CHAPTER 9

PUBLIC-KEY CRYPTOGRAPHY AND RSA

9.3 5

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 modulu $\phi(n)$ is 3031.

CHAPTER 10
KEY MANAGEMENT; OTHER PUBLIC-KEY CRYPTOSYSTEMS

10.2 **a.** $\phi(11) = 10$

$2^{10} = 1024 = 1 \bmod 11$

If you check 2^n for $n < 10$, you will find that none of the values is 1 mod 11.

b. 6, because $2^6 \bmod 11 = 9$

c. $K = 3^6 \bmod 11 = 3$

10.13

x	$(x^3 + x + 6) \bmod 11$	square roots mod p?	y
0	6	no	
1	8	no	
2	5	yes	4, 7
3	3	yes	5, 6
4	8	no	
5	4	yes	2, 9
6	8	no	
7	4	yes	2, 9
8	9	yes	3, 8
9	7	no	
10	4	yes	2, 9

10.15 We follow the rules of addition described in Section 10.4. To compute 2G = (2, 7) + (2, 7), we first compute

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

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)