MODULE DESCRIPTOR

Module Title

Cryptography

Reference	CM2136	Version	1
Created	November 2023	SCQF Level	SCQF 8
Approved	April 2024	SCQF Points	15
Amended		ECTS Points	7.5

Aims of Module

This module aims to provide students with essential knowledge of cryptography, covering concepts, standards, and schemes while emphasising its crucial role in securing computer systems. It also emphasises the development of practical skills in applying cryptography and identifying potential attacks against cryptographic algorithms and protocols.

Learning Outcomes for Module

On completion of this module, students are expected to be able to:

1	Show a comprehensive understanding of cryptography fundamentals.
2	Show an understanding of practical implementations of modern crypto-systems.
3	Combine theoretical knowledge and practical skills to select known cryptographic techniques for a given scenario.
4	Report vulnerabilities in digital systems deploying cryptography.

Indicative Module Content

Essential mathematical preliminaries for cryptography, digital threats, cryptographic basic terminology, symmetric cryptosystems, block ciphers, Feistel cipher, symmetric encryption algorithms (e.g., DES and AES), public key cryptosystems (e.g. public key encryption, public key signatures), public key algorithms (e.g.RSA), authentication protocols, key agreement protocols (e.g. Diffie-Hellman, key transport, station-to-station), public-key schemes with special properties (e.g. group, ring, blind signatures, homomorphic encryption), hash functions and message digests, digital signatures, security protocols, certificates and public key infrastructures, cryptographic security models.

Module Delivery

Lectures introduce and illustrate key concepts, while practical skills are honed through a series of laboratory exercises.

Module Ref:	CM2136 v1

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	N/A
Non-Contact Hours	120	N/A
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	N/A
Actual Placement hours for professional, statutory or regulatory body		

ASSESSMENT PLAN

If a major/minor model is used and box is ticked, % weightings below are indicative only.

Component 1

Type:	Coursework	Weighting:	100%	Outcomes Assessed:	1, 2, 3, 4
Description:	Coursework consisting of both practical and theoretical elements covering all module learning outcomes.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of Component 1. An overall minimum grade of D is required to pass this module.

Module Grade	Minimum Requirements to achieve Module Grade:
A	The student needs to achieve an A in Component 1
B	The student needs to achieve a B in Component 1
C	The student needs to achieve a C in Component 1
D	The student needs to achieve a D in Component 1
E	The student needs to achieve an E in Component 1
F	The student needs to achieve an F in Component 1
NS	Non-submission of work by published deadline or non-attendance for examination

Module Requirements

Prerequisites for Module	None.
Corequisites for module	None.
Precluded Modules	None.

INDICATIVE BIBLIOGRAPHY

1	Stallings, W. (2022). Cryptography and Network Security: Principles and Practice. Pearson.
2	Aumasson, J. P. (2017). Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press.
3	Smart, N. P. (2016).?Cryptography made simple. springer publication.
4	Stinson, D. R. (2018). Cryptography: Theory and Practice. CRC Press.
5	Pachghare, V. K. (2019).?Cryptography and information security. PHI Learning Pvt. Ltd..