}=8^{2}-2-2 \bmod 11=5 \\
& y_{3}=8(2-5)-7 \bmod 11=2 \\
& 2 G=(5,2)
\end{aligned}
$$

Similarly, $3 \mathrm{G}=2 \mathrm{G}+\mathrm{G}$, and so on. The result:

| $2 \mathrm{G}=(5,2)$ | $3 \mathrm{G}=(8,3)$ | $4 \mathrm{G}=(10,2)$ | $5 \mathrm{G}=(3,6)$ |
| :---: | :---: | :---: | :---: |
| $6 \mathrm{G}=(7,9)$ | $7 \mathrm{G}=(7,2)$ | $8 \mathrm{G}=(3,5)$ | $9 \mathrm{G}=(10,9)$ |
| $10 \mathrm{G}=(8,8)$ | $11 \mathrm{G}=(5,9)$ | $12 \mathrm{G}=(2,4)$ | $13 \mathrm{G}=(2,7)$ |

