UNIVERSITY of BRADFORD

Module Descriptor

Foundations of Cryptography

Module Code:	COS6007-B
Academic Year:	2018-19
Credit Rating:	20
School:	Department of Computer Science
Subject Area:	Computer Science
FHEQ Level:	FHEQ Level 6
Module Leader:	Dr David Holton

Additional Tutors:

Pre-requisites:

Co-requisites:

Contact Hours

Type	Hours
Lectures	24
Tutorials	11
Directed Study	162
Examinations DO NOT USE	3

Availability Periods

Occurrence	Location/Period
BDA	University of Bradford / Semester 2 (Feb - May)

Module Aims

To gain an 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 entry authentication. Digital signatures. Key establishment protocols. Key management techniques. Design and analysis of cryptographic protocols.

Module Learning Outcomes

On successful completion of this module, students will be able to...

1 Demonstrate an 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 will assess the learning outcomes.

Mode of Assessment

Type	Method	Description	Length	Weighting	Final Assess'
Summative	Examination - closed book	Examination - closed book	3 hours	80%	Yes
Referral	Examination - closed book	Supplementary assessment: closed book examination	3 hours	100%	No
Summative	Coursework	Ten short answer questions testing the ability to manipulate the formalisms introduced in the lecture	0 hours	20%	No

Legacy Code (if applicable)

CM-0348D

Reading List

To view Reading List, please go to **rebus:list**.