CSS322 – Quiz 4

Name: ____

ID: ____________________________ Mark: __________ (out of 10)

Question 1 [5 marks]

There are 4 users in a network: *Napat*, *Jira*, *Apiwat*, *Funtida*. Each user has their own pair of public/private keys: PU_{user} and PR_{user} (e.g. PU_{Napat} and PR_{Napat}). Using a public key algorithm, the encrypt and decrypt operations performed with a particular *key* can be written as: $C = \mathrm{E}_{key}(P)$ and $P = \mathrm{D}_{key}(C)$. Answer the following questions assuming all appropriate keys have been generated and distributed. Use the notation for keys and encrypt/decrypt as given above.

a) List all the keys known (or that can be easily obtained) by Napat. [2 marks]

b) If Napat wants to send a confidential message M to Jira, then write the operation the sender performs on M. [2 marks]

c) What key is used by the recipient to decrypt the received message? [1 mark]

Question 2 [5 marks]

Using RSA, encrypt the message $M = 4$, assuming the two primes chosen to generate the keys are $p = 13$ and $q = 7$. You should choose the smallest possible $e > 1$. Show your calculations and assumptions.