

Module Details	
Module Title	Applied Cryptography
Module Code	COS7052-B
Academic Year	2022/3
Credits	20
School	Department of Computer Science
FHEQ Level	FHEQ Level 7

Contact Hours	
Type	Hours
Lectures	24
Tutorials	11
Directed Study	165

Availability	
Occurrence	Location / Period
BDA	University of Bradford / Semester 1

Module Aims
To gain an understanding of the mathematical principles underlying cryptography and to be able to apply widely researched cryptographic techniques to securing network applications. To gain insight into further cryptographic primitives and protocols for information security, as well as some cryptoanalysis techniques.

Outline Syllabus
- Mathematical principles for cryptography techniques. - Types of cipher: block cipher; stream cipher. - Public key encryption. - Digital signatures, Hash functions and data integrity. - Identification and entity authentication. - Zero knowledge protocols. - Key establishment and key management.

Learning Outcomes	
Outcome Number	Description
LO1	Demonstrate an understanding of cryptographic primitives including ciphers, cryptographic hash functions and cryptographic signatures.
LO2	Demonstrate an understanding of cryptographic protocols including techniques for analysis, flaws in protocols, and techniques for attacking protocols.
LO3	Demonstrate knowledge of important techniques in security including: key exchange and management; identity authentication; data integrity and change detection.

Learning, Teaching and Assessment Strategy
Concepts, principles and theories are outlined in formal lectures and seminars. These are supported by demonstrations and by practical exercises undertaken during tutorials and as directed study. Oral feedback is given during tutorials and seminars.

Mode of Assessment			
Type	Method	Description	Weighting
Summative	Coursework - Written	Answer 2 questions testing the ability to apply a cryptographic primitive and analyse a cryptographic protocol	20%
Summative	Examination - Closed Book	Answer 3 questions drawn from topics covered in the module	80%

Reading List
To access the reading list for this module, please visit https://bradford.rl.talis.com/index.html

Please note:

This module descriptor has been published in advance of the academic year to which it applies. Every effort has been made to ensure that the information is accurate at the time of publication, but minor changes may occur given the interval between publishing and commencement of teaching. Upon commencement of the module, students will receive a handbook with further detail about the module and any changes will be discussed and/or communicated at this point.