CSS322 – Quiz 4

Name: _____

ID: _____   Mark: _____ (out of 10)

Question 1 [2 marks]

Calculate the following:

    a) $\Phi(24)$

    b) $\Phi(19)$

    c) $\Phi(323)$

Question 2 [2 marks]

Derive (or manually calculate) the answer to: $19^8 (mod\ 24)$

Question 3 [4 marks]

Using RSA, encrypt the message $M = 3$, assuming the two primes chosen to generate the keys are $p = 13$ and $q = 7$. You should choose a value $e < 10$. Show your calculations and assumptions.

Question 4 [2 marks]

If Alice used the RSA algorithm in Question 3 to send the message M = 3 to Bob so that Charlie could not read the message, then:

a) Do you know Alice's public key? If yes, what is it? [1 mark]

b) Do you know Bob's public key? If yes, what is it? [1 mark]

Bonus Question [Bonus 2 marks]

Assuming brute force attack on the keys is not possible, show the calculations that Charlie would need to perform to break the cipher from Questions 3 and 4.