University of the West of Scotland
Module Descriptor

Session: 2024/25

Last modified: 19/07/24

Title of Module: Cryptography

Code: COMP09106	**SCQF Level: 9** **(Scottish Credit and Qualifications Framework)**	**Credit Points: 20**	**ECTS: 10** **(European Credit Transfer Scheme)**
School:	School of Computing, Engineering and Physical Sciences		
Module Co-ordinator:	Althaff Mohideen		

Summary of Module

This module aims to provide students with an understanding of cryptography.

The module begins by presenting a range of topics in number theory, including divisibility, Euclid’s algorithm, linear Diophantine equations, prime numbers, congruences, and primitive roots. These concepts provide the theoretical underpinning needed for the rest of the module.

Cryptography is introduced and its historical significance is discussed. A range of cryptographic systems are then presented, in largely chronological order. These include the Ceasar shift, the Vigenere cipher, the Vernam cipher, the Hill cipher, the exponentiation cipher, the public key cryptosystems known as RSA and ElGamal, and the Merkle-Hellman cryptosystem. The Advanced Encryption Standard and elliptic curve cryptography are mentioned briefly.

Cryptographic protocols are discussed, including Diffie-Hellman key exchange and digital signatures.

Finally, cryptanalysis is considered. In particular, the following topics are explored: frequency analysis, integer factorisation, and the discrete logarithm problem.

This module will develop a range of graduate attributes, including numeracy skills, problem formulation, problem solving skills, and the ability to present a clear argument.

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:
			✓			D&G and NCL

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. Solve a range of problems in elementary number theory;

L2. Apply various encryption and decryption algorithms;

L3. Understand and implement cryptographic protocols;

L4. describe and apply cryptanalytical methods for breaking codes.

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 9. Demonstrating competence in solving problems in coding theory and elementary number theory.
Practice: Applied Knowledge and Understanding	SCQF Level 9. Implementing various coding systems, encryption and decryption algorithms, crypto- graphic protocols, and cryptanalytical methods.

Generic Cognitive skills	SCQF Level 9. Breaking down mathematical problems into a series of simpler problems which can be solved individually; making decisions about which cryptographic scheme, or cryptographic protocol, or cryptanalytical method to use in a particular context.
Communication, ICT and Numeracy Skills	SCQF Level 9. Working autonomously to produce individual output from mathematical problems. Constructing a written argument that is both logical and structured. Interpreting and analysing numerical information.
Autonomy, Accountability and Working with others	SCQF Level 9. Working autonomously to produce individual output from mathematical problems. Applying time management skills to meet a deadline.

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.

Learning and Teaching	
An appropriate blend of subject matter delivered in lectures and supported by tutorials. All teaching materials for the module will be available on the moodle site for Cryptography.	
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	24
Tutorial/Synchronous Support Activity	24
Independent Study	152
	200 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:

Martin, K. (2017) 2nd Ed. Everyday Cryptography: Fundamental Principles and Applications. Oxford UP.

Burton, D. (2012) 7th Ed. Elementary Number Theory, McGraw-Hill.

Rosen, K. (2013) 6th Ed. Elementary Number Theory and its Applications, Addison Wesley Longman.

Hoffstein, Pipher and Silverman. (2014) 2nd Ed. An Introduction to Mathematical Cryptography, Springer.

Katz and Lindell. (2014) 2nd Ed. Introduction to Modern Cryptography, Second Edition, CRC Press.

Singh, S.(2002) The Code Book: The Secret History of Codes and Code-Breaking, Harper Collins.

Internet access to Moodle to allow student access to all teaching material, including slides, tutorials, coursework and lab sheets for the practical aspects of the syllabus.

(**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)

Attendance 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. Please refer to the Academic Engagement and Attendance Procedure at the following link: Academic engagement and attendance procedure

Supplemental Information

Programme Board	Computing
Assessment Results (Pass/Fail)	No
Subject Panel	Business &amp; Applied Computing
Moderator	Graham Parsonage
External Examiner	H Al-Khateeb
Accreditation Details	
Version Number	1.05

Assessment: (also refer to Assessment Outcomes Grids below)
Coursework 1 - 60%
Coursework 2 - 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)**	**Learning Outcome (4)**	**Weighting (%) of Assessment Element**	**Timetabled Contact Hours**
Report of practical/ field/ clinical work	✓	✓	✓	✓	60	10

Component 2

Assessment Type (Footnote B.)	**Learning Outcome (1)**	**Learning Outcome (2)**	**Learning Outcome (3)**	**Learning Outcome (4)**	**Weighting (%) of Assessment Element**	**Timetabled Contact Hours**
Dissertation/ Project report/ Thesis	✓	✓	✓	✓	40	10
				Combined Total For All Components	100%	20 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)