GRIFFITH COLLEGE DUBLIN

COMPUTING ASSIGNMENT TITLE SHEET

Course:	M.Sc. in Computing
Stage/Year:	
Module:	Information Security
Semester:	Semester II
Assignment Number:	Assignment
Date of Title Issue:	19th Mar 2025
Assignment Deadline:	2nd April 2025 +3 days late 10 % penalty/day +3 days capped 40%
Assignment Submission:	Moodle only.
Assignment Weighting:	15%

Assignment Title

Literature Survey and Report

Research and analyze a specific topic within the field of **communication security**, focusing on a well-defined aspect rather than a broad overview. Then, compile a **detailed report** on your findings. The report should explore key elements related to the chosen topic, such as **performance, design, implementation, algorithms, comparisons, and operational aspects**, depending on its relevance.

Learning Outcomes

1. Describe the core principles and concepts of **communication security**.
2. Showcase an understanding of the **skills and tools** required to design and implement **secure communication systems**.
3. Utilize and apply key **cryptographic schemes** to enhance security.
4. Gain insights into **emerging trends and advancements** in the field of communication security.

MSc Network Security

Literature Survey and Report Assignment (15%)

Plagiarism

{{Plagiarism is to submit another person's work as your own (with or without modification of detail). It is plagiarism to allow another to take your work with the intent to misrepresent authorship. It is plagiarism to fail to take reasonable steps to protect the privacy of your work.}}

---

1. Investigation and Report Writing

i. Select and study a **specific topic** from the provided list, focusing on a **particular aspect** rather than a broad overview.
ii. Conduct a **detailed investigation** and compile a **comprehensive report** on your findings.
iii. Depending on the **relevance of the topic**, your report may cover various aspects, such as **performance, design, implementation, algorithms, comparisons, and operations**.

2. Report Formatting Guidelines

i. The report must be between **5 to 7 pages** in length when printed on **A4 paper**, using fonts between **10 and 14 points**.
ii. **Do not print the report**—it should be submitted electronically.

3. Submission Requirements

i. The report must be submitted as an **MS Word Document (.DOCX)** file.
ii. **PDF files, compressed files, or any other formats will not be accepted**.
iii. Files in the wrong format will be **discarded**, and no marks will be awarded.

4. File Naming Format

The submitted file must follow the **specific naming convention**:

```
<First Name> <Last Name> - MSCC-IS-assign - <Student Number> -
<Topic>.docx
```

Example:

```
Tom Smith - MSCC-IS-assign - 2623329 - RSA.docx
```

5. Submission Process

i. The report must be uploaded to the **module's Moodle page**.
ii. **Submissions via email will not be accepted**.
iii. If changes are required, you may **resubmit** before the deadline. However, **your previous submission will be overwritten**.
iv. **No submissions will be accepted after the deadline**.

6. First Page of the Report

i. The first page of your report must include:
ii. **A suitable title** that reflects your topic.
iii. **Your Student Number**.
iv. **Your full name**, clearly separated into **first name and last name**.
v. **The course name**, which should be:
    - *MSc in Information Security*

7. References

i. Use **recommended textbooks** for the course.
ii. Additional references may include **books, journals, research papers, or reputable websites**.
iii. Some **free online resources** include:
    - ScienceDirect
    - ERCIM News Journal
    - CiteSeer (http://citeseerx.ist.psu.edu/index)

Ensure your work adheres to these guidelines for proper evaluation.

Report Structure and Requirements

Your report must include, but is not limited to, the following **sections** and **key aspects** related to your chosen topic:

1.Abstract (10 points)

i. A brief summary outlining the **purpose** of the report.
ii. Clearly state **what the report discusses** and the key topics covered.
iii. Explain **what the reader can expect to learn** or **what question the report answers**.

2. Introduction (20 points)

i. Provide a **clear overview** of the topic.
ii. Explain its **relevance** to **networks and communications**.
iii. Describe **why this topic is important** in the field of **communication security**.

3. Detailed Discussion (20 points)

i. The **main body** of the report should provide an in-depth discussion of the **chosen topic**.
ii. Present **key concepts, methods, and analysis** relevant to the subject.
iii. Ensure that the content is **well-structured, logical, and directly related** to the topic.

4. Use of Examples, Cases, Drawings, and Diagrams (20 points)

i. Include **relevant examples, case studies, figures, and diagrams** to support explanations.
ii. Visual aids should **clarify complex ideas** and enhance understanding.
iii. Ensure that **all images, tables, and figures are properly labeled and referenced**.

5. Conclusion or Summary (10 points)

i. Summarize the **main findings** of the report.
ii. Provide a **concise closing statement** that ties the report together.
iii. If the **abstract posed a question**, briefly **answer it** in this section.

6. References (10 points)

i. List **all sources** used in the report, including:
    - **Books**
    - **Journals**
    - **Technical reports**
    - **Research papers**
    - **Reputable websites**
ii. At least **five references** are required, and proper **citation formatting** should be followed.

7. Lecturer's Evaluation (10 points)

i. The **lecturer will assess the overall quality** of the report based on:

(a) **Clarity** of writing
(b) **Substance and depth** of the discussion
(c) **Logical organization and presentation** of ideas

Final Notes

i. Ensure the report is **well-structured** and follows a **logical flow**.
ii. Use **clear language** and avoid unnecessary complexity.
iii. Proper formatting, citation, and **proofreading** are essential for a high-quality submission.

By following this structure, your report will be **comprehensive, well-organized, and aligned with the assessment criteria**.

List of suggested topics

01) Data Encryption Standard (DES)		02) Advanced Encryption Standard (AES)
03) Public Key Encryption		04) Hash Functions
05) Key management		06) Authentication
07) Digital Signatures		08) Public key Certification
09) IP Security		10) Security attacks
11) Diffie hillman		12) Security of Wireless networks
13) RSA encryption		14) Any of the Security standards.
15) Elliptic curve digital signature algo (ECDSA)		16) Blowfish encryption.
17) Password management		18) System penetration & prevention.
19) Message Authentication Code (MAC)		20) Security of Hash functions.
21) Key distribution (Public key systems)		22) Key distribution (conventional systems)
23) Kerberos		24) Pretty Good Privacy (PGP).
25) Certificate Revocation and Trust models		26) Password management
27) Secure Shell (SSH)		28) Secure Sockets Layer (SSL)
29) IPSec Protocol		30) Hyper-Text Transfer Protocol Secure HTTPS
31) Wire Equivalent Privacy WEP, WEP2		32) Wi-Fi Protected Access (WPA)
33) Security vulnerabilities in Windows		34) Security vulnerabilities in Unix/Linux
35) Simple Certificate Enrollment Proto (SCEP)		36) Various attacks
37) Man-in-the-Middle (MITM) Attacks		38) Denial-of-Service (DoS) and Distributed DoS (DDoS) Attacks
39) Zero-Day Exploits and Countermeasures		40) Blockchain and Its Impact on Communication Security
41) Security of Internet of Things (IoT)		42) Smartphone and Mobile Security Threats
43) AI in Cybersecurity & Threat Detection		44) Digital Forensics & Incident Response