Module Specification

Module Summary Information

1	**Module Title**	System Security Attacks and Defences
2	**Module Credits**	20
3	**Module Level**	5
4	**Module Code**	CMP5319

5 Module Overview

The module has been designed to provide you with the necessary theoretical framework, foundations and practical support for understanding security solutions with reference to the application of cryptography, access control and a wider range of security attack categories and defensive approaches and systems. This is underpinned by providing an understanding of the use of asymmetric cryptography for key management associated with the use of symmetric cryptography, cryptographic certificates and public key infrastructure (PKI). This module provides practical skills through the use and study of cryptographic and access control software. A theoretical underpinning is provided through a mathematical analysis of one or more public key cryptographic protocols.

These topics are considered to help provide a security foundation within courses including Forensics and Networking and Security in order to place other aspects of these courses within a structured understanding of security theory and practice.

This module will be taught using practical labs covering use of cryptographic and access control tools, and application of mathematical techniques. Lectures will be provided in order to outline the theoretical content and the relationship with practical application. Supported classes will be supplemented through student reading and completion of lab materials provided via Moodle.

6 Indicative Content

Asymmetric and symmetric cryptography, PKI, discretionary access control, mandatory access control, malware, firewalls, VPNs, code injection attacks and defences, RSA and Diffie Hellman mathematics and arithmetic, prime numbers, copyright and platform protection systems.

7	**Module Learning Outcomes** **On successful completion of the module, students will be able to:**	
	1	Describe the main classes of security attacks and how to defend against them.
	2	Explain the operation of discretionary and mandatory access control systems.
	3	Evaluate modern cryptographic techniques.
	4	Apply mathematical principles and arithmetic associated with a public key cryptography system.

8	**Module Assessment**		
Learning Outcome			
	Coursework	**Exam**	**In-Person**
1-4		**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, cryptography arithmetic exercises, as directed on VLE	80
Private Study (PS) includes preparation for exams	72
Total Study Hours:	200