Module Code	Pre-requisite Module codes	Co-Requisite Modules code(s)	ISCED Code	Subject Code	ECTS Credits	NFQ Level (CPD)#
CMPU 4044					5	8
Module Title	Security & Cryptography					

Security and Cryptography

School Responsible:	School of Computing

Module Overview:
Confidentiality, authenticity and integrity are the cornerstones of secure systems. Cryptography is indispensable to protecting information in computer systems. Students will learn inner workings of cryptographic systems and how to correctly use them in real-world applications. Further, the course will describe, critically analyze and discuss the security challenges faced by the society and the computing industry. The aims of this module are to: • Introduce the students to the cryptography and security principles • Give the students a thorough understanding of the network and application security issues • Provide them with sound knowledge of cryptography, security protocols, security audit and compliance • Provide them with an in-depth practical application of cryptography and systems security

Learning Outcomes (LO):	
On Completion of this module, the learner will be able to	
1	Describe the underlying principles of different cryptographic algorithms
2	Evaluate the effectiveness of cryptography algorithms according to well-known security requirements.
3	Recognise and justify the different scenarios of deploying cryptography algorithms.
4	Define and describe network security
5	Discuss and relate the fundamental concepts of security
6	Design and develop best practice techniques of security
7	Formulate security policy of an organisation
8	Critically analyze different aspects of security such as policies and auditing process
9	Assess security compliance of an organisation
10	Compare and contrast international and regional security standards

Module Code	Pre-requisite Module codes	Co-Requisite Modules code(s)	ISCED Code	Subject Code	ECTS Credits	NFQ Level (CPD)#
CMPU 4044					5	8
Module Title	Security & Cryptography					

11	Implement the different cryptographic algorithms

Indicative Syllabus:
Introduction to system security and cryptography. Classical Techniques, Modern Techniques, Algorithms, Confidentiality Using Conventional Encryption. Message Authentication and Hash Functions, Hash and MAC Algorithms, Integrity and Authenticity. Public-Key Cryptography, Digital Signatures and Authentication Protocols

Learning and Teaching Methods:	
The course delivery involves a combination of lectures and labs which may incorporate the use of blended learning techniques as appropriate throughout the delivery.	
Total Teaching Contact Hours	39
Total Self-Directed Learning Hours	61

Module Delivery Duration:
This module is delivered over 1 semester

Assessment		
Assessment Type	**Weighting (%)**	**LO Assessment (No.)**
Final Exam	40%	1-11
In Class Assessment	60%	1-11
Module Specific Assessment Arrangements (if applicable)		
(a) Derogations from General Assessment Regulations		
(b) Module Assessment Thresholds		

Module Code	Pre-requisite Module codes	Co-Requisite Modules code(s)	ISCED Code	Subject Code	ECTS Credits	NFQ Level (CPD)#
CMPU 4044					5	8
Module Title	Security & Cryptography					

(c) Special Repeat Assessment Arrangements	

Essential Reading

Stallings, W. (2014). Cryptography and network security: principles and practice Sixth Edition. Pearson

Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 2001.

Trappe, W., & Washington, L. C. (2006). Introduction to cryptography with coding theory. Pearson.

Forouzan, B. A., & Mukhopadhyay, D. (2011). Cryptography and Network Security. McGraw-Hill Education.

Supplemental Reading

Lee, A. (1999). Guideline for implementing cryptography in the federal government (No. NIST-SP-800-21).

National Institute of Standards and Technology Gaithersburg MD.

Shannon, C. E. (1949). Communication theory of secrecy systems. Bell system technical journal, 28(4), 656-715.

Grime, J. (2015) An Introduction to Cryptography. Enigma Project.

Version No:		**Amended By**	
Commencement Date		**Associated Programme Codes**	

# Modules that are to be offered as Stand-Alone CPD Programmes must have an NFQ level assigned

*Details of the assessment schedule should be contained in the student handbook for the programme stage.

Date of Academic Council approval ………………………….

Module Code	Pre-requisite Module codes	Co-Requisite Modules code(s)	ISCED Code	Subject Code	ECTS Credits	NFQ Level (CPD)#
CMPU 4044					5	8
Module Title	Security & Cryptography					