a.r.u.

Module Definition Form (MDF)

Module code: MOD003264	**Version:** 11 **Date Amended:** 27/Nov/2025

1. Module Title
Digital Security

2a. Module Leader
Nouman Nafees

2b. School
School of Computing and Information Sciences

2c. Faculty
Faculty of Science and Engineering

3a. Level
5

3b. Module Type
Standard (fine graded)

4a. Credits
15

4b. Study Hours
150

5. Restrictions

Type	**Module Code**	**Module Name**	**Condition**
Pre-requisites:	None		
Co-requisites:	None		
Exclusions:	None		
Courses to which this module is restricted:			

LEARNING, TEACHING AND ASSESSMENT INFORMATION

6a. Module Description

Digital security is a fundamental pillar of modern cybersecurity, providing the foundation for protecting data, networks and systems against rapidly evolving threat landscape. This module provides you with a solid technical foundation in the principles and practices of securing digital environments. It offers both conceptual clarity and applied perspectives that reflect contemporary industry expectations.

You'll develop an understanding of cryptographic mechanisms, secure communication protocols and threat mitigation techniques, exploring how these elements interact to protect critical assets and infrastructure. The module places a strong emphasis on practical security implementation, threat identification and incident response, ensuring that learners build both analytical and operational capabilities relevant to real-world security operations.

More importantly, the module considers the broader ethical, legal and regulatory frameworks that support digital security, preparing you to operate responsibly and professionally in diverse cybersecurity contexts.

By the end of this module, you'll be equipped with the essential knowledge and practical skills required to pursue roles in cybersecurity and information assurance, or progress to more advanced security-focused modules and professional certifications.

6b. Outline Content

- Digital Security Fundamentals - The legal and moral aspects of the security discipline. - Introduction to Cryptographic Principles - Symmetric and Asymmetric Encryption - Secure Hash Functions - Public Key Infrastructures and Certificate Authorities - Digital Signatures - Trusted Computing and Anonymous Systems - Securing Web Servers and Web Applications

6c. Key Texts/Literature

The reading list to support this module is available at: https://readinglists.aru.ac.uk/

6d. Specialist Learning Resources

Students will be given access to the on-line VLE resources and forensic based lab resources

7. Learning Outcomes (threshold standards)		
No.	**Type**	**On successful completion of this module the student will be expected to be able to:**
1	Knowledge and Understanding	Compare and contrast the use of cryptographic techniques for ensuring the confidentiality, integrity and availability of user data whether in transit, processing or storage.
2	Knowledge and Understanding	Critically analyse and appraise both the use of and application of cryptographic techniques that should be applied in certain case study scenarios such as trusted computing.
3	Intellectual, practical, affective and transferrable skills	Demonstrate how digital data security can be achieved in given scenario so that the principles of security are maintained.
4	Intellectual, practical, affective and transferrable skills	Configure and implement key digital security techniques to protect web servers and web applications from common vulnerabilities and security issues.

8a. Module Occurrence to which this MDF Refers				
Year	**Occurrence**	**Period**	**Location**	**Mode of Delivery**
2025/6	ZZF	Template For Face To Face Learning Delivery		Face to Face

8b. Learning Activities for the above Module Occurrence			
Learning Activities	**Hours**	**Learning Outcomes**	**Details of Duration, frequency and other comments**
Lectures	12	1, 2	Lecture 1 hr x 12 weeks
Other teacher managed learning	24	3, 4	Laboratory 2 hr x 12 weeks
Student managed learning	114	1 - 4	Background reading of course texts and completing lab logbook
TOTAL:	150		

9. Assessment for the above Module Occurrence					
Assessment No.	**Assessment Method**	**Learning Outcomes**	**Weighting (%)**	**Fine Grade or Pass/Fail**	**Qualifying Mark (%)**
010	Coursework	1-4	60 (%)	Fine Grade	30 (%)
ASSIGNMENT - 2000 WORDS					
Assessment No.	**Assessment Method**	**Learning Outcomes**	**Weighting (%)**	**Fine Grade or Pass/Fail**	**Qualifying Mark (%)**
011	Coursework	1-4	40 (%)	Fine Grade	30 (%)
IN-CLASS TEST – 1000 WORDS					

In order to pass this module, students are required to achieve an overall mark of 40% (for modules at levels 3, 4, 5 and 6) or 50% (for modules at level 7*).

In addition, students are required to:
(a) achieve the qualifying mark for each element of fine graded assessment as specified above
(b) pass any pass/fail elements

[* the pass mark of 50% applies for all module occurrences from the academic year 2024/25 – see Section 3a of this MDF to check the level of the module and Section 8a of this MDF to check the academic year]