WM141-18 Discrete Structures for Cyber Security

24/25

Department
WMG
Level
Undergraduate Level 1
Module leader
Henry Caushi
Credit value
18
Module duration
30 weeks
Assessment
40% coursework, 60% exam
Study location
University of Warwick main campus, Coventry

Description

Introductory description

Discrete mathematics forms the mathematical foundation of computer science and cyber security. It forms the basis of how computers work, allows us to prove system correctness and security, and underlies modern cryptography. This course introduces the discrete structures used by computers, as well as how to use them to solve problems in cyber security.

Module aims

This module aims to give students an understanding of the discrete structures used in cyber security, and how to use them to solve problems in cyber security.

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.

Numbers and sets: Basic algebra: Types of numbers and their properties. Sets and their operations, set countability and power sets.

Logic and proof: Proposition and predicates. Common proof techniques including direct proof, contrapositive, exhaustion, induction and more. Common mistakes made in proofs.
Functions and relations: Functions and their inverses. Injections, surjections and bijections. Properties of relations including (anti-)symmetry, reflexivity and transitivity. Partial orderings, total orderings and equivalence relations.
Number theory: Divisibility, modular arithmetic and Fermat's little theorem. The fundamental theorem of arithmetic. The GCD and LCM, and Euclid's algorithm.
Combinatorics: The multiplication and addition principles. Permutations.
Probability: Uniform distribution. Independent and mutually exclusive events.
Graph theory: Adjacency, distance and incidence matrices. Social network theory.

Learning outcomes

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

- Use a variety of techniques to prove and disprove mathematical statements
- Recognise common mistakes made in mathematical proofs
- Analyse the probabilities of random events, and use their findings to make informed recommendations
- Understand how people form social networks from a graph-theoretic perspective
- Use number-theoretic techniques to develop simple cryptographic systems
- Use formal verification techniques to analyse the security of simple programs

Indicative reading list

Johnsonbaugh, Richard, "Discrete mathematics", 8 Ed, Pearson Education Limited (2019)

Balakrishnan, V. K., “Schaum's Outline of Combinatorics”, McGraw-Hill (1995)

Karumanchi, Narasimha, “Data Structures and Algorithms Made Easy: Data Structure and Algorithmic Puzzles”, 2 Ed, CareerMonk (2011)

View reading list on Talis Aspire

Subject specific skills

This course equips students with the foundational mathematical skills necessary in computer science and cyber security, including logic and proof, functions and their inverses, graphs, and probability, and applies these skills in a cyber context.

Transferable skills

Numeracy, logical reasoning, problem solving, written communication skills, and increased numerical confidence

---

Study

Study time

Type	Required
Lectures	18 sessions of 1 hour (10%)
Supervised practical classes	18 sessions of 2 hours (20%)
Private study	54 hours (30%)
Assessment	72 hours (40%)
Total	180 hours

Private study description

Independent activity between workshops.

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 D4

	Weighting	Study time
In-class test 1	20%	18 hours
An in-class test covering content taught in the first half of the module.		
In-class test 2	20%	18 hours
An in-class test covering content taught in the second half of the module.		
End-of-year exam	60%	36 hours
An online open-book exam applying the content in the module to a cyber security context.		

~Platforms - WAS

- Online examination: No Answerbook required

Feedback on assessment

Students will receive a per-question breakdown of their mark along with any specific comments on

their answers, and a mark scheme for each paper will be released once all submissions are marked.

Past exam papers for WM141

Availability

Courses

This module is Core for:

- UWMA-H651 Undergraduate Cyber Security
  - Year 1 of H651 Cyber Security
  - Year 1 of H651 Cyber Security
  - Year 1 of H651 Cyber Security