University of the West of Scotland
Module Descriptor

Session: 2024/25

Title of Module: Applied Cryptography

Code: COMP11077	SCQF Level: 11 (Scottish Credit and Qualifications Framework)	Credit Points: 10	ECTS: 5 (European Credit Transfer Scheme)
School:	School of Computing, Engineering and Physical Sciences		
Module Co-ordinator:	Graham Parsonage		

Summary of Module

This module aims towards delivering a complete cryptography mechanism by advancing students from basics of cryptography to advanced authentication protocols, its verification and validation.

This module introduces the domain philosophies in cryptography protocols based on various topics such as cryptographic protocols designed and developed based on encryption or hashing techniques, PKI (public key infrastructure) mechanism, authentication protocols and schemes implemented on various domains of specialization using one-factor, two-factors, three-factors, or multifactor authentication. This module also covers a detailed cryptanalysis of authentication protocols, based on various factors like authentication threats, attacks, calculation techniques, and performance analysis. This module also covers a more validated approach towards validating various authentication protocols using security automated validating tools.

This module will work to develop a number of the key **'I am UWS' Graduate Attributes** to make those who complete this module:

Universal
- Critical Thinker
- Ethically-minded
- Research-minded

Work Ready
- Problem-Solver
- Effective Communicator
- Ambitious

Successful
- Autonomous
- Resilient
- Driven

Module Delivery Method

Face-To-Face	Blended	Fully Online
	✓	

Face-To-Face
Term used to describe the traditional classroom environment where the students and the lecturer meet synchronously in the same room for the whole provision.

Fully Online
Instruction that is solely delivered by web-based or internet-based technologies. This term is used to describe the previously used terms distance learning and e learning.

Blended
A mode of delivery of a module or a programme that involves online and face-to-face delivery of learning, teaching and assessment activities, student support and feedback. A programme may be considered "blended" if it includes a combination of face-to-face, online and blended modules. If an online programme has any compulsory face-to-face and campus elements it must be described as blended with clearly articulated delivery information to manage student expectations

Campus(es) for Module Delivery

The module will **normally** be offered on the following campuses / or by Distance/Online Learning: (Provided viable student numbers permit)

Paisley:	Ayr:	Dumfries:	Lanarkshire:	London:	Distance/Online Learning:	Other:
			✓	✓		

Term(s) for Module Delivery

(Provided viable student numbers permit).

Term 1		Term 2	✓	Term 3	

Learning Outcomes: (maximum of 5 statements)

On successful completion of this module the student will be able to:

L1. Demonstrate a critical understanding of cryptographic schemes, their development and design.

L2. Develop and implement rigorous cryptographic protocols based on varied factors of authentication.

L3. Analyse and critically validate cryptographic protocols using cryptanalysis or automated security verification and validation techniques.

Employability Skills and Personal Development Planning (PDP) Skills

SCQF Headings	During completion of this module, there will be an opportunity to achieve core skills in:
Knowledge and Understanding (K and U)	SCQF Level 11. Students will learn systematic and comprehensive knowledge cryptography. Students are expected to be familiar with the design and development of cryptographic schemes.
Practice: Applied Knowledge and Understanding	SCQF Level 11. Students will develop and implement rigorous cryptographic protocols based on varied factors of authentication.

Generic Cognitive skills	SCQF Level 11. Students will build skills to integrate information and apply knowledge from various sources including technology advances informed by research and industry.
Communication, ICT and Numeracy Skills	SCQF Level 11. Working in groups, students will develop communication skills as well as the ability to write technical reports and documentation.
Autonomy, Accountability and Working with others	SCQF Level 11. Exercise a substantial ability to work autonomously, demonstrating critical inquiry in producing quality work underpinned by rigorous investigation. Learn effectively for the purpose of continuing personal development planning through interacting with others in academic and professional bodies and organisations relevant to m-business. Demonstrate an ability to manage and work autonomously with a range of selfdirected m-business related learning resources.

Pre-requisites:	Before undertaking this module the student should have undertaken the following:	
	Module Code:	**Module Title:**
	Other:	
Co-requisites	**Module Code:**	**Module Title:**

* Indicates that module descriptor is not published.

Programme Board	Computing
Assessment Results (Pass/Fail)	No

Subject Panel	Business & Applied Computing

Learning and Teaching

The module will be delivered by means of lectures and supervised hands-on lab work. Lectures will cover the theoretical background and practical applicability in real life problems. Concepts will be introduced by posing a practical problem and working out the needed theoretical knowledge to solve them. The delivery will encourage student participation to ensure an active learning experience. Group discussions will be held to promote critical thinking and boost informed decisions on the suitability of different state-of-the-art methods. Lab exercises will help student develop their knowledge in incremental fashion using a learning-by-doing approach. This will support the development of knowledge and understanding of the topics.

Learning Activities During completion of this module, the learning activities undertaken to achieve the module learning outcomes are stated below:	Student Learning Hours (Normally totalling 200 hours): (Note: Learning hours include both contact hours and hours spent on other learning activities)
Lecture/Core Content Delivery	7
Tutorial/Synchronous Support Activity	7
Laboratory/Practical Demonstration/Workshop	14
Independent Study	72
	100 Hours Total

**Indicative Resources: (eg. Core text, journals, internet access)

The following materials form essential underpinning for the module content and ultimately for the learning outcomes:

Katz, A and Lindell, Y. (2014) 2nd Ed. Introduction to Modern Cryptography. Chapman and Hall/CRC

Jean-Philippe Aumasson. (2017) Serious Cryptography. No Starch Press

Ferguson et al. (2010) Cryptography Engineering: Design Principles and Practical Applications. Wiley

Paar, C and Pelzl, J. (2010) Understanding cryptography: a textbook for students and practitioners. Springer

(**N.B. Although reading lists should include current publications, students are advised (particularly for material marked with an asterisk*) to wait until the start of session for confirmation of the most up-to-date material)

Engagement Requirements

In line with the Academic Engagement and Attendance Procedure, Students are defined as academically engaged if they are regularly engaged with timetabled teaching sessions, course-related learning resources including those in the Library and on Moodle, and complete assessments and submit these on time.

Supplemental Information

Moderator	Althaff Mohideen
External Examiner	N Coull

Accreditation Details	
Version Number	1.05

Assessment: (also refer to Assessment Outcomes Grids below)
Practical Coursework (60%)
Project Report (40%)

(N.B. (i) **Assessment Outcomes Grids** for the module (one for each component) can be found below which clearly demonstrate how the learning outcomes of the module will be assessed.
(ii) An **indicative schedule** listing approximate times within the academic calendar when assessment is likely to feature will be provided within the Student Handbook.)

Assessment Outcome Grids (Footnote A.)

Component 1

Assessment Type (Footnote B.)	Learning Outcome (1)	Learning Outcome (2)	Learning Outcome (3)	Weighting (%) of Assessment Element	Timetabled Contact Hours
Clinical/ Fieldwork/ Practical skills assessment/ Debate/ Interview/ Viva voce/ Oral	✓	✓	✓	60	0

Component 2

Assessment Type (Footnote B.)	Learning Outcome (1)	Learning Outcome (2)	Learning Outcome (3)	Weighting (%) of Assessment Element	Timetabled Contact Hours
Dissertation/ Project report/ Thesis	✓	✓	✓	40	0
	Combined Total For All Components			100%	0 hours

Footnotes
A. Referred to within Assessment Section above
B. Identified in the Learning Outcome Section above

Note(s):
1. More than one assessment method can be used to assess individual learning outcomes.
2. Schools are responsible for determining student contact hours. Please refer to University Policy on contact hours (extract contained within section 10 of the Module Descriptor guidance note).
   This will normally be variable across Schools, dependent on Programmes &/or Professional requirements.

Equality and Diversity

This module is suitable for any student. The assessment regime will be applied flexibly so that a student who can attain the practical outcomes of the module will not be disadvantaged. When a student discloses a disability, or if a tutor is concerned about a student, the tutor in consultation with the School Enabling Support co-ordinator will agree the appropriate adjustments to be made.
UWS Equality and Diversity Policy

(N.B. Every effort will be made by the University to accommodate any equality and diversity issues brought to the attention of the School)