# Assignment/Tutorial/Practical Report Cover Sheet

|  |  |  |
| --- | --- | --- |
| Student’s Name | Matric Number | Signature |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Sharifah Amiza Binti Wan Wahab | 72848 | Miza |
| Sharifah Anira Binti Wan Wahab | 72663 | Nira |

|  |  |
| --- | --- |
| Group Name | NCY2\_07 |
| Subject Code | TMN2073 |
| Subject Name | Computer Security |
| Assignment/Tutorial/Practical Number of Title: | Tutorial 1 |
| Name of Lecturer | Dr Adnan Shahid Khan |
| Due Date | 10 April 2021 |
| Date Submitted | 10 April 2021 |

This cover sheet must be completed, signed and firmly attached to the front of the submission. All work must be submitted by the due date. If an extension of work is granted, an assignment extension acknowledgement slip must be signed by the lecturer/tutor and attached to assignment. Please note that is your responsibility to retain copies of your assignment.

|  |
| --- |
| ***Plagiarism and Collusion are methods of cheating that falls under Peraturan Akademik Universiti Malaysia Sarawak para 11: Etika Akademik***  **Plagiarism**  Plagiarism is the presentation of work which has been copied in whole or in part from another person’s work, or from any other source such as the internet, published books or periodicals without due acknowledgement given in the text.  **Collusion**  Collusion is the presentation of work that is the result in whole or in part of unauthorized collaboration with another person or persons.  Where there are reasonable grounds for believing that cheating has occurred, the only action that may be taken when plagiarism or collusion is detected is for the staff member not to mark the item of work and to report or refer the matter to the Dean. This may result in work being disallowed and given a fail grade or if the circumstances warrant, the matter may be referred to a Committee of inquiry for investigation. Such investigation may result in the matter being referred to the University Discipline Committee, **which** has the power to exclude a student. |

|  |
| --- |
| **Upon placing signature above, I certify that I have not plagiarized the work of others or participated in unauthorized collusion when preparing this assignment.**  **I also certify that I have taken proper case in safeguarding my work and have made all reasonable efforts to ensure that may work not be able to be copied.** |

|  |
| --- |
| **MARK:** |

TUTORIAL# 1

1. Refer to the attached article.

“A Lightweight Mutual Authentication and Key Agreement Scheme for Medical Internet of Thing”.

1. Answer the following question

|  |  |
| --- | --- |
| **QUESTION** | **ANSWER** |
| How do you feel that the proposed method is **mutual authentication**? |  |
| How **many factors** are involved in mutual authentication? What is the purpose of using those factors? |  |
| What is the **type of Mutual Authentication**? Refer to the slides for all different types. |  |
| Evaluate either the proposed methods is prone to **replay attack, man in the middle attack, impersonation attack or any other attack** you want to discuss. |  |
| Evaluate the proposed methods from **computation cost** and **authentication overhead.** | The proposed method from computation cost is 3904 bits in total. The communication cost between nodes SN and AP is 832 bits, AP and server is 864 bits, server and AP is 1120 bits and AP and SN is 1088 bits.  The proposed method from authentication overhead is 20 messages is transfer during the authentication process. |