



**UNSW**  
SYDNEY

**UNSW SCIENCE**  
**SCHOOL OF MATHS AND STATISTICS**

**MATH3411**  
**Information, Codes & Ciphers**  
**Term 3, 2019**

# MATH3411 – Course Outline

## Information about the course

**Course Authority:** Thomas Britz

**Lecturer:** Thomas Britz (RC-5111, [britz@unsw.edu.au](mailto:britz@unsw.edu.au), 9385 7115)

**Consultation:** Thursday 15:00-16:00

Also, please feel free to contact me (Thomas) at other times, by email, Facebook group/Messenger/Edstem, or just in person. Also, please help each other throughout the course, in class, in person, and through the Facebook group and Edstem forum (see below).

### **Credit, Prerequisites, Exclusions:**

This course counts for 6 Units of Credit (6UOC).

The prerequisites for this course are

MATH1081 or MATH1231(CR) or MATH1241(CR) or MATH1251(CR) or MATH2099.

There is no higher version of this subject.

### **Lectures:**

There will be 4 hours of lectures per week, from Week 1 to 10, except in Week 5 in which there will be only 2 hours of lectures.

Tuesday	12:00 - 14:00	Physics Theatre (K-K14-19)
Friday	14:00 - 16:00	Mathews Theatre B (K-D23-203)

### **Tutorials:**

There will be 1 tutorial per week, during Weeks 1 - 10, in one of the following slots:

Tuesday	14:00 - 15:00	RC-1043
Tuesday	15:00 - 16:00	RC-1043
Thursday	16:00 - 17:00	RC-2063
Thursday	17:00 - 18:00	RC-1043
Friday	13:00 - 14:00	RC-1043

To cover all tutorial problems, **additional tutorials will be held in Week 11**, in the Tuesday timeslots.

Note that there is a strong correlation between solving tutorial problems and attending tutorials and getting a good final mark.

See Moodle for a precise schedule of the problems that each week's tutorial will cover.

**Moodle:** Further information and other material will be provided via Moodle; see

<https://moodle.telt.unsw.edu.au/course/view.php?id=44356>

Check this regularly as more information will be added throughout the semester.

**Facebook:** Feel free to join the course Facebook group here:

MATH3411 Information, Codes and Ciphers 2019T3

This will probably be the easiest way to quickly find, ask, and contribute general information, and to chat, share and discuss more generally.

**Edstem:** Also please join the course Edstem forum. A link will soon follow.

This will probably be the best way to find and share mathematical content.

## Course aims

The aim of MATH3411 is to introduce you to the areas of information theory, coding theory and cryptography. It does not consider any of these topics in great depth: it is more of an overview. It will cover the mathematical aspects of these areas and will not cover any engineering or implementation aspects, although such aspects may be mentioned where relevant.

## Relation to other mathematics and computing courses

Mathematics may be divided into the broad categories of analysis (calculus), algebra, geometry, discrete mathematics, and applied mathematics. This subject fits into the algebra and applied-mathematics categories and follows on from material you will have learned in first year algebra, linear algebra and from certain other related courses you may have taken.

This course is very useful for those majoring in Pure Mathematics, those planning to teach, or those students of Mathematics who are interested in applications of pure mathematics to information technology. It might be of particular interest to computer science students and engineering students who have learned parts of the course from an implemental and practical approach: this course will provide the underlying mathematical understanding.

This is a 6 UOC 3rd level course, suitable for students with some maths background. For students interested in computer security, the Faculty of Engineering offers several courses more focused on security applications: COMP6441 is particularly relevant.

## **Student learning outcomes**

By the end of this course, you will understand various coding theory, information theory and cryptographic concepts and be able to apply various methods to solve simple and complex problems in coding theory, information theory and cryptography.

### **Relation to graduate attributes**

These outcomes are related to the development of Science Faculty Graduate Attributes

1. Research, inquiry and analytical thinking abilities;
6. Information literacy.

They are also related to the UNSW Graduate Attribute

3. Capacity for analytical and critical thinking and for creative problem solving.

## **Teaching strategies underpinning the course**

New ideas and skills are introduced and demonstrated in lectures. Students develop these skills by applying them to specific tasks in tutorials and assessments.

### **Rationale for learning and teaching strategies**

We believe that effective learning is best supported by a climate of enquiry, in which students are actively engaged in the learning process. To ensure effective learning, students should participate in class as outlined below.

We believe that effective learning is achieved when students attend all classes, have prepared effectively for classes by reading through previous lecture notes, in the case of lectures, and, in the case of tutorials, by having made a serious attempt at doing for themselves the tutorial problems prior to the tutorials.

Furthermore, lectures should be viewed by the student as an opportunity to learn, rather than just copy down lecture notes. Effective learning is achieved when students have a genuine interest in the subject and make a serious effort to master the basic material.

# Assessment

The assessment components for this course are

- one 30 minute online test worth 10%,
- two 45 minute online tests worth 15% each, and
- a final exam of 2 hours' duration, worth 60%.

Practice tests will be available in week leading up to each test.

**Assessment criteria:** Assessment in this course will involve demonstrating understanding of the coding theory, information theory and cryptographic concepts presented in lectures (Science Graduate Attribute 1) and will require problem-solving techniques developed in lectures as well as creativity and critical thinking (UNSW Graduate Attribute 3). The tests will also provide feedback on students' progress.

## Tests

### **Rationale:**

The Tests will give students feedback on their progress and mastery of the material.

**Weighting:** Test 1 is worth 10% of final mark; Tests 2 and 3 are each worth 15% of the final mark.

The online tests will be held on the Friday of **Weeks 4, 7, and 10**; that is, on

Friday 11 Oct, Friday 1 Nov, and Friday 22 Nov.

There will be three timeslots in which you will be able to take these tests:

09:00-10:00, 12:00-13:00, and 20:00-21:00.

Tests will be of a standard similar to the unstarred tutorial questions and online practice tests will be available in the week leading up to each test.

If you miss a class test through illness, show your medical certificate to your lecturer; **do not** apply centrally to the University.

## Examination

**Duration:** 2 hours.

**Rationale:** The final examination will assess student mastery of the material covered in the lectures.

**Weighting:** 60% of your final mark.

Further details about the final examination will be available in class closer to the time of the exam.

# Additional resources and support

## Course notes, YouTube videos and textbooks

The course notes for *Information Codes and Ciphers*, School of Mathematics and Statistics, UNSW, by Dennis Trenerry *et al.*, is available in electronic form on Moodle. These notes are comprehensive and cover more than the course material but are sometimes confusing to navigate and read.

There are therefore also separate but aligned lectures notes. The lectures will be based on these lecture notes. The lecture notes and lecture slides are available on Moodle.

The tutorial exercises are also available on Moodle, and a link is given to a playlist of YouTube video solutions to selected MATH3411 tutorial problems. A link to these will be provided on Moodle.

You may also choose to use additional sources, though they are not necessary. The book by Bose listed below covers much of the syllabus (and more), but not in the order we cover and not always with the same notation and techniques. The books by Pretzel or Roman and Salomaa or Schneier (all listed below) between them cover most of the syllabus (and much more) in the same way. These books may be as use to you during the course; however, you are not required to buy these; the course notes are sufficient.

## References

There are many books in the library on the topics covered in this subject but many are at a high level of difficulty. The following list is of some that are more readable.

- N. Abrahamson, *Information Theory and Coding*, McGraw-Hill (1963).PX519.7/9 (for Chapters 3, 4)
- R. Ash, *Information Theory*, John Wiley (1965), recently reprinted by Dover. PX519.7/12A (for Chapters 3, 4)
- R. Bose, *Information Theory, Coding and Cryptography*, Tata McGraw-Hill (2002).
- G. Brassard, *Modern Cryptography*, Springer (1988). P005.82/4 (for Chapter 7)
- R.W. Hamming, *Coding and Information Theory*, Prentice-Hall (1986).P003.54/3 (for Chapters 3,4)
- R. Hill, *A First Course in Coding Theory*, Clarendon (1986). P005.72/4 (for Chapters 2,6)
- V. Pless, *Introduction to the Theory of Error-Correcting Codes*, Wiley (1982/89). P001.539/23, P005.72/5 (for Chapters 2,6)
- O. Pretzel, *Error-Correcting Codes and Finite Fields*, Clarendon (1992). P003.54/20 (for Chapters 2,5,6)
- S. Roman, *Coding and Information Theory*, Springer (1992). P003.54/19 (for Chapters 2,3,4,5,6)
- A. Salomaa, *Public-key Cryptography*, Springer (1990/96). P005.82/11,11A (for Chapter 7)
- B. Schneier, *Applied Cryptography*, Wiley (1996). P005.82/10A (for Chapter 7)
- H.C.A. van Tilborg, *An Introduction to Cryptology*, Kluwer (1988). P652.8/5 (for Chapter 7)

# Course evaluation and development

The School of Mathematics and Statistics evaluates each course each time it is run. We carefully consider the student responses and their implications for course development. It is common practice to discuss informally with students how the course and their mastery of it are progressing.

## Administrative matters

### Exam information

Please note that the University will *not* provide calculators for students in examinations. You must supply your own, and *before the examination* you must have it labeled as an approved model. For full instructions, see

[www.maths.unsw.edu.au/currentstudents/exam-information-and-timetables](http://www.maths.unsw.edu.au/currentstudents/exam-information-and-timetables)

This includes a link to the lists of approved calculators.

### Additional assessment

Details on additional assessments are available at

[www.maths.unsw.edu.au/currentstudents/assessment-policies](http://www.maths.unsw.edu.au/currentstudents/assessment-policies)

### School rules and regulations

Details of the general School rules regarding attendance, release of marks, special consideration and so on are available here:

[www.maths.unsw.edu.au/currentstudents/assessment-policies](http://www.maths.unsw.edu.au/currentstudents/assessment-policies)

### Plagiarism and academic honesty

Plagiarism is the presentation of another's thoughts or work as one's own. Issues that you must be aware of regarding plagiarism and the university's policies on academic honesty and plagiarism can be found here:

<https://student.unsw.edu.au/plagiarism>

# Detailed course schedule

It is intended that the following topics will be covered in the given order. Any variation from this will be indicated by the lecturer.

## SYLLABUS

### Chapter 1: Introduction

A mathematical model of coding. A brief revision of modular arithmetic. Morse Code. ASCII Code. ISBN numbers.

### Chapter 2: Error detecting and correcting codes

Random noise. Error correcting capabilities of ISBN numbers. Burst noise and error correcting codes. Binary repetition codes. Information rate and redundancy. Binary Hamming codes. Hamming distance, weights and connection with error correction. Sphere packing. Perfect codes. Binary linear codes. Standard form matrices. Extending linear codes. Radix greater than 2.

### Chapter 3: Compression coding

Uniquely decodable (UD) codes, instantaneous codes. Decision trees. Kraft-McMillan theorem. Minimal UD-codes. Extensions of a source. Markov sources. Huffman coding for stationary Markov sources. Other text compression methods, including arithmetic coding and dictionary methods.

### Chapter 4: Information theory

Information and entropy. Maximum entropy theorem. Entropy and coding. Shannon-Fano coding. Entropy of extensions of sources. Entropy for Markov sources. Noisy channels. Channel capacity. Shannon's noisy channel coding theorem. Entropy of natural language.

### Chapter 5: Algebra and number theory (background)

Revision of discrete mathematics. Number theory results (no proofs). Polynomials over prime fields. Finite fields. Minimal and primitive polynomials. Primality testing, including pseudoprime test, Lucas test, Miller-Rabin test. Prime number generation. Factoring, including Fermat factorisation, Pollard's rho method. Random number generation, including linear congruential, linear feedback shift registers, cryptographic generators.

### Chapter 6: Algebraic coding

BCH codes: single error-correcting, double error-correcting and the general case.

### Chapter 7: Cryptography

Classical cryptography: Caesar cipher, simple substitution cipher, transposition ciphers. Vigenère cipher, Kasiski's method. Non-period polyalphabetic substitution ciphers, one-time pad. Types of ciphers. Encryption standards. One-way functions, hash functions, trapdoor functions. Diffie-Helman key exchange, Public-key cryptography, the RSA, the McEliece cryptosystem. Digital signatures, key certification. Probabilistic encryption: Goldwasser-Micali and Blum-Goldwasser. Entropy and Cryptography: perfect security, unicity distance.

## COURSE SCHEDULE

A rough lecture schedule is as follows:

Week 1	Introduction
Weeks 1-3	Error detecting and correcting codes
Weeks 3-5	Compression coding
Weeks 5-6	Information theory
Weeks 7-8	Algebra and number theory (background)
Weeks 8-9	Algebraic coding
Weeks 9-10	Cryptography

A more detailed schedule is available on Moodle.