Module Specification

Number Theory and Cryptography

Version: 2023-24, v2.0, 17 May 2023

Contents

Part 1: Information

Module title: Number Theory and Cryptography

Module code: UFMFYV-15-3

Level: Level 6

For implementation from: 2023-24

UWE credit rating: 15

ECTS credit rating: 7.5

Faculty: Faculty of Environment & Technology

Department: FET Dept of Computer Sci & Creative Tech

Partner institutions: None

Field: Computer Science and Creative Technologies

Module type: Module

Pre-requisites: Graphs, Algebra and Algorithms 2022-23

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: The module provides an introduction to number theory and shows how this theory may be applied to problems in cryptography. The module thus links a classical and central part of Mathematics with solving problems that arise in many everyday applications of cryptography such as the security of online financial transactions.

Features: Not applicable

Educational aims: The aim of this module is to introduce number theory and to demonstrate powerful applications in cryptography.

Outline syllabus: Number Theory [5/6 weeks]
Divisibility and Prime Numbers
Modular Arithmetic and Congruences
Euler's Function, the Group of Units and Primitive Roots
Introduction to Quadratic Residues

Cryptography [5/6 weeks]
Overview and History
Symmetric Systems
Cryptosystems based on Number Theory (e.g., RSA, ElGamal, Diffie-Hellman)
Elliptic Curves and Applications

Part 3: Teaching and learning methods

Teaching and learning methods: The teaching and learning strategy will involve taught material that is interspersed with individual or group activities that develop understanding of the theory and of its applications. The activites will include calculations and investigations within a framework of problem-based learning. It is envisaged that a single multi-purpose room, e.g., a TEAL space, will be utilised for all the contact sessions. A part of the learning will involve the students' engaging regularly and deeply with designated texts or with other resources.

Module Learning outcomes: On successful completion of this module students will achieve the following learning outcomes.

MO1 Analyse and solve problems in cryptography using number theory and other appropriate mathematical concepts.

MO2 Define the concepts of number theory clearly, state theorems precisely, and construct rigorous proofs.

MO3 Use technology to evaluate and solve large-scale problems in cryptography.

MO4 Communicate mathematical arguments clearly and effectively, by selecting and using appropriate notation, logic, concepts and techniques.

Hours to be allocated: 150

Contact hours:

Independent study/self-guided study = 114 hours

Face-to-face learning = 36 hours

Total = 150

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://rl.talis.com/3/uwe/lists/8AB92056-8746-18BE-EF0E-A75160CBBA68.html?lang=en-GB&login=1

Part 4: Assessment

Assessment strategy: The module will be assessment by an end of module examination. The examination will contain a mixture of questions that test understanding of the underlying theoretical concepts and applications of the theory.

Some questions will involve preparation exercises such as the use of appropriate software tools to generate date or to conduct an investigation which will then be assessed in the examination.

The resit assessment will have the same format as the first sit assessment.

Assessment tasks:

Examination (First Sit)
Description: written examination (3 hours)
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3, MO4

Examination (Resit)

Description: written examination (3 hours)

Weighting: 100 %

Final assessment: Yes

Group work: No

Learning outcomes tested: MO1, MO2, MO3, MO4

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Mathematics [Sep][FT][Frenchay][3yrs] BSc (Hons) 2021-22

Mathematics {Foundation}[Sep][FT][Frenchay][4yrs] BSc (Hons) 2020-21

Mathematics [Sep][SW][Frenchay][4yrs] BSc (Hons) 2020-21

Mathematics [Sep][SW][Frenchay][4yrs] BSc (Hons) 2020-21

Mathematics {Foundation} [Sep][SW][Frenchay][5yrs] BSc (Hons) 2019-20