

Module Details	
Module Title:	Foundations of Cryptography (PG)
Module Code:	COS7031-B
Academic Year:	2019-20
Credit Rating:	20
School:	Department of Computer Science
Subject Area:	Computer Science
FHEQ Level:	FHEQ Level 7 (Masters)
Pre-requisites:	
Co-requisites:	

Contact Hours	
Type	Hours
Lectures	24
Tutorials	11
Directed Study	165

Availability	
Occurrence	Location / Period
BDA	University of Bradford / Semester 1 (Sep - Jan)

Module Aims
An advanced understanding of the mathematical principles underlying cryptography and to be able to apply cryptographic techniques to securing network applications.

Outline Syllabus
Stream and block ciphers. Public key encryption. Hash functions and data integrity. Identification and entity authentication. Digital signatures. Key establishment protocols. Key management techniques. Design and analysis of cryptographic protocols.

Learning Outcomes	
1	Demonstrate an advanced understanding of the use of appropriate cryptographic primitives and protocols for securing network applications.
2	Analyse, and select from, a range of cryptographic primitives and protocols with a view to recommending appropriate cryptographic systems for securing network applications.
3	Display the ability to transfer theoretical concepts to practical applications.

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. The formal examination and coursework will assess the learning outcomes (LO1, LO2, LO3). The coursework is equivalent to 1000 words in total.

Mode of Assessment				
Type	Method	Description	Length	Weighting
Summative	Examination - closed book	Examination - closed book 2 hours	2 hours	80%
Summative	Coursework	Two questions testing the ability to apply a cryptographic primitive and analyse a cryptographic protocol.	Equivalent to 1000 words	20%

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.