# Module Descriptor

## Module Details

| | |
|---|---|
| Module Title | Foundations of Cryptography |
| Module Code | COS6007-B |
| Academic Year | 2024/5 |
| Credits | 20 |
| School | School of Computer Science, AI and Electronics |
| FHEQ Level | FHEQ Level 6 |

## Contact Hours

| Type | Hours |
|---|---|
| Lectures | 24 |
| Tutorials | 11 |
| Directed Study | 165 |

## Availability

| Occurrence | Location / Period |
|---|---|
| BDA | University of Bradford / Semester 2 |

## Module Aims

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

This module aims to give you an understanding of the mathematical principles underlying cryptography and to be able to apply widely researched cryptographic techniques to for information security.

It will also give you an understanding of the different types of cryptographic protocols, and the ability to analyse protocols so you can understand their strengths and weaknesses, and when they may be applied.

## Outline Syllabus

Mathematical principles for cryptography. 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 |
|---|---|
| 01 | Demonstrate an understanding of cryptographic primitives including ciphers, cryptographic hash functions and cryptographic signatures |
| 02 | Demonstrate an understanding of cryptographic protocols including techniques for analysis, flaws in protocols, and techniques for attacking protocols. |
| 03 | 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 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 - Written | Two short answer questions testing the ability to apply the formalisms introduced in the lecture.1500 words length. | 20% |
| Summative | Examination - Closed Book | Three questions drawn from the topics covered in the module (2 Hrs). | 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.*