**Homework 2**
**Deadline: 2010/11/23**
**Note:** Please hand in this homework to OPLab 503D by deadline. Or hand to TA before class.
**Homework:** 8.2, 8.10, 8.20, 9.2, 10.1, 10.15
**Reference solutions:**

**8.4**

Fermat's theorem states that if $p$ is prime and $a$ is a positive integer not divisible by $p$, then $a^{p-1}$   1 (mod $p$). Therefore $5^{10}$   1 (mod 11). So we get $5^{301} = (5^{10})^{30} \bullet 5$   5 (mod 11).

**8.21**

**a.** x = 2, 27 (mod 29)
**b.** x = 9, 24 (mod 29)
**c.** x = 8, 10, 12, 15, 18, 26, 27 (mod 29)

**9.3**

$M$=2.
To show this, note that we know that $n$ = 33, which has only two prime dividers. Therefore, $p$ = 3 and $q$ = 11. $\varphi(n)$ = 2 x 10 = 20. Using the Extended Euclidean Algorithm, $d$, the multiplicative inverse of $e$ mod $\varphi(n)$ = 11 mod 20, is found to be 17. Therefore, we can determine $M$ to be
$M = C^d \bmod n = 8^{17} \bmod 33 = 2$.

**10.2**

**a.** By reviewing, for all $i$ = 1, ..., 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
$K = (Y_B)^{Y_A} \bmod 13 = 12^3 \bmod 13 = 12$

**10.14**

We follow the rules of addition described in Section 10.3. To compute 2G = (2, 7) + (2, 7), we first compute
= $(3 \bullet 2^2 + 1)/(2 \bullet 7)$ mod 11 = 13/14 mod 11 = 2/3 mod 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) |