GRIFFITH COLLEGE

Course	MSCC
Module title	Information Security
Tutorial No.	2
Minimum Word Count	n/a
Issue Date	07/04/2025
Due Date	14/04/2025 @ 9.00 am
	Late submissions • possible up to 17.04.2025 @ 9am • penalised at a rate of 10% per day (or part thereof)

Important: Please Read

Tutorials are an important aid to learning.

All content should be your own work, copying and pasting content (*or AI generated content*) is NOT PERMITTED, and you will not receive a grade if you do so.

For problem-based questions, you must include all workings (step-by-step) in your solution.

Tutorial submissions should be:

1. Well written
2. Properly structured
3. Use citations and references where appropriate
4. Include a cover page and a cover sheet
5. YOUR OWN WORK!
6. ALL WORK WILL BE CHECKED FOR **PLAGIARISM**!

Tutorial 2 Questions

Q1	Explain how to generate a pair of RSA encryption keys given two prime numbers, p = 11 and q = 3.
Q2	Find out the secret key that Alice and Bob will share using the Diffie-Hellman key exchange when they start with: g=7 and n = 11. Alice generates a=3 and Bob generates b= 5 as their initial secret prime numbers.
Q3	With the help of a diagram, describe in detail how a Certification Authority can be used to provide a secure communication
Q4	What is a public key certificate? And what information does it contain?