IMPERIAL

Module Specification

Basic details

UID		Cohorts covered	Earliest cohort: Latest:
Long title	Cryptography and Coding Theory		
New code	ELEC70069	New short title	
Brief description of module *(approx. 600 chars.)*	The goal is to help you gain skills and fundamental knowledge on number theory, finite fields, cryptography, and error-correcting codes. You will state fundamental principles in number theory and finite fields, apply the principles for cryptography and error-correcting codes, perform secure information exchange using encryption/decryption and digital signature schemes, and correct communication errors using popular error-correcting codes for reliable information exchange.		
	476 characters		
Available as a standalone module/ short course?	No		

Statutory details

	ECTS	CATS	Non-credit		
Credit value	5	10	N	HECOS codes	
FHEQ level	L7				

Allocation of study hours

	Hours	
Lectures	20	
Group teaching	0	*Incl. seminars, tutorials, problem classes.*
Lab/ practical	0	
Other scheduled	0	*Incl. project supervision, fieldwork, external visits.*
Independent study	105	*Incl. wider reading/ practice, follow-up work, completion of assessment*
Placement	0	*Incl. work-based learning and study that occurs overseas.*
Total hours	125	
ECTS ratio	25.00	

Project/placement activity

Is placement activity allowed?	No

Module delivery

Delivery mode	Taught/ Campus	Other	
Delivery term	Term 1	Other	

Ownership

Primary department	Department of Electrical and Electronic Engineering
Additional teaching departments	0

Delivery campus	South Kensington

Collaborative delivery

Collaborative delivery?	N

External institution	N/A
External department	N/A
External campus	N/A

Associated staff

Role	CID	Given name	Surname
Module Leader		Wei	Dai
		0	0
		0	0
		0	0
		0	0
		0	0
		0	0
		0	0
		0	0
		0	0

Learning and teaching

Module description

Learning outcomes	Upon successful completion of this module, you will be able to: 1. State fundamental principles behind number theory and finite fields, conduct efficient computations related to large integer numbers and polynomials in finite fields, and apply the principles in cryptography and error-correcting codes. 2. Design and analyse encryption/decryption schemes for secure information exchange – Cryptography 3. Create digital signature schemes for secure information exchange – Cryptography 4. Detect and correct communication errors using popular error-correcting codes, including Hamming codes, Reed-Solomon codes, and/or BCH codes, for reliable information exchange – Error-correcting codes
Module content	Number theory: prime numbers, Euclidean algorithm, modular algebra, and integer divisibility. Finite fields: definition, properties, primitive element, and polynomial factorisation on finite fields; Cryptography: password storage and sharing, secret sharing, public key systems, and digital signature; Concepts of error detection and correction. Linear codes, generator and parity checking matrices, distance, and Hamming codes; Bounds to the performance of codes; Reed Solomon codes, Cyclic and BCH codes;

Learning support	1. Online lecture notes and videos for comprehensive review and revision. 2. GTAs host regular Q&A sessions to provide timely assistance and clarify concepts. 3. An online Q&A channel supports students who cannot attend in-person sessions. 4. Group projects as coursework foster peer-learning, collaboration, and teamwork. 5. Four coursework assignments throughout the term, followed by detailed performance charts for timely feedback and identifying areas of strength and improvement. 6. In-lecture discussions of selected coursework problems encourage peer-to-peer discourse and analysis of problem-solving strategies.
Pattern of learning and teaching activities	Two lectures per week, one Q&A session led by the GTAs weekly, and four coursework assignments distributed throughout the term.
Learning and Teaching Approach	1. Lectures delve into key concepts, fundamental theories, and various applications in detail. 2. Through coursework, students engage in learning and practical application of theory by solving problems. These exercises aim to enhance understanding and solidify theoretical concepts, drawing from both theoretical scenarios and real-world applications. 3. Selected problem solutions from coursework will be reviewed during lectures. This facilitates students' understanding of different problem-solving approaches, enabling them to tailor solutions to specific practical needs and compare various methods effectively.
Assessment Strategy	The module's assessment consists of four coursework assignments, with each assignment contributing 25% to the final mark.
Feedback	1. Regular Q&A sessions led by GTAs to clarify concepts, address questions, and offer timely assistance to students. 2. An online Q&A channel to offer help and support for students unable to attend regular sessions. 3. Detailed coursework performance charts to delineate areas of strength and areas needing improvement. 4. In-lecture discussions on selected problems to foster peer-to-peer discourse and analyze problem-solving approaches.
Reading list	Supplementary [1] Anshel, Michael, and Kent D. Boklan. "Introduction to cryptography with coding theory." The Mathematical Intelligencer 29, no. 3 (2007): 66-69. [2] R. M. Roth, Introduction to coding theory /. Cambridge :: Cambridge University Press, 2006. [3] Baldoni, M. Welleda, Ciro Ciliberto, and Giulia Maria Piacentini Cattaneo. Elementary number theory, cryptography and codes. Berlin: Springer, 2009.

Quality assurance

Date of first approval	February 2022
Date of last revision	May 2023
Date of this approval	
Module leader	Dr. Wei Dai

Office use only

QA Lead	
Department staff	
Date of collection	
Date exported	
Date imported	

Notes/ comments	

Assessment details

Grading method	Numerical	Pass mark	50%

Assessments

Assessment type	Assessment description	Weighting	Pass mark	Must pass?
Coursework	Design Project 1 (A Report)	25%	50%	N
Coursework	Design Project 2 (A Report)	25%	50%	N
Coursework	Design Project 3 (A Report)	25%	50%	N
Coursework	Design Project 4 (A Report)	25%	50%	N
0	0	0%	0%	0.00
0	0	0%	0%	0.00
0	0	0%	0%	0.00
0	0	0%	0%	0.00
0	0	0%	0%	0.00
0	0	0%	0%	0.00
0	0	0%	0%	0.00
0	0	0%	0%	0.00
0	0	0%	0%	0.00
		100%		