Module Specification

Cryptography

Version: 2023-24, v3.0, 17 Mar 2023

Contents

Part 1: Information

Module title: Cryptography

Module code: UFCFT4-15-3

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

Delivery locations: Not in use for Modules

Field: Computer Science and Creative Technologies

Module type: Module

Pre-requisites: Introduction to OO Systems Development 2023-24

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: Pre-requisites: students must take one out of UFCFC3-30-1 Introduction to OO Systems Development or UFCFF6-30-1 Programming in C

Features: Not applicable

Educational aims: See Learning Outcomes.

Outline syllabus: The syllabus includes:

Review of background mathematics: modular arithmetic, gcd algorithms, factorization algorithms, functions, pseudo random generators;

Historical ciphers: substitution, vignere & permutation ciphers, rotor machines and Enigma;

Perfect secrecy, semantic security;

Stream ciphers, block ciphers, modes of operation, symmetric and asymmetric encryption, RSA. cryptographic hash functions, data integrity and digital signatures, authenticated encryption, authenticated key exchange;

Error correcting principles. Some important codes: Hamming codes, Reed-Solomon, BCH, and Turbo codes;

Basic compression techniques: Huffman coding, LZW Compression.

Part 3: Teaching and learning methods

Teaching and learning methods: Students will learn through a combination of lectures, tutorials and practical activities in a computer laboratory with approximately one third of the contact time being devoted to each of these. Lectures will explore and illuminate the theoretical material. In the tutorials, students will have the opportunity to discuss the theory and tease out its implications for the practical work. In the practical activities, students will work in the computer labs and construct encryption and related software.

Students will also be expected to learn independently and carry out reading and directed study beyond that available within taught classes, as suggested in the table above.

Students will be given weekly practical tasks and problem sets. These weekly practical tasks are programming tasks which will be integrated into the assessed coursework. The weekly problem sets are designed to consolidate the learning and help student to check if they have fully understood the contents. These weekly problems are not formally assessed.

Contact Hours:

Activity:
Contact time: 36 hours
Assimilation and development of knowledge: 74 hours
Exam preparation: 10 hours
Coursework preparation: 30 hours
Total study time: 150 hours

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

MO1 Recognise the importance and need for coding data streams in computer science for security, error correcting, compression

MO2 Understand and manipulate the mathematical and theoretical methods on which designs are based

MO3 Implement algorithms and protocols to for particular coding schemes, recognising the need for efficiency in terms of delay, throughput, jitter, computing resources and quality of service

MO4 Use cryptographic and coding classes available in modern programming language environments, such as Java Security, to implement secure applications

MO5 Evaluate the performance of various coding schemes under application load and change configuration parameters to optimise them

MO6 Determine modern encryption techniques appropriate for a variety of applications

MO7 Explain the strategies that need to be employed whilst attempting to break a cipher

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://uwe.rl.talis.com/modules/ufcft4-15-3.html

Part 4: Assessment

Assessment strategy: The module is assessed by a 3 hour examination at the end of the teaching and also by coursework. These components of assessment are equally weighted. The exam assesses the students' understanding of the theoretical aspects of the module whereas the coursework is an opportunity for students to demonstrate their grasp of the application of these concepts to a problem in the area of cryptography.

The assessed practical work will involve at least one activity from the following list:

The construction of :
Encryption & decryption,
Error coding, and,
Compression software.

Benchmarking, performance analysis and optimisation of:
Encryption/decryption algorithms,
Error correction codes, and,
Compression coding schemes.

Attacking software to attempt the breaking of the ciphers given encrypted texts. An interesting measure of the success of both encryption and attacking software.

Assessment components:

Examination (Online) (First Sit)
Description: Online Exam (2 hours) 24-hour window
Weighting: 25 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3, MO6, MO7

Written Assignment (First Sit)
Description: Practical coursework involving, for example, the production of encryption or benchmarking software
Weighting: 75 %
Final assessment: No
Group work: No
Learning outcomes tested: MO2, MO3, MO4, MO5, MO7

Examination (Online) (Resit)
Description: Online Exam (2 hours) 24-hour window
Weighting: 25 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3, MO6, MO7

Written Assignment (Resit)
Description: Practical coursework involving, for example, the production of encryption or benchmarking software
Weighting: 75 %
Final assessment: No
Group work: No
Learning outcomes tested: MO2, MO3, MO4, MO5, MO7

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Information Technology {Top-Up} [Frenchay] BSc (Hons) 2023-24

Information Technology {Top-Up} [SHAPE] BSc (Hons) 2023-24

Information Technology {Top-Up} [SHAPE] BSc (Hons) 2023-24

Information Technology {Top-Up} [Phenikaa] BSc (Hons) 2023-24

Information Technology {Top-Up} [Frenchay] BSc (Hons) 2022-23

Information Technology {Top-Up} [SHAPE] BSc (Hons) 2022-23

Computer Science [Sep][FT][Villa][3yrs] - Not Running BSc (Hons) 2021-22

Computer Science [May][FT][Villa][3yrs] - Not Running BSc (Hons) 2021-22

Computer Science [Jan][FT][Villa][3yrs] - Not Running BSc (Hons) 2021-22

Software Engineering for Business [Sep][FT][Frenchay][3yrs] BSc (Hons) 2021-22

Cyber Security and Digital Forensics [Sep][FT][Frenchay][3yrs] BSc (Hons) 2021-22

Cyber Security and Digital Forensics [Jan][FT][NepalBrit][3yrs] BSc (Hons) 2021-22

Computing {Dual} [Aug][FT][Taylors][3yrs] - Not Running BSc (Hons) 2021-22

Computing {Dual} [Mar][FT][Taylors][3yrs] - Not Running BSc (Hons) 2021-22

Computing [Sep][FT][Frenchay][3yrs] - Not Running BSc (Hons) 2021-22

Forensic Computing and Security {Dual} [Mar][FT][Taylors][3yrs] - Not Running BSc (Hons) 2021-22

Forensic Computing and Security {Dual} [Aug][FT][Taylors][3yrs] - Not Running BSc (Hons) 2021-22

Information Technology {Dual}[Mar][FT][Taylors][3yr] BSc (Hons) 2021-22

Computer Security and Forensics {Foundation} [Feb][FT][GCET][4yrs] BSc (Hons) 2020-21

Computer Security and Forensics {Foundation} [Oct][FT][GCET][4yrs] BSc (Hons) 2020-21

Software Engineering for Business {Foundation} [Sep][FT][Frenchay][4yrs] BSc (Hons) 2020-21

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

Computing {Foundation} [Sep][FT][Frenchay][4yrs] - Not Running BSc (Hons) 2020-21

Computer Science {Foundation} [Sep][FT][Frenchay][4yrs] - Not Running BSc (Hons) 2020-21

Computer Science [Sep][SW][Frenchay][4yrs] - Not Running BSc (Hons) 2020-21

Forensic Computing and Security {Foundation} [Sep][FT][Frenchay][4yrs] - Not Running BSc (Hons) 2020-21

Forensic Computing and Security [Sep][SW][Frenchay][4yrs] - Not Running BSc (Hons) 2020-21

Cyber Security and Digital Forensics [Sep][SW][Frenchay][4yrs] BSc (Hons) 2020-21

Cyber Security and Digital Forensics {Foundation} [Sep][FT][Frenchay][4yrs] BSc (Hons) 2020-21

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

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

Forensic Computing and Security {Foundation} [Sep][SW][Frenchay][5yrs] BSc (Hons) 2019-20