Module Specification

Module Summary Information

1	**Module Title**	Cyber Security
2	**Module Credits**	20
3	**Module Level**	5
4	**Module Code**	CMP5329

5 Module Overview

Computer Scientists need to address the realities of the application of their field within an environment where cyber security threats present unique challenges to application and system developers, in relation to the requirement for secure design and operation. This module provides a foundation for security consideration as required in the design of software expected to perform within a networked and data sharing environment. This module has been designed to provide the necessary theoretical framework, foundations and practical support for effectively pursuing security solutions with reference to the requirement for secure application development.

This is underpinned by providing an understanding of software-based access control mechanisms, systems and frameworks, symmetric and asymmetric cryptography, cryptographic hash functions, use of network firewalls, application gateways and virtual private networks, financial and reputation based security, relevant computer law and standards and their respective roles in realising security solutions. This module also covers attack methods including trojans, worms, viruses, cross site scripting (XSS) and request forwarding (CSRF), buffer overflow and SQL injection and side-channel software attacks. This module provides practical skills through the use and study of appropriate security programs, attack simulation and testing.

This module will be delivered through lectures and security practical exercises and tutor led class discussion.

6 Indicative Content

- Asymmetric and symmetric cryptography.
- Hash functions.
- PKI.
- Financial security models.
- Discretionary access control, mandatory access control.
- Malware.
- Firewalls.
- VPNs.
- Code injection attacks and defences.
- Security-relevant legislation and best practice frameworks.

7	Module Learning Outcomes On successful completion of the module, students will be able to:	
	1	Explain the operation of discretionary and mandatory access control systems.
	2	Examine and evaluate the application of various applied information security mechanisms (e.g. symmetric and asymmetric cryptography and cryptographically secure hash functions, digital signatures, certificates and PKI).
	3	Evaluate network and platform technical security defence and attack methodologies.
	4	Apply compliance with cyber security related legislation, best practices, and financial security models.

8	Module Assessment		
Learning Outcome			
	Coursework	Exam	In-Person
1, 2	X		
3, 4		X	

9	Breakdown Learning and Teaching Activities
Learning Activities	Hours
Scheduled Learning (SL) includes lectures, practical classes and workshops, peer group learning, Graduate+, as specified in timetable	48
Directed Learning (DL) includes work-based learning, completing practical preparation and tests, module recommended reading, as directed on VLE	80
Private Study (PS) includes preparation for exams	72
Total Study Hours:	200