UNIVERSITY of BRADFORD

Module Descriptor

Module Details	
Module Title:	Advanced Cryptography
Module Code:	COS7047-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

To gain an advanced 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 an protocols for information security, as well as some advanced cryptanalysis techniques.

Outline Syllabus

Mathematical principles for cryptography techniques. Types of cipher. Digital signatures, Hash functions and data integrity. Identification and entity authentication. Key establishment key management. Encryption and signature schemes based on advanced discrete logarithms and factoring algorithms. Multivariate cryptography & algebraic attacks. Side-channel & fault attacks.

Learning Outcomes	
1	Demonstrate an advanced understanding of cryptographic primitives and protocols, such as zero knowledge proofs of knowledge or secure multi-party computation, for securing network applications.
2	Demonstrate knowledge of advanced cryptanalysis techniques, such as the function field sieve, side-channel attacks or quantum attacks
3	Explore alternative ways to build standard primitives and protocols based on elliptic curves, lattice problems, syndrome decoding, computational group theory problems or polynomial system solving problems.

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	Closed book 2 hours	0 hours	80%
Summative	Coursework	Two questions testing the ability to apply a cryptographic primitive and analyse a cryptographic protocol	-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.