MA300-15 Mathematics of Cryptography

26/27

Department
Warwick Mathematics Institute
Level
Undergraduate Level 3
Module leader
Helena Verrill
Credit value
15
Module duration
10 weeks
Assessment
Multiple
Study location
University of Warwick main campus, Coventry

Description

Introductory description

An introduction to mathematics of cryptography.
This will cover various cryptographic schemes, including public key cryptography, private key cryptography, hash functions, key exchange, digital signatures. Elliptic curve cryptography and its usage in many popular applications, such as bitcoin, will be described in detail. This module will build on concepts students have studied in second year algebra and number theory modules.

Module aims

Students will understand the mathematics of commonly used cryptographic methods. This module shows how pure mathematics is important in modern technology, and shows the importance of applied algebra and number theory.
Transferable skills include practice with python, group work, and presentation skills.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be

covered. Actual sessions held may differ.

- Private key cryptography
- Block ciphers
- Stream ciphers
- Hash functions
- RSA Public key cryptography
- Elliptic curve cryptography
- Key exchange
- Zero knowledge proof

Learning outcomes

By the end of the module, students should be able to:

- A theoretical and practical knowledge and understanding of the main methods of public key cryptography
- A theoretical understanding of some common methods of private key crypography
- An theoretical and computational understanding of elliptic curve cryptography
- Understanding of digital signature algorithms and their use
- Understanding of the mathematics of cryptocurrencies, block chains, and hash functions
- Competency with use of python applied for cryptographic purposes
- Ability to write a formal mathematical project
- Skills of working in a group
- Practice of presentation skills

Indicative reading list

Reading lists can be found in Talis

Research element

Potentially investigating real world applications of the cryptographic systems they will study in abstract in the classes.

Subject specific skills

Mathematical analysis of cryptographic systems
Coding in python and sage

Transferable skills

Group work skills
academic writing skills
presentation/speaking skills

Study

Study time

Type	Required
Lectures	30 sessions of 1 hour (20%)
Private study	45 hours (30%)
Assessment	75 hours (50%)
Total	150 hours

Private study description

Around 3 hours per lecture private study. May be included in quiz and assignment work. Regular group work for the project is expected.

Costs

No further costs have been identified for this module.

Assessment

You do not need to pass all assessment components to pass the module.

Assessment group A

	Weighting	Study time	Eligible for self-certification
Moodle Quiz	10%	5 hours	No
short formative quizzes on moodle. 10 questions per quiz. Best 4 of 5 count. Due every other week. Multiple attempts allowed, but must be completed by fortnightly deadlines.			
Assignments	40%	20 hours	No
5 written assignments, including sage/python components. Best 4/5 count			
Group Project	40%	40 hours	No
Students will work in groups of about 5 students to produce a written project which will be around 25 pages long. This may include coding elements in sage/python. Length flexible, depending on coding content, diagrams, etc.			
Project presentation	10%	10 hours	No
Group talk about the project			

Assessment group R

	Weighting	Study time	Eligible for self-certification
Project	80%		No
Project selected from a list of topics in cryptography			
Project presentation	20%		No
A talk about the project			

Feedback on assessment

Written feedback

Availability

Pre-requisites

some familiarity with python programming or similar.

Courses

This module is Optional for:

- Year 1 of TMAA-G1P0 Postgraduate Taught Mathematics
- TMAA-G1PC Postgraduate Taught Mathematics (Diploma plus MSc)
  - Year 1 of G1PC Mathematics (Diploma plus MSc)
  - Year 2 of G1PC Mathematics (Diploma plus MSc)
- Year 3 of UCSA-G4G1 Undergraduate Discrete Mathematics
- UCSA-G4G3 Undergraduate Discrete Mathematics
  - Year 3 of G4G1 Discrete Mathematics
  - Year 3 of G4G3 Discrete Mathematics
- Year 4 of UCSA-G4G4 Undergraduate Discrete Mathematics (with Intercalated Year)
- Year 4 of UCSA-G4G2 Undergraduate Discrete Mathematics with Intercalated Year

This module is Core option list C for:

- Year 3 of UMAA-GV17 Undergraduate Mathematics and Philosophy
- Year 3 of UMAA-GV19 Undergraduate Mathematics and Philosophy with Specialism in Logic and Foundations

This module is Core option list F for:

- Year 4 of UMAA-GV19 Undergraduate Mathematics and Philosophy with Specialism in Logic and Foundations

This module is Option list A for:

- UMAA-G105 Undergraduate Master of Mathematics (with Intercalated Year)
  - Year 4 of G105 Mathematics (MMath) with Intercalated Year
  - Year 5 of G105 Mathematics (MMath) with Intercalated Year
- Year 3 of UMAA-G100 Undergraduate Mathematics (BSc)
- UMAA-G103 Undergraduate Mathematics (MMath)
  - Year 3 of G100 Mathematics
  - Year 3 of G103 Mathematics (MMath)
  - Year 4 of G103 Mathematics (MMath)
- Year 4 of UMAA-G107 Undergraduate Mathematics (MMath) with Study Abroad
- Year 4 of USTA-G1G3 Undergraduate Mathematics and Statistics (BSc MMathStat)
- Year 4 of UMAA-G101 Undergraduate Mathematics with Intercalated Year

This module is Option list B for:

- Year 3 of USTA-GG14 Undergraduate Mathematics and Statistics (BSc)

This module is Option list C for:

- Year 3 of USTA-G1G3 Undergraduate Mathematics and Statistics (BSc MMathStat)