1 Short Answer Solutions:

1. (a) Choose e and d such that $\gcd(e, \phi(n)) = 1$ and $ed = 1 \pmod{\phi(n)}$. Encryption is $c = m^e \pmod{n}$ and decryption is $m = c^d \pmod{n} = m^{ed}$. Due to Euler’s Theorem and the fact $ed = 1 \pmod{(p-1)(q-1)}$ we have $m^{ed} = m \pmod{n}$.

(b) p and q should be chosen randomly, of large size, and such that p and q are not too close in size, e.g. $p > 2q$. If they are too close, then techniques like Fermat Factorization facilitate easier factoring of n, which would make it easy for an adversary to calculate d.

2. Choose $x_1$ and $x_2$ as input and calculate $y_1 = ax_1 + b \pmod{n}$ and $y_2 = ax_2 + b$. Now set up a system of 2 equations and 2 unknowns and solve. An easy choice of $x_1 = 0$ makes this fairly simple.

3. Look at Figure 4.1 on pg 99 of the book, and see the explanation for L’s, R’s, and K’s.

2 Quick Calculation Solutions

1. $n = 143$ so $n = 11 \cdot 13$. Hence $\phi(n) = 10 \cdot 12 = 120$. We need to find d such that $7d = 1 \pmod{120}$. Divide 120 by 7 to get $120 - 7 \cdot 17 = 1$. Hence, mod 120 we have $7 \cdot (-17) = 1 \pmod{120}$ and so $d = -17 = 103 \pmod{120}$.

2. This problem tanked– the notation was ambiguous. Basically, whether you interpreted it as $((2^3)^2)^3$ or $2^{3(2^3)}$ or even $2^{233}$, what you would have worked it down to something of the form $2^x$ where x needed to be considered mod $\phi(1000) = 400$. Unfortunately, there were many interpretations of this problem, so I cancelled it and gave full credit to everyone.

3. Observe $(a + b)^p = (a + b) \pmod{p}$ by Fermat’s Little Theorem. Also observe that $a^p = a \pmod{p}$ and $b^p = b \pmod{p}$, so $a + b = a^p + b^p \pmod{p}$. Hence $(a + b)^p = a^p + b^p \pmod{p}$.

4. Yes, this was meant to be free points. $x \oplus y = 111111$.

3 Challenge Question Solution

1. (a). Just plug in. $c_2 = (m_1 + 1)^3 = m_1^3 + 3m_1^2 + 3m_1 + 1$. The fraction becomes

$$\frac{(m_1^3 + 3m_1^2 + 3m_1 + 1) + 2m_1^3 - 1}{(m_1^3 + 3m_1^2 + 3m_1 + 1) - m_1^3 + 2} = \frac{3m_1^3 + 3m_1^2 + 3m_1}{3m_1^2 + 3m_1 + 3}.$$

Factor out $m_1$ and cancel.

(b). This one’s trickier. The idea is that by plugging in on part (a), you will have seen the basic tricks needed. Again, calculate

$$c_2 = (am_1 + b)^3 = a^3m_1^3 + 3a^2m_1^2b + 3ab^2m_1 + b^3 \pmod{n}.$$

You will need this, so keep it handy. Look at the denominator from part (a). Notice that we needed some way to cancel the $m_1^3$ part. Well in $c_2$ the $m_1^3$ component is $a^3m_1^3$ so we need to subtract off $a^3c_1$. Our denominator will look like $? (c_2 - a^3c_1 + ?)$ where we have to fill in the ‘?’s. Now switch to the numerator. Since the denominator will have a $3a^2m_1^2b$ term in it, we know that we need a leading 3 for the $a^3m_1^3b$ term in the numerator. To get this we can do $b(c_2 + 2a^3c_1 - ?)$. The ? in the numerator is easily solved for by realizing that we need to get rid of the $b^3$ in order for things to cancel nicely. Hence the numerator is $b(c_2 + 2a^3c_1 - b^3)$. Now, back to the denominator. Using the numerator expression
that we have calculated, we see that we need the denominator to be $a(c_2 - a^3c_1 + 2b^3)$. Hence, to solve for $m_1$ we calculate:

$$\frac{b(c_2 + 2a^3c_1 - b^3)}{a(c_2 - a^3c_1 + 2b^3)} = m_1 \pmod{n}.$$