Prifysgol **Wrecsam**
Wrexham University

Module specification

When printed this becomes an uncontrolled document. Please access the Module Directory for the most up to date version by clicking on the following link: Module directory

Module Code	COM658
Module Title	Cryptography and Defensive Systems
Level	6
Credit value	20
Faculty	FACE
HECoS Code	100376
Cost Code	GACP

Programmes in which module to be offered

Programme title	Is the module core or option for this programme
BSc (Hons) Computer Science	Core
BSc (Hons) Computer Science with Industrial Placement	Core
BSc (Hons) Cyber Security	Core
BSc (Hons) Cyber Security with Industrial Placement	Core
BSc (Hons) Software Engineering	Core
BSc (Hons) Software Engineering with Industrial Placement	Core

Pre-requisites

N/A

Breakdown of module hours

Learning and teaching hours	12 hrs
Placement tutor support	0 hrs
Supervised learning e.g. practical classes, workshops	12 hrs
Project supervision (level 6 projects and dissertation modules only)	0 hrs
Total active learning and teaching hours	**24** hrs
Placement / work based learning	0 hrs
Guided independent study	176 hrs
Module duration (total hours)	**200** hrs

For office use only	
Initial approval date	08/11/2023
With effect from date	Sept 2026

For office use only	
Date and details of revision	
Version number	1

Module aims

The module aims to provide students with a comprehensive understanding of cryptography and defensive systems. Through a combination of theoretical concepts and practical applications, students will delve into the principles and techniques behind cryptography, including encryption algorithms, cryptographic protocols, and key management. They will also explore defensive systems designed to protect sensitive information and secure communication channels. The module aims to equip students with the knowledge and skills necessary to analyse cryptographic systems, identify vulnerabilities, and implement effective defensive measures.

Module Learning Outcomes - at the end of this module, students will be able to:

1	Compare and contrast cryptographic principles, algorithms and protocols.
2	Analyse cryptographic systems and identify vulnerabilities or weaknesses in their design.
3	Evaluate the strengths and weaknesses of cryptographic algorithms and defensive systems in different scenarios.
4	Identify and critically analyse complex problems related to cryptography and defensive systems, considering various attack vectors and countermeasures
5	Effectively communicate and explain cryptographic concepts, protocols, and system designs to both technical and non-technical audiences.

Assessment

Indicative Assessment Tasks:
This section outlines the type of assessment task the student will be expected to complete as part of the module. More details will be made available in the relevant academic year module handbook.

The assessment strategy for this module adopts a portfolio-based approach, aiming to comprehensively evaluate students' knowledge, skills, and understanding of cryptography and defensive systems. Throughout the module, students will engage in regular portfolio tasks designed to reinforce, consolidate, and expand upon their learning experiences. These portfolio tasks serve as opportunities for students to demonstrate their understanding, application, and critical analysis of the concepts and skills taught in the module.

The portfolio will include diverse components aligned with the learning outcomes, such as written assignments, practical projects, problem-solving scenarios, group presentations, online quizzes, and peer review.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)
1	1,2,3,4,5	Portfolio	100%

Derogations

None

Learning and Teaching Strategies

Aligned with the principles of the Active Learning Framework (ALF), the module will incorporate a blended digital approach utilising a Virtual Learning Environment (VLE). These resources may include a range of content such as first and third-party tutorials, instructional videos, supplementary files, online activities, and other relevant materials to enhance their learning experience.

Indicative Syllabus Outline

Indicative syllabus includes topic areas that may include:

- Introduction to Cryptography
- Symmetric Key Cryptography
- Public Key Cryptography
- Hash Functions and Message Digests
- Cryptographic Protocols
- Key Management and Cryptographic System Design
- Defensive Systems
- Emerging Trends in Cryptography
- Case Studies

Indicative Bibliography:

Please note the essential reads and other indicative reading are subject to annual review and update.

Essential Reads

W. Stalling, *Cryptography and Network Security: Principles and Practice.* Pearson, 2020.

Other indicative reading

S. Nielson and C. Monson, *Practical Cryptography in Python,* APress, 2019.