Module Descriptor

Title	Cryptography		
Session	2025/26	**Status**	Published
Code	COMP09106	**SCQF Level**	9
Credit Points	20	**ECTS (European Credit Transfer Scheme)**	10
School	**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	**On-Campus[1]**	**Hybrid[2]**	**Online[3]**	**Work -Based Learning[4]**
	☒	☐	☐	

[1] Where contact hours are synchronous/ live and take place fully on campus. Campus-based learning is focused on providing an interactive learning experience supported by a range of digitally-enabled asynchronous learning opportunities including learning materials, resources, and opportunities provided via the virtual learning environment. On-campus contact hours will be clearly articulated to students.

[2] The module includes a combination of synchronous/ live on-campus and online learning events. These will be supported by a range of digitally-enabled asynchronous learning opportunities including learning materials, resources, and opportunities provided via the virtual learning environment. On-campus and online contact hours will be clearly articulated to students.

[3] Where all learning is solely delivered by web-based or internet-based technologies and the participants can engage in all learning activities through these means. All required contact hours will be clearly articulated to students.

[4] Learning activities where the main location for the learning experience is in the workplace. All required contact hours, whether online or on campus, will be clearly articulated to students

				☐
Campuses for Module Delivery	☐ Ayr ☐ Dumfries	☒ Lanarkshire ☐ London ☐ Paisley	☐ Online / Distance Learning ☐ Other (specify)	
Terms for Module Delivery	Term 1 ☒	Term 2 ☐	Term 3 ☐	
Long-thin Delivery over more than one Term	Term 1 – Term 2 ☐	Term 2 – Term 3 ☐	Term 3 – Term 1 ☐	

Learning Outcomes	
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.
L5	N/A

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 9** Demonstrating competence in solving problems in coding theory and elementary number theory.
Practice: Applied Knowledge and Understanding	**SCQF 9** Implementing various coding systems, encryption and decryption algorithms, crypto-graphic protocols, and cryptanalytical methods.
Generic Cognitive skills	**SCQF 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 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 9** Working autonomously to produce individual output from mathematical problems. Applying time management skills to meet a deadline.

Prerequisites	**Module Code**	**Module Title**
	Other	
Co-requisites	**Module Code**	**Module Title**

Learning and Teaching	
In line with current learning and teaching principles, a 20-credit module includes 200 learning hours, normally including a minimum of 36 contact hours and maximum of 48 contact hours. 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** (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
Please select	
Please select	
Please select	
TOTAL	200

Indicative Resources
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. VirtualBox software and VBOX extension
(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 and Engagement Requirements
In line with the Student Attendance and Engagement Procedure, Students are academically engaged if they are regularly attending and participating in timetabled on-campus and online teaching sessions, asynchronous online learning activities, course-related learning resources, and complete assessments and submit these on time. **For the purposes of this module, academic engagement equates to the following:**

The School of Computing, Engineering and Physical Sciences considers attendance and engagement to mean a commitment to attending, and engaging in, timetabled sessions. You will scan your attendance via the scanners each time you are on-campus and you will login to the VLE several times per week. Where you are unable to attend a timetabled learning session due to illness or other circumstance, you should notify the Programme Leader that you cannot attend. Across the School an 80% attendance threshold is set. If you fall below this, you will be referred to the Student Success Team to see how we can best support your studies.

Equality and Diversity
The University's Equality, Diversity and Human Rights Procedure can be accessed at the following link: UWS Equality, Diversity and Human Rights Code. Aligned with the University's commitment to equality and diversity, this module supports equality of opportunity for students from all backgrounds and learning needs. Using the VLE, material will be presented electronically in formats that allow flexible access and manipulation of content. This module complies with University regulations and guidance on inclusive learning and teaching practice. This module has lab-based teaching and as such you are advised to speak to the Module Co-ordinator to ensure that specialist assistive equipment, support provision and adjustment to assessment practice can be put in place, in accordance with the University's policies and regulations.
(N.B. Every effort will be made by the University to accommodate any equality and diversity issues brought to the attention of the School)

Supplemental Information

Divisional Programme Board	**Computing**
Overall Assessment Results	☐ **Pass / Fail** ☒ **Graded**
Module Eligible for Compensation	☒ **Yes** ☐ **No** **If this module is eligible for compensation, there may be cases where compensation is not permitted due to programme accreditation requirements. Please check the associated programme specification for details.**
School Assessment Board	Business & Applied Computing
Moderator	Graham Parsonage
External Examiner	M Davis
Accreditation Details	
Module Appears in CPD catalogue	☐ **Yes** ☒ **No**
Changes / Version Number	1.06

Assessment (also refer to Assessment Outcomes Grids below)
Assessment 1
Coursework 1 - 60%
Assessment 2
Coursework 2 - 40%
Assessment 3

(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 Module Handbook.)

Component 1							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Report of practical/ field/ clinical work	☒	☒	☒	☒	☐	60	10

Component 2							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Dissertation/ Project report/ Thesis	☒	☒	☒	☒	☐	40	10

Component 3							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
	☐	☐	☐	☐	☐		
Combined total for all components						100%	20 hours

Change Control

What	**When**	**Who**
Attendance and Engagement and Equality and Diversity Statement	20.01.25	R Moffat
External Examiner updated	22/01/2025	A Adamson