# CSS 322 – QUIZ 4

First name: _____ Last name: _____

ID: _____ Total Marks: _____
out of 10

- Write your name and ID in the space provided at the top of the sheet.
- Answer the questions on this sheet(s) only, using the space given.

**Question 1** [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 2** [4 marks]

If Alice used the RSA algorithm in Question 1 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?

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

c) Assuming a brute force attack is not possible, explain the steps that Charlie could take to break the encrypted message. (You do not need to perform the calculations, you just need to say what Charlie needs to calculate and why).

d) Although breaking RSA in this example with the steps from part (c) is possible, in general, why is RSA hard to break?

**Question 3** [2 marks]

In the above questions, if a central Certificate Authority is used, then what is its purpose? (That is, what does the Certificate Authority do).

**Bonus Question** [Bonus 3 marks]

Show the calculations to break the cipher from Question 2(c).