Module Descriptor

Title	Number Theory and its Applications		
Session	2025/26	**Status**	Published
Code	MATH10009	**SCQF Level**	10 (Scottish Credit and Qualifications Framework)
Credit Points	20	**ECTS (European Credit Transfer Scheme)**	20
School	**Computing, Engineering and Physical Sciences**		
Module Co-ordinator	Dr Kwok Chi Chim		

Summary of Module

A range of topics in number theory are presented:

Divisibility, prime numbers, prime number theorem and Euler's totient function.

Congruences and their properties, linear congruence, Chinese remainder theorem, Fermat's little theorem, Wilson's theorem, Lagrange's theorem, primality tests, primitive roots, indices.

Quadratic residues, Legendre symbol, law of quadratic reciprocity.

Definition of groups, rings and fields are mentioned as well as cyclic groups and finite fields. Elliptic curves and the group law are introduced.

These concepts provide the theoretical underpinning needed for cryptography.

The wireless communication system, Huffman coding, Hamming codes are introduced.

Cryptography is introduced and its historical significance is discussed. Cryptographic systems including the RSA public key cyptosystem, ElGamal encryption scheme and Elliptic Curve Cryptography are presented. Cryptographic protocols, including Diffie-Hellman key exchange, are discussed.

The Graduate Attributes relevant to this module are given below:

- Academic: Critical thinker; Analytical; Inquiring; Knowledgeable; Problem-solver; Digitally literate; Autonomous; Incisive; Innovative.
- Personal: Motivated, Creative; Imaginative; Resilient
- Professional: Ambitious; Driven.

Module Delivery Method	On-Campus[1] ☒	Hybrid[2] ☐	Online[3] ☐	Work -Based Learning[4] ☐
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	Demonstrate a good understanding of divisibility, prime numbers, and congruences.
L2	Demonstrate a knowledge of groups, rings, fields and elliptic curves.
L3	Demonstrate a good understanding of various encryption and decryption algorithms, as well as cryptographic protocols.
L4	
L5	

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 10** Demonstrating a detailed knowledge and understanding of a range of standard techniques in number theory and its application in cryptography. Demonstrating critical awareness of established techniques of enquiry.
Practice: Applied Knowledge and Understanding	**SCQF 10** Using a range of standard techniques to solve problems that are specialised, advanced of number theory and its applications in cryptography.

[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

	Carrying out defined investigative problems within a mathematically based subject and implementing relevant outcomes.
Generic Cognitive skills	**SCQF 10** Critically identify, define, conceptualise and analyse complex problems. Critically review and consolidate knowledge, skills, practices and thinking in number theory and its applications in cryptography.
Communication, ICT and Numeracy Skills	**SCQF 10** Present, formally and/or informally, information about number theory and its applications in cryptography to informed audiences.
Autonomy, Accountability and Working with Others	**SCQF 10** Exercise autonomy and initiative in professional/equivalent activities.

Prerequisites	**Module Code** MATH08007	**Module Title** Linear Algebra
	Other or equivalent	
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.	
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	12
Independent Study	164
Please select	
Please select	
Please select	
TOTAL	200 Hours Total

Indicative Resources
The following materials form essential underpinning for the module content and ultimately for the learning outcomes: Class notes as published on the University VLE.

"Number Theory", A Dujella "Understanding Crytography, From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms", second edition, C. Paar, J. Pelzl and T. Gueneysu. "Elementary Number Theory", D Burton "Elementary Number Theory and its Applications", K Rosen "An Introduction to Mathematical Cryptography", J Hoffstein, J Pipher, and JH Silverman
(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. Specialist assistive equipment, support provision and adjustment to assessment practice 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	**Engineering Physical Sciences**
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	Computing, Engineering and Physical Sciences
Moderator	Dr Raymond Carragher
External Examiner	P Wilson
Accreditation Details	
Module Appears in CPD catalogue	☐ **Yes** ☒ **No**
Changes / Version Number	1.10 Change to summary of module and indicative resources Term for module delivery: Term 1 Change to assessment component Change to attendance and engagement requirements Change to equality and diversity

Assessment (also refer to Assessment Outcomes Grids below)
Assessment 1
Class Test (Unseen, closed book) (80%)
Assessment 2
A series of coursework assignments (20%)
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**
Class Test (unseen, closed book)	☒	☒	☒	☐	☐	80%	2

Component 2							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Coursework	☒	☒	☒	☐	☐	20%	

Component 3							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
	☐	☐	☐	☐	☐		
Combined total for all components						100%	2 hours

Change Control

What	**When**	**Who**
Change to summary of module and indicative resources Term for module delivery: Term 1 Change to assessment component Change to attendance and engagement requirements Change to equality and diversity	March 2025	Dr Kwok Chi Chim