

## 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:  $C = E_{key}(P)$  and  $P = D_{key}(C)$ . Answer the following questions assuming all appropriate keys have been generated and distributed. Use the notation for keys and encrypt/decrypt as given above.

- List all the keys known (or that can be easily obtained) by *Apiwat*. [2 marks]
- If *Napat* wants to send a authenticated message  $M$  to *Funtida*, then write the operation the sender performs on  $M$ . [2 marks]
- What key is used by the recipient to decrypt the received message? [1 mark]

### Question 2 [5 marks]

Using RSA, encrypt the message  $M = 6$ , assuming the two primes chosen to generate the keys are  $p = 17$  and  $q = 5$ . You should choose the smallest possible  $e > 1$ . Show your calculations and assumptions.