GRIFFITH COLLEGE

Course	MSCC
Module title	Information Security
Tutorial No.	1
Minimum Word Count	n/a
Issue Date	10/03/2025
Due Date	17/03/2025 @ 9.00 am
	Late submissions • possible up to 20.03.2025 @ 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 1 Questions

Q1 (i) Find the 26 modular key matrix and its modular inverse matrix for the following matrix A.

$$A = \begin{matrix} 7 & 11 \\ -16 & 3 \end{matrix}$$

ii) Then use the modular inverse matrix to decipher the ciphered message "ZMTV". Show your work.

Q2 Given the following S-Box table as used in the DES algorithm, find the output produced for each of the following binary input values:

a) 110000 b) 100001 c) 011110
d) 000111 e) 111111 f) 111110

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Q3 State five advantages of public key encryption systems over conventional encryption systems.

Q4 Analyse the reasons why DES encryption uses a set of eight transformation S-boxes?

Q5 Using the regular Column Transposition Cipher, use the keyword "**DUSTED**" and show steps involved in how to decipher the following ciphered message:

"**TYISW UOLWI OONGN EMNYW NERDN NNHOU OKGOI HTSII KT**"