UNIVERSITY of BRADFORD

Module Descriptor

Module Details	
Module Title	Applied Cryptography
Module Code	COS7052-B
Academic Year	2023/4
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

Cryptography is vital to many aspects of modern life, such as ecommerce, using mobile devices, and safeguarding our information on social media.

The aims of this module are to gain an advanced understanding of the mathematical principles underlying cryptography; 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 advanced cryptanalysis techniques.

Outline Syllabus

Cryptography Schemes, Symmetric Cryptography, Public-Key Cryptography, Cryptographic Security Models, Cryptography protocols, Applied Cryptography Algorithms, Applied Cryptography Schemes, Applied Cryptography Protocols.

Learning Outcomes

Outcome Number	Description
LO1	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.
LO2	Demonstrate knowledge of advanced cryptanalysis techniques, such as the function field sieve, side-channel attacks or quantum attacks.
LO3	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 presented in lectures, which includes worked examples and tasks for the students to complete so they can test their understanding of the material. These are supported by tutorials, where students are free to ask any questions they may have about the material and can receive feedback on exercises they have completed, and by directed study. Extensive oral feedback is given during tutorials.

An individual coursework (20%) assesses the students? ability to apply a cryptographic primitive and analyse a cryptographic protocol. A closed book exam (80%) assesses the students? ability to apply the knowledge from the module to a variety of scenarios.

Mode of Assessment

Type	Method	Description	Weighting
Summative	Coursework - Artefact	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%
Formative		Exercises associated with each topic covered are provided to allow students to test their understanding of the material. Feedback on these exercises is provided during tutorials.	N/A

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.

https://bradford.ac.uk