Q1. (a) In a cryptographic hash function, what is a preimage attack?
(b) What characteristics are needed to make a hash function secure against preimage attacks?
(c) Consider the following hash function
H: $\{0, 1, \ldots. 2^{2048} - 1\} \rightarrow \{0, 1, \ldots. 2^{256} - 1\}$ that satisfy the property $x1 \equiv x2 \pmod{2^{32}} \Rightarrow h(x1) = h(x2)$
How many different values H can produce?
(d) Let Y be a uniformly distributed random element of $\{0, 1, \ldots. 2^{256} - 1\}$. Compute an upper bound on the probability that Y has a preimage.
(e) Given a value $y = h(x)$, show how to take the advantage of the above property in order to find a preimage of y. Compute the worst-case complexity of this algorithm.
(f) Is the above property useful for performing a second preimage attack? Explain your answer.
(g) Is the above property useful for finding a collision? Explain your answer. [7 x 5 = 35]

Q2. (a) What is an elliptic curve?
(b) What is the "zero point" of an elliptic curve?
(c) Consider the elliptic curve $E_{11}(1,6)$; that is the curve is defined by $y^2 = x^3 + x + 6$ with a modulus of $p = 11$. Determine all the points in $E_{11}(1,6)$.
(d) For $E_{11}(1,6)$, consider the point $P = (2,7)$. Compute (i) 2P and (ii) 3P.
(e) In general, how many tangents can be drawn to E from a point P? [5 x 5 = 25]