MODULE SPECIFICATION

Part 1: Information			
Module Title	Cryptography		
Module Code	UFCFGU-30-2	Level	Level 5
For implementation from	2021-22		
UWE Credit Rating	30	ECTS Credit Rating	15
Faculty	Faculty of Environment & Technology	Field	
Department	FET Dept of Computer Sci & Creative Tech		
Module type:	Standard		

Pre-requisites	None
Excluded Combinations	None
Co- requisites	None
Module Entry 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.

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.

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.

Part 3: Assessment

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

Component A:
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.

Component B:
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.

First Sit Components	**Final Assessment**	**Element weighting**	**Description**
Practical Skills Assessment - Component A		50 %	30 minute demonstration that illustrates how a chosen cryptographic algorithm solves a given requirement.
Portfolio - Component B	✓	50 %	Portfolio of research tasks.
Resit Components	**Final Assessment**	**Element weighting**	**Description**

Practical Skills Assessment - Component A		50 %	Reworked demonstration.
Portfolio - Component B	✓	50 %	Reworked portfolio of research tasks.

Part 4: Teaching and Learning Methods

Learning Outcomes

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

Module Learning Outcomes	**Reference**
Implement and analyse algorithms.	MO1
Configure and use security technology components and key management	MO2
Analyse well-established mathematical techniques relevant to practical computing scenarios.	MO3
Research and explain how hardware and cryptographic techniques are used to protect systems.	MO4
Communicate complex cryptographic concepts in a manner appropriate to a non-expert audience.	MO5

Contact Hours

Independent Study Hours:	
Independent study/self-guided study	135
Total Independent Study Hours:	135
Placement Study Hours:	
Placement	75
Total Placement Study Hours:	75
Scheduled Learning and Teaching Hours:	
Face-to-face learning	90
Total Scheduled Learning and Teaching Hours:	90
Hours to be allocated	300
Allocated Hours	300

Reading List

The reading list for this module can be accessed via the following link:

https://rl.talis.com/3/uwe/lists/8AC128C9-B5DE-6261-A86C-905DD2E0A3C2.html

Part 5: Contributes Towards
This module contributes towards the following programmes of study: BSc (Hons) Cyber Security Technical Professional (integrated degree) BSc (Hons) 2020-21