Module Specification

Cryptography

Version: 2023-24, v2.0, 19 Jul 2023

Contents

Part 1: Information

Module title: Cryptography

Module code: UFCFGU-30-2

Level: Level 5

For implementation from: 2023-24

UWE credit rating: 30

ECTS credit rating: 15

Faculty: Faculty of Environment & Technology

Department: FET Dept of Computer Sci & Creative Tech

Partner institutions: None

Field:

Module type: Module

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview:

This module introduces students to the principles of cryptography and looks at practical applications, many of which are used daily. Apprentices are expected to investigate the inner workings of cryptographic systems and how to correctly use them in real-world applications. Apprentices are expected to compare and contrast the symmetric encryption methods and ciphers, public key cryptography and the security issues related to their implementation. In addition, apprentices are expected

to investigate advanced encryption protocols and their applications.

The module covers some of the mathematical principles and theory that underpin computing.

Features: Not applicable

Educational aims: Contributes to technical aspects of cyber security knowledge together with theoretical computer science underpinnings.

Outline syllabus: automata, computability and complexity

sets, relations and functions

graphs and trees

main cryptographic techniques

concepts of confidentiality, authentication, integrity and non-repudiation

e.g. symmetric, public key, secure hash, digital signing, block cipher etc.

how they are applied and to what end and their limitations

examples of badly applied or implemented cryptographic techniques

key management

key features, benefits and limitations of symmetric and public key cryptosystems

significance of entropy

Certificate authorities

the role of cryptographic techniques in a range of different systems
e.g., GSM, chip and pin, hard disk encryption, TLS, SSL, privacy enforcing

technology

practical issues introducing such into service and updating them.

Part 3: Teaching and learning methods

Teaching and learning methods: Lecture sessions cover the technical knowledge required. Practical sessions give the students the opportunity to putt the underpinning knowledge into practise and to ensure that students have absorbed and understood the key principles involved.

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

MO1 Implement and analyse algorithms.

MO2 Configure and use security technology components and key management

MO3 Analyse well-established mathematical techniques relevant to practical computing scenarios.

MO4 Research and explain how hardware and cryptographic techniques are used to protect systems.

MO5 Communicate complex cryptographic concepts in a manner appropriate to a non-expert audience.

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 135 hours

Placement = 75 hours

Face-to-face learning = 90 hours

Total = 300

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/8AC128C9-B5DE-6261-A86C-905DD2E0A3C2.html

Part 4: Assessment

Assessment strategy: This module is assessed by a combination of techniques: Completion of a portfolio based on classroom tasks and a 30 minute presentation.

A 30 minute demonstration where apprentices will show how they have chosen an appropriate algorithm and technique to solve a given requirement. They will demonstrate the solution and satisfactorily explain its operation to an audience without specialised expertise. In addition to demonstrating their grasp of the module outcomes, the demonstration will give the students the opportunity to practice their oral skills, particularly in speaking to a non-expert audience.

Students will build up a portfolio from tasks undertaken during classroom sessions. The short tasks will require some research and will require them to demonstrate their understanding of how cryptographic techniques are applied to protect systems.

The resit strategy is the same as the first sit.

Assessment tasks:

Practical Skills Assessment (First Sit)
Description: 30 minute demonstration that illustrates how a chosen cryptographic algorithm solves a given requirement.
Weighting: 50 %
Final assessment: No
Group work: No
Learning outcomes tested: MO2, MO5

Portfolio (First Sit)
Description: Portfolio of research tasks.
Weighting: 50 %
Final assessment: Yes
Group work: No

Learning outcomes tested: MO1, MO2, MO3, MO4

Practical Skills Assessment (Resit)
Description: 30 minute demonstration that illustrates how a chosen cryptographic algorithm solves a given requirement.
Weighting: 50 %
Final assessment: No
Group work: No
Learning outcomes tested: MO2, MO5

Portfolio (Resit)
Description: Portfolio of research tasks.
Weighting: 50 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security Technical Professional {Apprenticeship-GLOSCOLL} [GlosColl] BSc (Hons) 2022-23