

Family Name:	Student ID: - - - - - - - -											
Given Name:												
Tutorial:	Wed	Thur	Fri									
	10am	10:30am	11am	11:30am	12:30am	1pm	2pm	2:30pm	3pm	3:30pm	4pm	
	4:30pm	5pm										
Tutor:	Cahit	Jerry	Jie	Murray	Roumani	Sherwin	Tim	Tom				

37181 DISCRETE MATHEMATICS LEARNING PROGRESS CHECK 9

©MURRAY ELDER, UTS AUTUMN 2022

INSTRUCTIONS. 40-60 minutes.

Upload **as a single PDF file** on Canvas/Assignments/LPC9 before 7:59pm Tuesday 10 May 2022. Name your file as `LPC9-LastName-StudentID.pdf`. Show all relevant working and steps. You may use the powermod website mentioned in worksheet 10 to speed up your RSA calculations. You may refer to your personal class notes, and a basic (non-programmable) calculator. Work on this on your own, do not discuss with anyone or using Discord/WeChat/Whatsapp/any websites including paid homework sites. Questions 3–4 refer to Alice’s page published on the 37181-Autumn-2022 Canvas site.

- (1 mark) Draw the graphs which have the given degree sequence, or explain why no such graph exists.

(a) 2, 2, 1, 1, 1
(b) 2, 2, 2, 1, 1

2. (1 mark) Draw a graph which has the following adjacency matrix, or explain why no such graph exists.

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

3. (1 mark) Let e be the number published on Alice's page on the 37181 Canvas site.

(a) Compute $\gcd(17220, e)$ using the Euclidean algorithm. Show all steps.

(b) Find $d \in \mathbb{Z}_{17220}$ such that $e \cdot d \equiv 1 \pmod{17220}$

4. (2 marks) Alice has published n, e on her page on the 37181 Canvas site.

(a) Bob wishes to send $m = 27$ to Alice using the RSA protocol. What encoded number c does Bob send to Alice?

(b) Alice computes $\varphi(n)$. What number does she get?

(c) Bob has sent $c = d_3d_4d_5$ where $d_1d_2d_3d_4d_5d_6d_7d_8$ is your student ID number to Alice using the RSA protocol. ¹ What number m did Bob encode and send to Alice?

END OF LPC9

¹For example, if my student ID number is 43018065, then $d_3d_4d_5 = 018 = 18$, and if my student ID number is 43218765, then $d_3d_4d_5 = 218$.