Question 1

31531 is maybe prime

520482 is composite

Factor found: 6

485827 is maybe prime

15485863 is maybe prime

Question 2

(20,14)

$$14^2 = 20^3 + 9(20) + 17 \; mod \; 23$$

$$196 \; mod \; 23 = 8000 + 180 + 17 \; mod \; 23$$

$$12 \neq 9$$

(20,14) is not on the EC

(19,20)

$$20^2 = 19^3 + 9(19) + 17 \; mod \; 23$$

$$400 \; mod \; 23 = 6859 + 171 + 17 \; mod \; 23$$

$$9 = 9$$

(19,20) is on the EC

(4,5)

$$5^2 = 4^3 + 9(4) + 17 \; mod \; 23$$

$$25 \; mod \; 23 = 64 + 36 + 17 \; mod \; 23$$

$$2 = 2$$

(4,5) is on the EC

$$8P = (12,17)$$

$$9P = 8P + P = (12,17) + (16,5)$$

$$m = \frac{5 - 17}{16 - 12} = -3$$

$$x_3 = 9 - 12 - 16 = 4$$

$$y_3 = -(-3)(4) - 17 + (-3)(12) = 5$$

$$9P = Q = (4,5)$$

Question 3

Find 2P

$$\frac{dy}{dx} = \frac{3x^2 - 36}{2y}$$

$$\frac{dy}{dx}@P = \frac{3}{76}$$

$$x_3 = (\frac{dy}{dx})^2 - x_1 - x_2 = \left(\frac{3}{76}\right)^2 + 3.5 + 3.5 = 7.002$$

$$y_3 = \left(\frac{dy}{dx}\right)(x_1 - x_3) - y_1 = \left(\frac{3}{76}\right)(-3.5 - 7.002) - 9.5 = -9.915$$

$$2P = (7.002, -9.915)$$

Find P+Q

$$m = \frac{8.5 - 9.5}{-2.5 + 3.5} = -1$$

$$x_3 = 1 + 3.5 + 2.5 = 7$$

$$y_3 = -1(-3.5 - 7) - 9.5 = 1$$

$$P + Q = (7,1)$$

Question 4

a. Suppose Alice and Bob both have the same plaintexts A and B. Then Alice chooses one plaintext at random and encrypts it using Charlie's public key, then sends it to Charlie. If Bob was to intercept this message, he could encrypt A and B with Charlie's public key and compare them to Alice's ciphertext. Since RSA is deterministic, Alice's ciphertext should match one of Bob's ciphertexts, and Bob would know which message Alice sent.
b. In order to make RSA semantically secure, some randomness needs to be added so that it is not deterministic. One way to do this is for Alice to pad her plaintext message with some amount of random string. This solves the problem that Bob could easily guess what the plaintext would be and choose plaintexts to compare.