



DEPARTMENT OF MATHEMATICS

POSTGRADUATE TAUGHT STUDENT HANDBOOK

2011/2012

Telephone +44 (0)1784 443091

Department of Mathematics
Royal Holloway, University of London
Egham Hill, Egham
Surrey TW20 0EX

Disclaimer

This document was published in September 2011 and was correct at that time. The Department* reserves the right to modify any statement if necessary, make variations to the content or methods of delivery of programmes of study, to discontinue programmes, or merge or combine programmes if such actions are reasonably considered to be necessary by the College. Every effort will be made to keep disruption to a minimum, and to give as much notice as possible.

* Please note, the term 'Department' is used to refer to both 'Departments' and 'Schools'. Students on joint or combined degree programmes will need to use two departmental handbooks.

An electronic copy of this handbook can be found on your Departmental website <http://www.ma.rhul.ac.uk/> where it will be possible to follow the hyperlinks to relevant webpages.

Contents

1	INTRODUCTION TO THE DEPARTMENT	5
1.1	WELCOME	5
1.2	HOW TO FIND US: THE DEPARTMENT	7
1.3	MAP OF THE EGHAM CAMPUS	7
1.4	HOW TO FIND US: THE STAFF	8
1.5	HOW TO FIND US: THE DEPARTMENTAL OFFICE	8
1.6	THE DEPARTMENT: PRACTICAL INFORMATION	9
1.7	STAFF RESEARCH INTERESTS	9
2	COMMUNICATION	9
2.1	EMAIL	9
2.2	POST	10
2.3	TELEPHONE AND POSTAL ADDRESS	10
2.4	NOTICE BOARDS	11
2.5	PERSONAL ADVISERS	11
2.6	QUESTIONNAIRES	11
3	TEACHING	11
3.1	DATES OF TERMS	11
3.2	READING WEEKS	11
3.3	ATTENDANCE REQUIREMENTS	11
3.4	NOTIFICATION OF ABSENCE	13
3.5	CONSEQUENCES OF FAILING TO ATTEND	14
3.6	MEETINGS	14
3.7	DISCIPLINARY ACTION	15
3.8	WITHDRAWAL OF VISA	15
4	DEGREE STRUCTURE	17
4.1	LIST OF COURSES	17
4.2	COURSE CHOICES	19
5	FACILITIES	20
5.1	LIBRARIES	20
5.2	PHOTOCOPYING, PRINTING AND COMPUTING	20
6	COURSEWORK ESSAYS AND DISSERTATION	21
6.1	COURSEWORK	21
6.2	THE DISSERTATION	22
6.3	CHOICE OF DISSERTATION TOPIC	22
6.4	THE DISSERTATION SUPERVISOR	22
6.5	PROPOSAL	22
6.6	CONTENT OF DISSERTATION	23
6.7	BIBLIOGRAPHY	23
6.8	MARKING CRITERIA	24
7	ASSESSMENT INFORMATION	25
7.1	ILLNESS OR OTHER EXTENUATING CIRCUMSTANCES	25
7.2	SUBMISSION OF WRITTEN WORK	26
7.3	EXTENSIONS TO DEADLINES	26
7.4	PENALTIES FOR LATE SUBMISSION OF WORK	26
7.5	ANONYMOUS MARKING AND COVER SHEETS	27
7.6	PENALTIES FOR OVER-LENGTH WORK	27

7.7	RETURN OF WRITTEN COURSEWORK.....	28
7.8	PLAGIARISM.....	28
7.9	ASSESSMENT OFFENCES.....	28
7.10	MARKING OF ILLEGIBLE SCRIPTS.....	29
7.11	PROGRESSION AND AWARD REQUIREMENTS.....	29
7.12	EXAMINATION RESULTS.....	30
8	STUDENT SUPPORT.....	31
8.1	STUDENTS IN NEED OF SUPPORT (INCLUDING STUDENTS WITH SPECIAL NEEDS).....	31
8.2	STUDENT-STAFF COMMITTEE.....	31
8.3	STUDENTS' UNION.....	31
8.4	CAREERS INFORMATION.....	32
8.5	NON-ACADEMIC POLICIES.....	32
8.6	COMPLAINTS AND ACADEMIC APPEALS PROCEDURE.....	32
9	HEALTH AND SAFETY INFORMATION.....	32
9.1	CODE OF PRACTICE ON HARASSMENT FOR STUDENTS.....	32
9.2	LONE WORKING POLICY AND PROCEDURES.....	32
10	EQUAL OPPORTUNITIES STATEMENT AND COLLEGE CODES OF PRACTICE.....	33
10.1	EQUAL OPPORTUNITIES STATEMENT.....	33
10.2	COLLEGE CODES OF PRACTICE.....	34
11	COURSE DESCRIPTIONS.....	34

1 Introduction to the Department

1.1 Welcome

Welcome to the **Department of Mathematics**.

This booklet contains important information for graduates registered for a taught degree programme in Mathematics; please read it carefully.

The Department complies with the College Regulations, Student Charter and Codes of Practice. The Codes of Practice cover Academic Welfare, Freedom of Speech, Student Union Affairs, Personal Harassment, and Health and Safety. No interpretation of the information presented here should conflict with these regulations or a Code of Practice. In the case of any apparent difference, the College regulations will prevail.

A satisfactory programme of study at university requires students and the Department to enter an informal 'contract' of obligations and expectations by which all should abide.

What you can expect from us:

The Mathematics Department is committed to effective teaching, but we judge our success in terms of how well you learn. We will do all we can to stimulate your interest in Mathematics, to make the aims of each course clear, to train you by means of interesting coursework and projects, to provide appropriate support, and to monitor and guide your progress. We hope our enthusiasm for the subject will prove infectious and will motivate you to pursue your studies energetically. Most of all, we hope you will find the Department a friendly, supportive and inspiring place in which to work.

You can expect the Department to:

- provide lectures and projects in a series of course units which will make up your degree programme;
- help finding a research topic and a supervisor for your dissertation;
- take reasonable steps to assist students who are disadvantaged through illness or other problems;
- nominate a personal adviser who will act as your point of contact with the Department;

- assess and examine your work;
- provide verbal or written feedback on coursework and drafts of your dissertation where appropriate;
- provide a feedback mechanism for student evaluation of courses through questionnaires;
- provide reasonable notice of all coursework deadlines at lectures or electronically;
- treat all students in a fair and just manner without any form of prejudice.

What we expect from you:

Your degree course should challenge you to deal with difficult concepts, to become skilled in new and demanding techniques, and to push your intellectual powers to the limit. If not, then you will not have used your opportunity to the full. The MSc and PgDip programmes aim to provide students with a solid mathematical foundation and a knowledge and understanding of the subjects of cryptography and communications, and various applications of mathematics, as appropriate. Students who successfully complete the programme will be prepared for research or professional employment in these areas.

Employers and PhD supervisors are not only interested in the knowledge you have acquired, though knowledge is obviously relevant to careers in mathematics. They are also interested in personal qualities like self-reliance and initiative, and in your capacity to think rationally and independently, to work in a team, to write clear reports within a firm deadline, and so on.

These qualities cannot be taught. They depend on many factors, among them the energy you put into your studies and the drive with which you pursue your career goals. We want you to enjoy your studies and your time here; when you enjoy what you do, you will work harder and learn more effectively.

You are expected to:

- attend all lectures, workshops and tutorials;
- keep your personal adviser fully informed of any problems which may affect your studies;
- complete all coursework and attend all examinations;

1.4 How to find us: the staff

Academic staff all have offices in the McCrea Building. You should only visit them during their office hours; these are posted on the door of their office and on the Department's website. If you cannot visit during office hours, please email the staff member asking for an appointment and saying when you are free.

There is a staff list with office information on the Department's website, and in the foyer of the McCrea Building.

If you have problems, the following list shows who to contact:

- **Course units** – the lecturer
- **Course selection** – your personal adviser
- **Your degree programme** – your personal adviser and the MSc Programme director
- **A personal problem** – your personal adviser, or the Welfare Services (Counsellors, Health Centre, Chaplaincy, Student Union)
- **A problem common to other students** – the lecturer, your Student-Staff Committee representative
- **College registration, enrolment, fees, accommodation, loans etc.** – the Student Administration Centre, Crosslands Bungalow

Your key contacts for 2011-12 are:

- **Personal Adviser:** You will be allocated a Personal Adviser during Induction week (see 2.5 for the role of Personal Advisers)
- **Senior Faculty Administrator:** Mr Guillaume Subra 01784 443085
guillaume.subra@rhul.ac.uk
- **Computer Technical Support:** Ms Lisa Nixon 01784 443106
lisa.nixon@rhul.ac.uk
- **MSc Programme director:** Dr Teo Sharia, 01784 414331
t.sharia@rhul.ac.uk
- **Special Needs Coordinator:** Mr Guillaume Subra
- **Health and Safety Coordinator:** Mr Guillaume Subra

1.5 How to find us: the Departmental office

The Departmental Office is in room C243. The office's opening hours will be posted on the door of C243. You can phone the Office on 01784 44 3091/3093, or you can email maths@rhul.ac.uk.

1.6 The Department: practical information

Safety. Please make yourself aware of the procedure for fire evacuation. The Mathematics Assembly Point is between McCrea and Horton, at Fire Assembly Point 11.

Smoking. Please note that smoking is not allowed in the McCrea Building.

1.7 Staff research interests

The research interests in the Department include information security, cryptography, coding theory, algebra, number theory, graph theory, the mathematics of atomic processes, quantum theory, quantum information theory, and statistics.

2 Communication

It is vitally important that you keep in touch with us and we keep in touch with you. Members of staff will often need to be able to contact you to inform you about changes to teaching arrangements, special preparations you may have to do for a class or meetings you might be required to attend. You will need to be able to contact members of the Department for example, if you are unable to attend a class, or wish to arrange a meeting with a tutor or your Personal Adviser.

Email to your College email address is routinely used and **you should check regularly** (at least daily) if any official communication has been sent to your email address. **Do not** ignore the email as it will be assumed that it will have been received by you within 48 hours, excluding Saturdays and Sundays.

You should also make a habit of checking the student pigeonholes in the Department.

2.1 Email

The College provides an email address for all students free of charge and stores the address in a College email directory (the Global Address List). Your account is easily accessed, both on and off campus, via the **student portal** <https://campus-connect.rhul.ac.uk/> (Campus Connect) or direct via **Outlook.com** <http://outlook.com/> **Email to this address will be used routinely for all communication with students.** Email may be used for urgent communication and by course tutors to give or confirm instructions or information related to teaching so it is important that you

build into your routine that you **check your emails once a day**. Email communications from staff and all the Faculty Administrators should be treated as important and read carefully.

The College provides a number of PC Labs around Campus for student use, and you can also use your own laptop/smart phone etc, so the Department expects you to check your email regularly. It is also important that you regularly clear your College account of unwanted messages or your in-box may become full and unable to accept messages. **Just deleting messages is not sufficient; you must clear the 'Sent Items' and 'Deleted Items' folders regularly. It is your responsibility to make sure your College email account is kept in working order.** If you have any problems contact the **IT Service Desk** <http://itservicedesk.rhul.ac.uk/>

The Mathematics Department will only use the address in the College Global Address List and **does not** use private or commercial email addresses, such as hotmail or Gmail. Students who prefer to use commercial email services are responsible for making sure that their College email is diverted to the appropriate commercial address. Detailed instructions on how to forward mail can be accessed by visiting <http://help.outlook.com/> and searching for **forwarding**. This process is very easy, but you do have to maintain your College account. When you delete a forwarded message from, say, hotmail, it will not be deleted from the RHUL account. You **must** log on to your College account occasionally and conduct some account maintenance or your account may become full and therefore will not forward messages.

If you send an email to a member of staff in the Department during term time you should normally receive a reply within 3-4 working days of its receipt. Please remember that there are times when members of staff are away from College at conferences or undertaking research.

2.2 Post

All post addressed to MSc students in the Mathematics Department is delivered to the student pigeonholes (alphabetical by surname) in C254. At the end of each term student pigeonholes are cleared of accumulated mail which is then destroyed. Important information from Registry is often sent by internal post and tutors sometimes return work to you via the pigeonholes so you are advised to check them regularly.

2.3 Telephone and postal address

It is **your responsibility** to ensure that your telephone number (mobile and landline) and postal address (term-time and forwarding) are kept up to date on the **student portal** (Campus Connect) <https://campus->

connect.rhul.ac.uk/. There are occasions when the Department needs to contact you urgently by telephone or send you a letter by post.

The Department does not disclose students' addresses and telephone numbers to anybody else (including relatives and fellow students) without the student's specific permission to do so.

2.4 Notice boards

The general student noticeboards are in the foyer of the McCrea building. There is a noticeboard especially for MSc students in McCrea between rooms C250 and C253.

Every effort is made to post notices relating to class times etc well in advance, but occasionally changes have to be made at short notice and in that case email will be used.

It is your responsibility to check the times and venues of all class meetings and of any requirements (e.g. essay deadlines) relating to your courses, so, if in doubt, please ask!

2.5 Personal Advisers

Each student has a personal adviser. The personal adviser may help with course choices, and with finding a dissertation topic and supervisor. The adviser provides a point of contact between students and the Mathematics Department.

2.6 Questionnaires

Towards the end of each teaching term there will be a questionnaire for each course. At the end of the programme we will ask the students to fill out a questionnaire to evaluate the entire programme.

3 Teaching

3.1 Dates of terms

Term dates can be found on the College website
<http://www.rhul.ac.uk/aboutus/collegecalendar/home.aspx>

3.2 Reading weeks

There are no reading weeks during term times.

3.3 Attendance requirements

The Department monitors your attendance, academic engagement

and progress in order to offer you appropriate academic and pastoral support and to identify where support from outside the Department may be necessary. Inadequate engagement on a course may lead to disciplinary action which can result in the termination of your registration (see section on [Disciplinary action](#)) or the award of an Incomplete (IN) on a course.

Students **must**

- attend all classes necessary for the pursuit of their studies,
- undertake all assessments,
- attend meetings and other activities as required by the Department.

A class is any learning and teaching activity and the term is used to encompass such things as lectures, seminars, tutorials, workshop, field work, laboratories, advisor meetings etc. This means not simply turning up – but arriving having undertaken whatever reading, thinking, or research was identified as necessary preparation. You are also expected to arrive punctually - teaching activities are timetabled to start at 5 minutes past the hour and finish 5 minutes before the hour. You may be marked absent if you turn up late without good reason.

The Department will monitor your attendance at all parts of the course(s) for which you are registered. It is your responsibility to complete any attendance register that is circulated and to make sure that your attendance has been noted. The activities at which your attendance is monitored may vary depending upon the discipline in which you are studying.

It is important that you attend all the learning activities related to your programme of study. Whilst attendance is compulsory at all learning activities it is recognised that emergencies may occur at any time throughout the year and therefore a minimum 80% attendance level has been set. You should also be aware that there may be some courses which you study which have a specific course attendance requirement. If you face difficulty in attending any classes or undertaking an assessment it is your responsibility to inform the Department(s) in which you are studying and provide a satisfactory explanation. As long as you are meticulous in your honesty in reporting and explaining these exceptions, we aim to be understanding in our response.

You must manage your time so that any paid employment, voluntary or other activities fit into the times when you are not required to be in a class. You are reminded that PG Regulations stipulate that the amount of paid work undertaken by a student enrolled with the College on a full-time basis shall not exceed 20 hours per week during term time. No

student may undertake paid work which may conflict with his/her responsibilities as a student of the College.

If you are having other problems that are causing you to miss classes, you should talk to your Personal Adviser, year tutor or another member of staff, or visit the Student Advisory Service or **Students' Union** before your problems get out of control. There are many people who can provide **Support** on <http://www.rhul.ac.uk/forstudents/home.aspx> and <http://www.su.rhul.ac.uk/support/> but remember - they cannot help if you do not ask.

In recognition of its legal responsibilities under the Equality Act 2010, the College may adjust the attendance requirement. It will only do this when such adjustment does not compromise competence standards or the ability of the student to reach the learning outcomes of the course. Any need to adjust attendance requirements will be treated on a case by case basis and discussed by the Department with the Educational Support Office and Academic Development Services.

3.4 Notification of absence

This guidance applies if you are absent from classes for any reason.

You must

- a. advise your department(s). This is done by sending an email to MathsAttendance@rhul.ac.uk,
- b. submit doctor's note to your department(s) either before your absence or within TWO working days of the end of the period of absence. Failure to do so may result in the absence being counted as unacceptable and counting against the minimum attendance level,
- c. ensure that you meet any departmental requirements concerning notification of absence or request for leave of absence as you may be required to meet formally with an academic tutor.

This table shows the documentation that is required should you be absent for any reason.

Reason for absence	Documentation required
Illness up to and including 5 consecutive term-time days (excluding Saturdays and Sundays)	Completed Notification of Absence Form – Self Certification
Illness for more than 5 consecutive term-time days (excluding Saturdays and Sundays)	Completed Notification of Absence Form - Self Certification plus Formal Medical Certification signed by the Health Centre, your GP or hospital consultant
Unrelated to sickness	Notification of Absence Form plus supporting evidence (see www.rhul.ac.uk/attendance for details of required evidence)
Leave of absence request	Notification of Absence Form plus any

Note:

- If you should be absent for a prolonged period it is important that you keep in touch with your department.
- Departments will monitor the frequency of self-certified absences and a Head of Department may request that you provide a doctor's medical certificate in multiple and sustained instances of self-certified illness.
- It is at the discretion of the Department as to whether any absence is deemed acceptable or unacceptable (see www.rhul.ac.uk/attendance for details of required evidence) for details of 'acceptable' and 'unacceptable' absences). If deemed unacceptable the absence will be recorded as such and will count against the minimum attendance level.

If you are absent from an examination or assessment then you must follow the guidance in the [Essential Examinations Information](#).

<http://www.rhul.ac.uk/registry/Examinations/Essential-info.html> (see also the section on [Assessment information](#))

For further details on the kinds of circumstances where absence may be deemed as 'acceptable' and 'unacceptable' and for the type of supporting evidence that you may be required to provide as justification of absence, please click on 'Studying' tab on the Student Home page. www.rhul.ac.uk/attendance.

3.5 Consequences of failing to attend

Where, in the absence of a satisfactory and adequately documented reason, a student has failed to satisfy the requirements for attendance or submission of work specified for one or more courses, the Head of Department or School responsible for the course may terminate that student's registration for the course.

3.6 Meetings

You are likely to be 'invited' to meet with a member of academic staff in your department:

- if you fail to attend all learning activities in two consecutive weeks without providing an explanation
- where your pattern of absences is:
 - considered to be having an effect your work or causing concern for the your well being
 - pointing to a possible disability that you may not have disclosed

- where your attendance is approaching the minimum attendance level

You should take any meeting 'invitation' seriously. If you should have problems you are being offered an opportunity to seek advice and assistance. At the meeting the Department's expectation of you will be made clear and the formal disciplinary process will be outlined to you.

3.7 Disciplinary action

Should you choose not to pay attention to your studies then formal disciplinary action may be implemented. You could be issued with a formal warning which can escalate to the termination of your registration at the College

(<http://www.rhul.ac.uk/forstudents/studying/academicregulations/ugregs/ugtermination.aspx>).

On courses where there is a specified attendance level requirement the Departmental Sub-Board of Examiners may judge that you have not fulfilled the learning outcomes of a course and award the outcome of IN (Incomplete) for the course. Students who receive the outcome of IN for a course have not passed the course; they are not permitted to re-sit the assessment for the course and must repeat the course in attendance in order to complete it.

In situations where documented severe difficulties are experienced by a student the College will make every effort to support the student and counsel them as to the best course of action. However, there may be cases where, although non-attendance is explained by an acceptable reason the student's level of attendance falls to a level which compromises educational standards or the ability of the student to reach the learning outcomes of the course. In such cases it will be necessary to implement disciplinary procedures as detailed above.

3.8 Withdrawal of visa

If you are in receipt of a Tier 4 visa you should be aware that it a **legal requirement for Royal Holloway to report any student admitted to the College on a student visa who does not appear to be in attendance to the UK Border Agency**. Such students will be issued with warnings, both formal and informal, and failure to respond to these warnings will result in the College notifying the UK Border Agency and the student having their student visa withdrawn. Please see the College **Postgraduate Regulations**

<http://www.rhul.ac.uk/forstudents/studying/academicregulations/home.aspx>

4 Degree Structure

The *full time* MSc lasts for 50 weeks, from late September until beginning of September of the following year. The *full time* PgDip lasts from late September until early June of the following year.

The MSc is examined in two parts; by written examination (mainly in May), and by a dissertation on a main project to be submitted early in September. This is called the main project to distinguish it from any projects that form part of a course unit. The PgDip has the same course structure but there is no main project.

Students initially choose 8 courses of which they specify 6 courses (including the core courses below) during the second term that will count towards the examination. The two unspecified courses are 'electives'. Elective courses appear on students' transcripts but do not contribute to the final degree classification. The 6 specified courses count as a half unit each. The main project counts as a full unit, so that each MSc student will be examined on $6 \times 0.5 + 1 = 4$ units and PgDip students will be examined on $6 \times 0.5 = 3$ units.

Students write at least the 6 examination papers of their specified courses but may choose to write examination papers in their elective courses in addition. The marks for the elective courses will appear on their transcript but do not count towards the degree classification.

A *part time* MSc lasts for 102 weeks, from September to September two years later. The normal outline is:

Year 1: lectures and examinations on four half-units (typically the core courses). A student must pass 1.5 units in order to proceed to Year 2.

Year 2: four more half-units followed by the main project.

The Examinations office will probably ask you to specify the examination papers that you intend to write very early. The reason is the involved exam timetable. In the past, the department was able to negotiate a later deadline, watch out for information (by email) from the programme director.

4.1 List of Courses

Core Courses on the MSc Mathematics for Applications

Code	Title	Term	Lecturer
MT5400	Main Project	Summer	
MT5462	Advanced Cipher Systems	1	Dr Ng
MT5461	Theory of Error Correcting Codes	2	Dr Wildon

Core Courses on the MSc Mathematics of Cryptography and Communications

Code	Title	Term	Lecturer
MT5400	Main Project	Summer	
MT5441	Channels	1	Dr Barrett
MT5462	Advanced Cipher Systems	1	Dr Ng
MT5461	Theory of Error Correcting Codes	2	Dr Wildon
MT5466	Public Key Cryptography	2	Prof Blackburn

Courses

Code	Title	Term	Lecturer
MT5400	Main Project	Summer	
MT5412	Computational Number Theory	1	Dr Busuioc
MT5441	Channels	1	Dr Barrett
MT5454	Combinatorics	1	Dr Wildon
MT5462	Advanced Cipher Systems	1	Dr Ng
MT5413	Complexity Theory	2	TBA
MT5420	Quantum Theory II	2	Dr Bolte
MT5447	Advanced Financial Mathematics	2	Dr Sheer
MT5461	Theory of Error Correcting Codes	2	Dr Wildon
MT5466	Public Key Cryptography	2	Prof Blackburn
MT5485	Applications of Field Theory	2	Dr Klopsch

Note that some courses consist of 3 lectures a week, and others consist of 4 lectures a week. Courses with 4 lectures a week: MT5461, MT5462. Ask the lecturer for details.

This booklet gives descriptions of all postgraduate (MT5xxx) courses. Note that many of these courses coincide with fourth year MSci courses, though for MSci students the course numbers are different but related: for example MT5485 (MSc) is the same as MT4850 (MSci).

The following final year undergraduate, and MSc courses may be relevant. The syllabi are on the web sites

<http://www.ma.rhul.ac.uk/courses201112/year3>

and

<http://www.isg.rhul.ac.uk/msc/modules>

<i>Code</i>	<i>Title</i>	<i>Term</i>
MT3200	Quantum Theory I	1
MT3220	Dynamics of Real Fluids	1
MT3320	Inference	1
MT3340	Time Series Analysis	1
MT3470	Mathematics of Financial Markets	1
MT3110	Number Theory	2
MT3280	Non-Linear Dynamical Systems	2
MT3360	Applied Probability	2
IY5511	Network Security	1
IY5512	Computer Security	1
IY5604	Database Security	2
IY5605	Computer Crime	2
IY5607	Software Security	2

4.2 Course choices

Each student must take the core courses listed above and choose further courses such that each student attends lectures on 8 taught half units. MSc students write a dissertation in addition.

At the discretion of the Programme Director, the requirement to take a core course may be dropped if a student has already taken an equivalent course at a comparable level as part of their previous studies (in which case the student will take an extra optional course).

A full list of other optional courses is also given above. Recommended optional courses for the MSc of Cryptography and Communications are Applications of Finite Fields (MT5485), Computational Number Theory (MT5412), Complexity Theory (MT5413), and Combinatorics (MT5454). Students on the MSc Mathematics for Applications may choose from the whole range of MT5xxx courses.

A student may also, in agreement with the Programme Director, choose one course from the third year options of the undergraduate degree programme in Mathematics (MT3xxx range), and one from the list of MSc courses in Information Security (IY5xxx range). Normally, permission will only be given if the material has not been covered as part of their previous studies. Note that these courses can only be taken as 'electives', and the marks obtained in such courses cannot be included in the calculation of the degree classification.

All MSc students (but not PgDip students) will do a main project, which is a major piece of independent study. This project work will be undertaken

under the supervision of a member of staff. The assessment will be on the basis of a written dissertation; the examiners may also at their discretion require an oral examination. Please refer to Section 6.2 for more information on the dissertation. The dissertation must be submitted by the first Thursday of September of the calendar year of completion of the written part of the examination by 2pm (14:00).

5 Facilities

5.1 Libraries

The Bedford Library is adjacent to the McCrea building and has a full range of relevant mathematics and computer science books and journals. There is an online library catalogue and the Department also subscribes to a number of electronic journals, which students are encouraged to use.

5.2 Photocopying, printing and computing

Room C254 on the second floor of the McCrea building is a common room for all the MSc students in the Mathematics Department. This room contains a photocopier which can be used by all MSc students. It also contains a ring-binding machine which may be used for your dissertation. As well as the PCs available in C103 (shared with the Computer Science Department) and C356, you have access to PCs in the Computer Centre, the library and elsewhere on campus. For access to the PC's in the MSc room C254 you need to sign an extra form, please see Lisa Nixon in C243. Details of all the Department computer facilities are available on the Department website:

<http://www.ma.rhul.ac.uk/students/it>

You will be given a department printing allowance each teaching term, which may be used to print on departmental and Computer Centre printers. Once the departmental allowance has been used additional print credit may be purchased from the Computer Centre service desk or credit machines around campus. Please note that the departmental allowance is used in preference to any personal credit a user may have. Please do not disclose your password to anyone or permit anyone else to use your account. Always ensure you have logged off whenever you have finished using a computer. Department print credit will not be refunded if you forget to logout and someone else uses your account. Further details about the Department printing allowance are available from the website above.

Departmental support for any hardware or software issues can be obtained from the Department IT helpdesk at

<https://helpdesk.ma.rhul.ac.uk>.

Use of the Departments computer facilities is subject to the Computer Centre regulations as listed on the Computer Centre website:

<http://www.rhul.ac.uk/Information-Services/Computer-Centre/>

Please note the Department operates a no food or drink policy within the computer laboratories. Breaches of these regulations are treated very seriously and may result in withdrawal of access to facilities.

Online resources, Moodle

Moodle is Royal Holloway's Virtual Learning Environment. Lecturers for most of our courses use Moodle for providing information: course details, announcements, worksheets, project materials, useful links, and so on.

Many lecturers use Moodle (<http://moodle.rhul.ac.uk/>) to post their weekly problem sheets or other information on the course. Some departmental online resources, for example previous exams, are at

<http://www.ma.rhul.ac.uk/static/PastExams/>

The library also has many online resources that may be of use for your course.

6 Coursework Essays and Dissertation

6.1 Coursework

There are homework exercises for each course. These are distributed during lectures or are available on the course page on Moodle. Each lecturer will specify when and how the homework has to be submitted. The homework exercises are marked but these marks do not contribute to the final grade for the course.

Solving problems is an essential part of the learning process in mathematics. The homework exercises are designed to reinforce and progressively develop the ability to solve problems in mathematics. Some problems are harder than others, and students should not necessarily expect to solve every exercise on every sheet.

It is a college regulation that all course work is completed and submitted for assessment. Failure to comply may lead to a formal warning and the award of incomplete or non-examined status on that course.

If, due to illness or another good cause, students fail to attend an examination or their performance is affected, the record of their homework marks will be taken into account.

6.2 The dissertation

The dissertation accounts for 25% of the assessment for the MSc degree. Two bound hard-copies of the dissertation have to be submitted to the secretaries in McCrea 243 by 2pm on the first Thursday of September in the year of the written examination. You should plan to work conscientiously throughout the summer if you are to produce a satisfactory dissertation by the September deadline. You are reminded that the MSc course is full time education until beginning of September (unless you have part time status) and that you are not supposed to take on any commitment during the summer that prevents you from spending most of your time on the dissertation.

Students are advised to use Latex or Word for preparing the MSc dissertation. Latex is particularly suitable for mathematical content and we encourage the use of it. For some help please see <http://www.ma.rhul.ac.uk/latex-help> .

The dissertation is usually of length between 8,000 and 16,000 words. The margins should be at least 2cm wide and the font size 11pt. Two bound hard-copies of the thesis have to be submitted. Students may use the ring-binder provided in the MSc common room. You can find some of the dissertations by students of previous years in the mathematics office C243 to get an idea how they look like.

6.3 Choice of dissertation topic

The first task, which should be completed by the middle of term 2, is to decide upon a general area of research (this can be rather vague, e.g., coding theory, symmetric cryptography, quantum computing etc.) and a suitable project supervisor.

6.4 The dissertation supervisor

Course lecturers, the adviser and the programme director may help in suggesting research areas and finding a supervisor. The supervisor will help the student to find a specific topic in the area of the student's interest. Note that students are not guaranteed the supervisor of their choice, though we try to ensure that all students have a supervisor who is willing to supervise the student's chosen topic. If you are unable to find a supervisor or a research area then you should see the programme director during the first half of term 2.

6.5 Proposal

By the end of term 2 (last week of lectures) students should produce a brief research proposal, of about 10 pages. This should give an introduction to the general subject area and of the more specific problems and objectives to be studied. It should mention which literature has been studied so far and how

the research will continue. This will usually be prepared in consultation with the project supervisor.

While this proposal does not count toward the final grade it is still compulsory part of the dissertation. The research proposals are approved by the external examiner for the MSc programme at the Examinations Sub-Board meeting in June. Failure to complete a satisfactory proposal may result in the student being moved from the MSc programme to the PgDip.

6.6 Content of dissertation

The final part of the main project is to prepare the dissertation. It is important to allow plenty of time for this stage (typically at least one month). It is usually best not to leave writing of the entire dissertation to the end but to write parts of it during the summer. Usually your supervisor will read one draft version, (but will not usually read the same chapter several times) if it is given to her/him in good time. The students may want to give draft parts to the supervisor at earlier stages and not the entire dissertation towards the end of project.

The dissertation must include:

- Title page.
- Abstract (or Summary), which explains the aims of the dissertation and summarises the results.
- An introduction which outlines and motivates the topic of the thesis.
- A discussion of the existing literature on the subject.
- A presentation of the original content of the project, with a full explanation of the methods used and outcomes obtained.
- Conclusions which describe how the results relate to the wider subject area and/or suggests some possible future lines of enquiry.
- Bibliography

6.7 Bibliography

It is crucial to properly acknowledge other people's work. The bibliography usually consists of a list of publications in alphabetical order of the author's names. Each entry contains at least the author's names, the title of the publication, the journal, publisher or website, the year of publication and in case of a journal article, the volume and the page numbers of the entire article. It is unusual to quote verbatim in mathematics (apart from definitions, lemmas and theorems), and one usually refers to the entire article if one is

using a result of it. Sometimes when citing long articles or books it is helpful if one refers to a particular theorem. If you use material from websites you must reference the sites.

The supervisor will give feedback on your citing, referencing and the bibliography if she/he is given a draft.

6.8 Marking criteria

Each dissertation is independently marked by two examiners; one of these is normally the supervisor. An external examiner moderates the assessment. The examiners may conduct an oral examination if they wish to check the depth of the student's understanding and to ensure that the dissertation is the student's own work. **Student must obtain a pass grade on the dissertation to pass the MSc degree.** The examiners give up to 100 points where the points translate to the following categories:

- 85–100:** An exceptionally high level of understanding and outstanding research potential.
- 70–84.99:** Very high competence and excellent research potential.
- 60–69.99:** Evidence of some creativity and independence of thought.
- 50–59.99:** Sound understanding of the literature, but lack of accuracy or originality.
- 0–49.99:** Insufficient or no understanding of the topic, poor quality of work.

The points are given according to the following guidelines:

Knowledge of subject (25)

- 21–25:** Deep understanding and near-comprehensive knowledge
- 18–20:** Deep understanding
- 15–17:** Very good understanding
- 12–14:** Sound knowledge of relevant information
- 10–11:** Basic understanding of the main issues
- 0–9:** Little or no understanding of the main issues

Organisation of material (25)

- 21–25:** Of publishable quality
- 18–20:** Arguments clearly constructed; material very well-organised
- 15–17:** Well-organised; aims met with no significant errors or omissions
- 12–14:** Coherent and competent organisation
- 10–11:** Lack of clarity in written presentation or aims only partially met
- 6–9:** Major flaws in arguments; aims of project not met
- 0–5:** Arguments are missing/deficient. Disorganised or fragmentary

Originality, interpretation and analysis (20)

- 17–20:** Significant originality in the interpretation and/or analysis; project aims challenging
- 14–16:** Some originality; evidence of excellent analytical and problem-solving skills
- 12–13:** Good attempt to interpret and analyse existing literature
- 10–11:** Minor flaws in interpretation/analysis of existing literature
- 5–9:** Poor interpretation/analysis or project aims too simple
- 0–4:** Little or no interpretation or analysis; project aims trivial

Evidence of reading (10)

- 8–10:** Independent reading including research papers
- 6–7:** Good use of outside reading
- 4–5:** Some evidence of outside reading
- 0–3:** Little or no evidence of outside reading

Bibliography and referencing (10)

- 9–10:** Of publishable quality
- 7–8:** Good referencing and bibliography
- 5–6:** Either poor bibliography or poor referencing
- 3–4:** Poor bibliography and little or no referencing
- 0–2:** No bibliography and little or no referencing

Style, spelling, punctuation and grammar (10)

- 9–10:** Incisive and fluent, no errors of spelling, punctuation or grammar
- 7–8:** Very minor errors of spelling, punctuation or grammar
- 4–6:** Some errors of spelling, punctuation or grammar
- 0–3:** Many errors of spelling, punctuation or grammar

7 Assessment Information

7.1 Illness or other extenuating circumstances

If you are taken ill or there are other extenuating circumstances that you believe have adversely affected your performance in relation to any aspect of your course/programme (for example, your attendance, submission of work, or examination performance) at any point during the academic year, you must inform your department(s)/school(s) in writing, and provide the appropriate evidence. Please read the “**Instructions to Candidates**” issued by the Examinations Office <http://www.rhul.ac.uk/registry/Examinations/Essential-info.html> for full details on how and when to inform your department about such circumstances as well as the **deadline for submission of such information**.

Absence from an examination / failure to submit coursework

If you miss an examination or fail to submit a piece of assessed coursework without acceptable cause, this will normally be given an outcome of 'Incomplete'.

If you miss an examination or fail to submit a piece of assessed coursework through illness, or other acceptable cause for which adequate documentation is provided in accordance with the section on **Illness or other extenuating circumstances** in the **Instructions to Candidates** the Sub-board of Examiners may take this into account when considering your results.

Special arrangements for examinations for disabled students and those in need of support

For all such students there is a process to apply for special arrangements for your examinations and other forms of assessment. Such requests should be made to the Educational Support Office (ESO) which will carry out an assessment of your needs. Please see the section **Students in need of support** (*including disabled students*) for further guidance about registering with the Educational Support Office.

7.2 Submission of written work

Usually homework assignments are collected during lectures but some lecturers may have different arrangements of which they will inform the students at the beginning of the course. The dissertation resulting from the main project must be given to the secretaries in C243 during the office hours by 2pm on the first Thursday of September in the year of the written exams.

7.3 Extensions to deadlines

An extension to a deadline can only be given if there are extenuating circumstances. A written request to extend the deadline must reach the programme director before the deadline.

7.4 Penalties for late submission of work

The following College policy applies to all students on taught programmes of study.

All coursework should be submitted by the specified deadline. Please ensure that you are aware of the deadlines set by your department(s). Work that is submitted after the deadline will be penalised as follows:

- For work submitted up to 24 hours late, the mark will be reduced by ten percentage marks* subject to a minimum mark of a minimum pass;
- For work submitted more than 24 hours late, the maximum mark will be zero.

*e.g. an awarded mark of 65% would be reduced to 55%.

If you have had extenuating circumstances which have affected your ability to submit work by the deadline these should be submitted in writing, accompanied by any relevant documentary evidence, to your department(s). As with all extenuating circumstances it is the discretion of the examiners whether to accept these as a reason for having not submitted work on time. Please see the section on applying for an **extension to the deadlines** set, and the section for details on **submitting requests for extenuating circumstances** to be considered.

7.5 Anonymous marking and cover sheets

All work that is submitted for assessment is marked anonymously. The only exception to this is the main project.

7.6 Penalties for over-length work

The dissertation on the main project is usually of length between 8,000 and 16,000 words. A modern word-processing program (e.g. LaTeX or Word) should be used. The margins should be at least 2cm wide and the font size 11pt.

The following College policy applies to all students on taught programmes of study:

All over-length work submitted on undergraduate and taught postgraduate programmes will be penalised as follows:

- For work which exceeds the upper word limit by at least 10% and by less than 20%, the mark will be reduced by ten percentage marks*, subject to a minimum mark of a minimum pass.
- For work which exceeds the upper word limit by 20% or more, the maximum mark will be zero.

*e.g. an awarded mark of 65% would be reduced to 55%.

In addition to the text, the word count should include quotations and footnotes. Please note that the following are excluded from the word count: candidate number, title, course title, preliminary pages, bibliography and appendices.

7.7 Return of written coursework

The following College policy applies to the return of coursework:

Assessed work (other than formal examinations) should be returned within 4 weeks of the submission deadline, except in cases where it is not appropriate to do so for academic reasons. The deadline for the return of marked work should be made clear to students when they receive their assignments.

7.8 Plagiarism

Definition of plagiarism

'Plagiarism' means the presentation of another person's work in any quantity without adequately identifying it and citing its source in a way which is consistent with good scholarly practice in the discipline and commensurate with the level of professional conduct expected from the student. The source which is plagiarised may take any form (including words, graphs and images, musical texts, data, source code, ideas or judgements) and may exist in any published or unpublished medium, including the internet.

Plagiarism may occur in any piece of work presented by a student, including examination scripts, although standards for citation of sources may vary dependent on the method of assessment. Group working would constitute plagiarism where the discipline or the method of assessment emphasises independent study and collective ideas are presented as uniquely those of the individual submitting the work.

Identifying plagiarism is a matter of expert academic judgement, based on a comparison across the student's work and on knowledge of sources, practices and expectations for professional conduct in the discipline. Therefore it is possible to determine that an offence has occurred from an assessment of the student's work alone, without reference to further evidence.

7.9 Assessment offences

The College has regulations governing **assessment offences** which can be found on the following website:

<http://www.rhul.ac.uk/forstudents/studying/academicregulations/home.aspx>.

Offences include plagiarism, duplication of work, falsification, collusion, failure to comply with the rules governing assessment (including those set out in the 'Instructions to candidates'). The Regulations set out the procedures for investigation into allegations of an offence and the penalties for such offences.

7.10 Marking of illegible scripts

It is College policy not to mark scripts which are illegible. If you anticipate that you may have difficulty in handwriting scripts which would lead to your scripts being illegible you should contact the **Educational Support Office**.

<http://www.rhul.ac.uk/studentlife/supporthealthandwelfare/eso.aspx>

7.11 Progression and award requirements

The Regulations governing progression and award requirements are set out in your Programme Specification (PS) which can be found on the following website:

PS for MSc in Mathematics of Cryptography & Communications

[http://www.rhul.ac.uk/mathematics/coursefinder/mscmathematicsofcryptographyandcommunications\(msc\).aspx](http://www.rhul.ac.uk/mathematics/coursefinder/mscmathematicsofcryptographyandcommunications(msc).aspx)

PS for MSc in Mathematics for Applications

<http://www.rhul.ac.uk/mathematics/coursefinder/MScMathematicsforApplications.aspx>

Also, more generally, the regulations can be found in the **Postgraduate Regulations** http://www.rhul.ac.uk/Registry/academic_regulations/

If you do not pass a course unit at a first attempt you may be given an opportunity to 're-sit' or 'repeat' the course unit.

Re-sit of a failed unit - Normally the opportunity to re-sit any failed parts of a course unit not passed will be during the following academic session.

Repeat - If you are given the opportunity to repeat a course unit you will need to register for the course unit for the next academic session and satisfy afresh the coursework and attendance requirements.

Please note that it is **not** possible to re-sit or repeat a course unit which you have passed.

NB: Students entered to resit an examination will normally not receive an overall percentage mark greater than 50% for that course unit.

Outcomes of course unit assessment

The Postgraduate Regulations require that for a student to qualify for final consideration in a course unit by the Sub-board of Examiners, a candidate must first:

- (a) have satisfied the attendance requirements specified for the course;
- (b) have completed and presented for assessment all work specified for the course within specified deadlines.

The Sub-board of Examiners will determine an outcome and a percentage mark recorded as an integer between 0% and 100% inclusive for each candidate who qualifies for final consideration, as follows:

- (a) an outcome of Pass (P) with a percentage mark will be returned where the candidate has gained a mark of 50% or above overall and in all elements of the assessment which carry an individual pass requirement;
- (b) an outcome of Fail (F) with a percentage mark will be returned where the candidate has gained a mark of less than 50% overall or in any element of the assessment which carries an individual pass requirement.

The assessment of a candidate who does not qualify for final consideration will be marked Incomplete (IN) without a percentage mark.

For details on the requirements governing the level of award please see the section on the **Consideration and Classification of Candidates for the Award** in the Postgraduate Regulations.

<http://www.rhul.ac.uk/forstudents/studying/academicregulations/pgregs/pgawardofpgt.aspx>

7.12 Examination results

Please see the **Examinations Office** webpage

<http://www.rhul.ac.uk/registry/Examinations/> for details of how you will be issued with your **results**.

<http://www.rhul.ac.uk/registry/Examinations/results.html>

The Examinations website is the place where you can access the **“Instructions to Candidates”** and details of the examinations appeals procedures.

8 Student Support

8.1 Students in need of support (including students with special needs)

Your first point of reference for advice within the Department is the Senior Faculty Administrator Mr Guillaume Subra. Inevitably, problems will sometimes arise that the Senior Faculty Administrator is not qualified to deal with. The College offers a high level of student welfare support which includes a comprehensive Health Centre, a highly regarded Counselling Service, dedicated educational and disability support, as well as a wealth of financial, career and other advice. Further details of each service can be found on the College web on the **Student Support** page:

<http://www.rhul.ac.uk/forstudents/home.aspx>

If you have a disability or specific learning difficulty, it is important that you bring it to our attention as soon as possible. The Departmental Educational Support Office (ESO) representative is the Senior Faculty Administrator. You must also contact the ESO (Founders East 151; tel: +44 (0)1784 443966; email: educational-support@rhul.ac.uk) who will arrange for an assessment of needs to be carried out and will advise on appropriate sources of help. Further information is available on the College web on the ESO **Support, health and welfare** page

<http://www.rhul.ac.uk/studentlife/supporthealthandwelfare/eso.aspx>

8.2 Student-staff committee

There is a student-staff committee on which both taught and research students are represented. The Committee meets at least once every teaching term and plays an important role in the Department as a forum for airing student views. You can use the Committee to raise any issues which concern students. Notices will appear on departmental notice boards giving details of forthcoming elections or the names of current representatives.

8.3 Students' Union

The **Students' Union** offers a wide range of services and support, from entertainment and clubs/societies to advice on welfare and academic issues. The Advice and Support Centre, situated on the first floor of the Students' Union, runs a confidential service that is independent from the College. Open 9.30am - 5pm, Monday – Friday, it operates an open door policy exclusively for students during term time. However, during vacation periods students should call to book an appointment. Full

details can be found at www.su.rhul.ac.uk/support

8.4 Careers information

The College has a **careers advisory service**, housed in the Horton Building, which is open to any student during normal College hours.

<http://www.rhul.ac.uk/careers/home.aspx>

8.5 Non-academic policies

Please see the **Codes and Regulations** webpage

<http://www.rhul.ac.uk/forstudents/regulations/home.aspx>

which includes information on non-academic policies, regulations, and codes of practice as well as the **Student Charter**.

<http://www.rhul.ac.uk/aboutus/governancematters/studentcharter.aspx>

8.6 Complaints and academic appeals procedure

If you have a complaint relating to any aspect of the Department or its staff or to any academic or College matter, you should first discuss it informally with your Personal Advisor or with another member of staff in the Department. We would hope that the majority of issues of this kind can be resolved by informal discussion. There are, however, procedures that can be invoked in serious cases. These are set out in the **College Complaints Procedures** for students. You should raise your complaint **as soon as possible**.

<http://www.rhul.ac.uk/forstudents/studying/complaintsprocedure.aspx>

If the complaint concerns an academic decision, there is an academic appeals process. Please note that an academic appeal can **only** be submitted once you have received your results. Details of the **appeals procedures** and permitted grounds for appeal can be found on the following webpage.

<http://www.rhul.ac.uk/forstudents/studying/academicappeals/home.aspx>

9 Health and Safety Information

9.1 Code of practice on harassment for students

This can be found on the student home pages under codes and regulations

<http://www.rhul.ac.uk/forstudents/documents/pdf/codesandregulations/studentharassment.pdf>

9.2 Lone working policy and procedures

The College has a 'Lone Working Policy and Procedure' that can be found on the **Health and Safety Web pages**

<http://www.rhul.ac.uk/health-and-safety/policies-and-procedures.html>

Lone working is defined as working during either normal working hours at an isolated location within the normal workplace or when working outside of normal hours. The Department and the type of work conducted by students is classified as a low risk activity.

Any health and safety concerns should be brought to the attention of the Departmental Health and Safety Co-ordinator Mr Guillaume Subra or the College Health and Safety Office.

It is likely that most activities will take place on College premises. However, the principles contained in the above section will apply to **students undertaking duties off campus.**

10 Equal Opportunities Statement and College Codes of Practice

10.1 Equal opportunities statement

The University of London was established to provide education on the basis of merit above and without regard to race, creed or political belief and was the first university in the United Kingdom to admit women to its degrees.

Royal Holloway, University of London (hereafter 'the College') is proud to continue this tradition, and to commit itself to equality of opportunity in employment, admissions and in its teaching, learning and research activities.

The College is committed to ensure that;

- all staff, students, applicants for employment or study, visitors and other persons in contact with the College are treated fairly, have equality of opportunity and do not suffer disadvantage on the basis of race, nationality, ethnic origin, gender, age, marital or parental status, dependants, disability, sexual orientation, religion, political belief or social origins
- both existing staff and students, as well as, applicants for employment or admission are treated fairly and individuals are judged solely on merit and by reference to their skills, abilities qualifications, aptitude and potential
- it puts in place appropriate measures to eliminate discrimination and to promote equality of opportunity

- teaching, learning and research are free from all forms of discrimination and continually provide equality of opportunity
- all staff, students and visitors are aware of the Equal Opportunities Statement through College publicity material
- it creates a positive, inclusive atmosphere, based on respect for diversity within the College
- it conforms to all provisions as laid out in legislation promoting equality of opportunity.

10.2 College codes of practice

Royal Holloway is committed to upholding the dignity of the individual. Personal harassment can seriously harm working, learning and social conditions at the College. Harassment will be regarded seriously and could be grounds for disciplinary action, which may include termination of registration as a student. Royal Holloway's Code of Practice on Personal Harassment for Students is available at

<http://www.rhul.ac.uk/registry/onlinestudenthandbook/studentharassment.pdf>

11 Course descriptions

The information contained in these course outlines is correct at the time of publication, but may be subject to change as part of the Department's policy of continuous improvement and development. Every effort will be made to notify you of any such changes.

COURSE SPECIFICATION FORM
for new course proposals and course amendments

DEPARTMENT OF MATHEMATICS					
Course Code:	MT5412	Course Value:	200hr	Status: (ie:Core, or Optional)	Optional
Course Title:	Computational Number Theory			Availability: (state which teaching terms)	Term 1
Prerequisites:	UG course in number theory			Recommended:	none
Aims:	To provide an introduction to many major methods currently used for testing/proving primality and for the factorisation of composite integers. The course will develop the mathematical theory that underlies these methods, as well as describing the methods themselves.				
Learning Outcomes:	<p>On completion of the course, students should:</p> <ul style="list-style-type: none"> • Be familiar with a variety of methods used for testing/proving primality, and for the factorisation of composite integers. • Have an introductory knowledge of the theory of binary quadratic forms, elliptic curves, and quadratic number fields, sufficient to understand the principles behind state-of-the art factorisation methods. • Be equipped with the tools to analyse the complexity of some fundamental number-theoretic algorithms. 				
Course Content:	<p>Background: Complexity analysis; revision of Euclid's algorithm, and continued fractions; the Prime Number Theorem; smooth numbers; elliptic curves over a finite prime field; square roots modulo a prime; quadratic number fields; binary quadratic forms; fast polynomial evaluation.</p> <p>Primality tests: Fermat test; Carmichael numbers; Euler test; Euler-Jacobi test; Miller-Rabin test; Lucas test; AKS test.</p> <p>Primality proofs: succinct certificates; $p - 1$ methods; elliptic curve method; AKS method.</p> <p>Factorisation: Trial division; Fermat's method, and extensions; methods using binary quadratic forms; Pollard's $p - 1$ method; elliptic curve method; Pollard's rho and roo methods; factor-base methods; quadratic sieve; number field sieve.</p>				
Teaching & Learning Methods:	33 hours of lectures and examples classes. 167 hours of private study, including work on problem sheets and examination preparation. This may include discussions with the course leader if the student wishes.				
Key Bibliography:	<p>Prime Numbers: a Computational Perspective – R. Crandall and C. Pomerance (Springer 2005). 512.91 CRA</p> <p>A course in number theory and cryptography – N Koblitz (Springer 1994). 512.91 KOB</p> <p>A course in number theory – H.E. Rose (Oxford, 1994)</p>				
Formative Assessment & Feedback:	Formative assignments in the form of 8 problem sheets. The students will receive feedback as written comments on their attempts.				
Summative Assessment:	<p>Exam (%) Four questions out of five in a two-hour paper: 100%</p> <p>Coursework (%) None</p> <p>Deadlines: n/a</p>				

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department's policy of continuous improvement and development. Every effort will be made to notify you of any such changes

COURSE SPECIFICATION FORM
for new course proposals and course amendments

DEPARTMENT OF: MATHEMATICS					
Course Code:	MT5413	Course Value:	200hr	Status: <i>(ie:Core, or Optional)</i>	Optional
Course Title:	Complexity theory			Availability: <i>(state which teaching terms)</i>	Term 2
Prerequisites:	UG course in discrete mathematics			Recommended:	
Aims:	To introduce the technical skills to enable the student to understand the different classes of computational complexity, recognise when different problems have different computational hardness, and to be able to deduce cryptographic properties of related algorithms and protocols.				
Learning Outcomes:	<p>At the end of this course the student should</p> <ul style="list-style-type: none"> • understand the formal definition of algorithms and Turing machines • understand that not all languages are computable and prove simple examples • organise the low-level complexity classes (P, NP, coNP, NP-complete, RP, ZPP, BPP, PSPACE) into a hierarchy and prove simple languages exist in each class • give examples of one-way functions and hardcore functions, and demonstrate that every NP function has a hardcore predicate • use complexity theoretic techniques as a method of analysing communication services 				
Course Content:	<p>Algorithms: Motivation for complexity; languages; deterministic Turing machines; Church-Turing thesis; randomised algorithms.</p> <p>Computability: Goedel numbers; incomputable languages.</p> <p>Low-level complexity classes: Class P; 2-SAT; class NP; Cook's theorem; 3-SAT; coNP; class RP; class BPP; probability amplification; relation between classes; class PSPACE.</p> <p>One-way functions: One-way functions; one-way permutations; trapdoors; hardcore functions; Goldreich-Levin theorem</p> <p>Applications of complexity theory to communication: Applications of complexity theory to analysing the efficiency of communications' services.</p>				
Teaching & Learning Methods:	<p>33 hours of lectures with weekly question sheets</p> <p>167 hours of private study, including time spent on exercises and exam preparation</p>				
Key Bibliography:	<p>Complexity and cryptography by Talbot and Welsh (001.5436 TAL)</p> <p>Introduction to the theory of complexity by Bouvet and Crescenzi (519.22 BOV)</p> <p>Foundations of cryptography by Goldreich (001.5436 GOL)</p>				
Formative Assessment & Feedback:	Formative assignments in the form of 8 problem sheets. The students will receive feedback as written comments on their attempts.				
Summative Assessment:	<p>Exam Four questions out of five in a two-hour paper: 100%</p> <p>Coursework (%) None</p> <p>Deadlines: n/a</p>				

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department's policy of continuous improvement and development. Every effort will be made to notify you of any such changes.

COURSE SPECIFICATION FORM

DEPARTMENT OF MATHEMATICS					
Course Code:	MT5420	Course Value:	200 hours	Status: (ie:Core, or Optional)	Optional
Course Title:	Quantum Theory II			Availability: (state which teaching terms)	Term 2
Prerequisites:	An undergraduate course in quantum theory			Recommended:	None
Aims:	<ul style="list-style-type: none"> • To derive methods, such as the Rayleigh-Ritz variational principle and perturbation theory, in order to obtain approximate solutions of the Schrödinger equation. • To introduce spin and the Pauli exclusion principle and hence explain the mathematical basis of the Periodic table of elements. • To introduce the quantum theory of the interaction of electromagnetic radiation with matter using time dependent perturbation theory. • To show how scattering theory is used to probe interactions between particles and hence to show how the probability or cross section for a scattering event to occur can be derived from quantum theory. 				
Learning Outcomes:	<p>On completion of the course students should be able to:</p> <ul style="list-style-type: none"> • use various methods to obtain approximate eigenvalues and eigenfunctions of any given Schrödinger equation, • to understand the importance of spin in quantum theory, • to appreciate how the Periodic Table of elements follows from quantum theory, • to write down the Schrödinger equation for the interaction of electromagnetic radiation with the hydrogen atom and to work out photoabsorption cross sections for hydrogen, • to define the scattering cross section and to work it out for some simple systems. 				
Course Content:	<p>Variational principles in quantum mechanics: the Rayleigh-Ritz variational principle. Bounds on energy levels for quantum systems.</p> <p>Perturbation theory: Rayleigh-Schrödinger time-independent perturbation theory. Perturbations of energy levels due to external electromagnetic fields.</p> <p>The electron's spin: the eigenfunctions and eigenvalues of the spin operator. The Pauli exclusion principle. The periodic table of elements. Spin precession in an external magnetic field.</p> <p>Radiative transitions: the absorption and emission of electromagnetic radiation by matter. Photoabsorption cross-sections for the hydrogen atom.</p> <p>Scattering theory: definition of the scattering cross-section and the scattering amplitude. Decomposition of the scattering amplitude into partial waves. Phase shifts and the S-matrix. Integral representations of the scattering amplitude. The Born approximation. Potential scattering.</p>				
Teaching & Learning Methods:	<p>33 hours of lectures and examples classes. 167 hours of private study, including work on problem sheets and examination preparation. This may include discussions with the course leader if the student wishes.</p>				
Key Bibliography:	<p>Quantum Physics – S. Gasiorowicz (Wiley 1974) <i>Library reference 530.12 GAS</i> Quantum Mechanics – P C W Davies (Chapman and Hall 1984) <i>Library reference 530.12 DAV</i></p>				
Formative Assessment & Feedback:	<p>Formative assignments in the form of 8 problem sheets. The students will receive feedback as written comments on their attempts.</p>				
Summative Assessment:	<p>Exam (%) (hours) Four questions out of five in a two-hour paper: 100% Coursework (%) None Deadlines: n/a</p>				

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department's policy of continuous improvement and development. Every effort will be made to notify you of any such changes.

COURSE SPECIFICATION FORM

DEPARTMENT OF MATHEMATICS					
Course Code:	MT5441	Course Value:	200 hours	Status: <i>(ie:Core, or Optional)</i>	Core for MCC, optional for MfA
Course Title:	Channels			Availability: <i>(state which teaching terms)</i>	Term 1
Prerequisites:	Undergraduate courses in probability and algebra.			Recommended:	None
Aims:	To investigate the problems of data compression and information transmission in both noiseless and noisy environments.				
Learning Outcomes:	<p>On completion of the course the student should be able to</p> <ul style="list-style-type: none"> • state and derive a range of information-theoretic equalities and inequalities; • explain data-compression techniques for ergodic as well as memoryless sources; • explain the asymptotic equipartition property of ergodic sources; • understand the proof of the noiseless coding theorem; • define and use the concept of channel capacity of a noisy channel; • explain the noisy channel coding theorem; • understand a range of further applications of the theory. 				
Course Content:	<p>1. Entropy: Definition and mathematical properties of entropy, information and mutual information.</p> <p>2. Noiseless coding: Memoryless sources: proof of the Kraft inequality for uniquely decipherable codes, proof of the optimality of Huffman codes, typical sequences of a memoryless source, the fixed-length coding theorem.</p> <p>Ergodic sources: entropy rate, the asymptotic equipartition property, the noiseless coding theorem for ergodic sources. Lempel-Ziv coding.</p> <p>3. Noisy coding: Noisy channels, the noisy channel coding theory, channel capacity.</p> <p>4. Further topics, such as hash codes, or the information-theoretic approach to cryptography and authentication.</p>				
Teaching & Learning Methods:	<p>33 hours of lectures and examples classes.</p> <p>167 hours of private study, including work on problem sheets and examination preparation. This may include discussions with the course leader if the student wishes.</p>				
Key Bibliography:	<p>Codes and Cryptography, D Welsh (Oxford UP 1988), Library reference 001.5436 WEL</p> <p>Elements of Information Theory, TM Cover and JA Thomas (Wiley 1991), Library Reference 001.539 COV</p> <p>Information Theory, Inference, and Learning Algorithms, DJC MacKay (Cambridge UP 2003), Library Reference 001.539 MAC</p>				
Formative Assessment & Feedback:	Formative assignments in the form of 8 problem sheets. The students will receive feedback as written comments on their attempts.				
Summative Assessment:	<p>Exam (%) Four questions out of five in a two-hour written paper: 100%</p> <p>Coursework (%) None</p> <p>Deadlines: n/a</p>				

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department's policy of continuous improvement and development. Every effort will be made to notify you of any such changes.

COURSE SPECIFICATION FORM

DEPARTMENT OF MATHEMATICS					
Course Code:	MT5447	Course Value:	200 hours	Status: <i>(ie: Core, or Optional)</i>	Optional
Course Title:	Advanced Financial Mathematics			Availability: <i>(state which teaching terms)</i>	Term 2
Prerequisites:	An undergraduate course in financial mathematics			Recommended:	None
Aims:	<ul style="list-style-type: none"> • To investigate the validity of various linear and non-linear time series occurring in finance; • To extend the use of stochastic calculus to interest rate movements and credit rating; 				
Learning Outcomes:	<p>On completion of the course, students should:</p> <ul style="list-style-type: none"> • make use of some of the ARCH (autoregressive conditionally heteroscedastic) family of models in time series; • appreciate the ideas behind the use of the BDS test and the bispectral test for time series. • understand the partial differential equation for interest rates and the assumptions that lead to it; • be able to model forward and spot rates; • see how to model the prices for certain exotic options. 				
Course Content:	<p>Financial time series: Linear time series: ARMA and ARIMA models, stationarity, autoregressions. Testing of linearity, using spectral analysis. ARCH and GARCH models.</p> <p>Structure of financial series: The random walk model, trend and volatility, moments. Comparison with chaotic systems, dimensionality and memory effects in financial series. The nearest neighbour algorithm and the BDS test.</p> <p>Interest rate analysis: Revision of ideas in stochastic calculus. Modelling of interest rates, the bond pricing equation. Bond derivatives. The Heath-Jarrow-Morton model.</p> <p>Exotic options: Asian and barrier options.</p>				
Teaching & Learning Methods:	<p>33 hours of lectures and examples classes. 167 hours of private study, including work on problem sheets and examination preparation. This may include discussions with the course leader if the student wishes.</p>				
Key Bibliography:	<p>Paul Wilmott Introduces Quantitative Finance – P Wilmott (Wiley 2007) <i>Library reference 332.632 WIL</i></p> <p>Analysis of Financial Time Series – R S Tsay (Wiley 2005) <i>Library reference 330.0151 TSA</i></p>				
Formative Assessment & Feedback:	<p>Formative assignments in the form of 8 problem sheets. The students will receive feedback as written comments on their attempts.</p>				
Summative Assessment:	<p>Exam (%) Four questions out of five in a two-hour paper: 100%</p> <p>Coursework (%) None</p> <p>Deadlines: n/a</p>				

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department's policy of continuous improvement and development. Every effort will be made to notify you of any such changes.

COURSE SPECIFICATION FORM
for new course proposals and course amendments

DEPARTMENT OF MATHEMATICS					
Course Code:	MT5454	Course Value:	200 hours	Status: <i>(ie:Core, or Optional)</i>	Optional
Course Title:	Combinatorics			Availability: <i>(state which teaching terms)</i>	Term 1
Prerequisites:	An undergraduate course in discrete mathematics			Recommended:	None
Aims:	<p>To introduce some standard techniques and concepts of combinatorics, including</p> <ul style="list-style-type: none"> • methods of counting including the principle of inclusion and exclusion; • generating functions; • probabilistic methods; • permutations, Ramsey theory. 				
Learning Outcomes:	<p>On completion of the course, students should be able to:</p> <ul style="list-style-type: none"> • perform simple calculations with generating functions; • understand Ramsey numbers and calculate upper and lower bounds for these (where practical); • calculate sets by inclusion and exclusion and understand the applications to number theory; • use simple probabilistic tools for solving combinatorial problems. 				
Course Content:	<p>Enumeration: Binomial identities. The Principle of Inclusion-Exclusion with applications to number theory. Rook polynomials. Generating functions: Linear recursion. Power series and ordinary generating functions. Singularities. Ramsey Theory: Monochromatic subsets, Ramsey numbers and Ramsey's Theorem. Probabilistic methods: First-moment method, Lovász local lemma.</p>				
Teaching & Learning Methods:	<p>33 hours of lectures and examples classes. 167 hours of private study, including work on problem sheets and examination preparation. This may include discussions with the course leader if the student wishes.</p>				
Key Bibliography:	<p>Discrete Mathematics – N L Biggs (Oxford UP) <i>510 BIG</i>. Combinatorics: Topics, Techniques, Algorithms – P J Cameron (Cambridge UP) <i>512.23 CAM</i>. Invitation to Discrete Mathematics = J Matoušek and J Nešetřil (Oxford UP) <i>512.23 MAT</i></p>				
Formative Assessment & Feedback:	<p>Formative assignments in the form of 8 problem sheets. The students will receive feedback as written comments on their attempts.</p>				
Summative Assessment:	<p>Exam (%) Four questions out of five in a two-hour paper: 100% Coursework (%) None Deadlines: n/a</p>				

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department's policy of continuous improvement and development. Every effort will be made to notify you of any such changes.

COURSE SPECIFICATION FORM
for new course proposals and course amendments

DEPARTMENT OF MATHEMATICS					
Course Code:	MT5461	Course Value:	200hr	Status: (ie:Core, or Optional)	Core for MfA and MCC MScs
Course Title:	Theory of Error-Correcting Codes			Availability: (state which teaching terms)	Term 2
Prerequisites:	Undergraduate courses on linear algebra and finite fields			Recommended:	none
Aims:	To provide an introduction to the theory of error-correcting codes employing the methods of elementary enumeration, linear algebra and finite fields.				
Learning Outcomes:	<p>On completion of the course, students should:</p> <ul style="list-style-type: none"> • calculate the probability of error or the necessity of retransmission for a binary symmetric channel with given cross-over probability, with and without coding; • prove and apply various bounds on the number of possible code words in a code of given length and minimal distance; • use MOLSs and Hadamard matrices to construct medium-sized linear codes of certain parameters; • reduce a linear code to standard form, finding a parity check matrix, building standard array and syndrome decoding tables, including for partial decoding; • know/prove/apply the theorem that a cyclic code of length n over a field consists of the codewords corresponding to all multiples of any factor of $x^n - 1$; • understand the structure of BCH codes. 				
Course Content:	<p>Basic theory of coding: Words, codes, errors, t-error detection and t-error correction. The Hamming distance in the space $V(n,q)$ of n-tuples over an alphabet of q symbols (with emphasis on $(Z_2)^n$). Probability calculations.</p> <p>The main coding theory problem: Construction of small binary codes. Rate of a code. Equivalence of codes. The Hamming, Singleton, Gilbert-Varshamov and Plotkin bounds. Puncturing a code. Perfect codes. Hadamard codes and Levenshtein's Theorem. Codes based on mutually orthogonal latin squares (MOLS).</p> <p>Linear codes: Linear codes as linear subspaces of $V(n,q)$. Generator and parity check matrices, standard array and syndrome decoding. Dual of a code. Hamming codes.</p> <p>Cyclic codes: Structure of $GF(q)$ relevant to coding theory, minimal polynomial of an element of $GF(q)$; generator polynomial, check polynomial; BCH codes, RS codes.</p>				
Teaching & Learning Methods:	44 hours of lectures and examples classes. 156 hours of private study, including work on problem sheets and examination preparation. This may include discussions with the course leader if the student wishes.				
Key Bibliography:	<p>A First Course in Coding Theory – R Hill (Oxford UP) 001.539 HIL</p> <p>Coding Theory – a First Course – S Ling and C Xing (Cambridge UP) 001.539 LIN</p> <p>The Theory of Error-Correcting Codes – F J MacWilliams and N J A Sloane (North-Holland) 512.23 MAC</p>				
Formative Assessment & Feedback:	Formative assignments in the form of 8 problem sheets. The students will receive feedback as written comments on their attempts.				
Summative Assessment:	<p>Exam (%) Four questions out of five in a two-hour paper: 100%</p> <p>Coursework (%) None Deadlines: n/a</p>				

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department's policy of continuous improvement and development. Every effort will be made to notify you of any such changes.

COURSE SPECIFICATION FORM
for new course proposals and course amendments

DEPARTMENT OF MATHEMATICS					
Course Code:	MT5462	Course Value:	200hr	Status: (ie:Core, or Optional)	Core for MfA and MCC MScs
Course Title:	Advanced Cipher Systems			Availability: (state which teaching terms)	Term 1
Prerequisites:	UG courses in linear algebra and probability			Recommended:	none
Aims:	To introduce and study the mathematical and security properties of both symmetric key cipher systems and public key cryptography, covering methods for obtaining confidentiality and authentication.				
Learning Outcomes:	<p>On completion of the course the student should be able to:</p> <ul style="list-style-type: none"> • Understand the concepts of secure communications and cipher systems; • Understand and use statistical information and the concept of entropy in the cryptanalysis of cipher systems; • Understand the main properties of Boolean functions, and their applications and use in cryptographic algorithms; • Understand the structure of stream ciphers and block ciphers; • Know how to construct as well as have an appreciation of desirable properties of keystream generators, and understand and manipulate the concept of perfect secrecy; • Understand the main mathematical and statistical properties of Feedback Shift Registers, and of FSR-based stream ciphers; • Understand the modes of operation of block ciphers and their properties; • Understand the main design principles and cryptographic techniques of modern symmetric cryptography algorithms; • Understand the concept of public key cryptography, including the details of the RSA and ElGamal cryptosystems, both in the description of the schemes and in their cryptanalysis; • Understand the concepts of authentication, identification and signature, be familiar with techniques that provide these, including one-way functions, hash functions and interactive protocols, and the Fiat-Shamir scheme; • Understand the problems of key management, and be aware of key distribution techniques. 				
Course Content:	<p>Cipher systems: An introductory overview of the aims and types of ciphers. Methods and types of attack. Information theory. Boolean functions. Statistical tests.</p> <p>Stream ciphers: The one-time pad. Pseudo-random key streams – properties and generation. Mathematical and statistical properties of feedback shift registers. Berlekamp-Massey algorithm. Design principles and cryptanalytic techniques of modern stream ciphers.</p> <p>Block ciphers: Confusion and diffusion. Iterated block ciphers – substitution/permutation. SP-networks. The Feistel principle. DES, AES. Modes of operation. Linear and differentiable cryptanalysis, and related cryptographic techniques.</p> <p>Public key ciphers: Discussion of key management. Diffie-Hellman key exchange. One-way functions and trapdoors. RSA, ElGamal cryptosystem.</p> <p>Authentication/identification: Protocols. Challenge/response. MACs. Zero-knowledge protocols; Fiat-Shamir protocol.</p> <p>Digital signatures: Digital signature methods. Hash functions – design and analysis techniques. DSS. Digital certificates.</p>				

Teaching Learning Methods:	&	44 hours of lectures and examples classes. 156 hours of private study, including work on problem sheets and examination preparation. This may include discussions with the course leader if the student wishes.
Key Bibliography:		Codes and Cryptography – D Welsh (Oxford 1988) <i>001.5436 WEL</i> Cipher Systems – H J Beker and F C Piper (Van Nostrand 1982) <i>001.5436 BEK</i>
Formative Assessment & Feedback:	&	Formative assignments in the form of 8 problem sheets. The students will receive feedback as written comments on their attempts.
Summative Assessment:		Exam (%) Four questions out of five in a two-hour paper: 100% Coursework (%) None Deadlines: n/a

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department's policy of continuous improvement and development. Every effort will be made to notify you of any such changes.

COURSE SPECIFICATION FORM

DEPARTMENT OF MATHEMATICS					
Course Code:	MT5466	Course Value:	200hr	Status: <i>(ie:Core, or Optional)</i>	Optional for MfA, core for MCC
Course Title:	Public Key Cryptography			Availability: <i>(state which teaching terms)</i>	Term 2
Prerequisites:	MT5462			Recommended:	none
Aims:	<ul style="list-style-type: none"> To introduce some of the mathematical ideas essential for an understanding of public key cryptography, such as discrete logarithms, lattices and elliptic curves; To introduce several important public key cryptosystems, such as RSA, Rabin, ElGamal Encryption, Schnorr signatures; To discuss modern notions of security and attack models for public key cryptosystems. 				
Learning Outcomes:	<p>On completion of the course, students should:</p> <ul style="list-style-type: none"> be familiar with the RSA and Rabin cryptosystems, the hard problems on which their security relies and certain attacks on them; have a basic knowledge of finite fields and elliptic curves over finite fields, and the discrete logarithm problem in these groups; be familiar with cryptosystems based on discrete logarithms, and some algorithms for solving the discrete logarithm problem; know the definition of a lattice and be familiar with the LLL algorithm and some applications of lattices in cryptography and cryptanalysis; be able to define security notions and attack models relevant for modern theoretical cryptography, such as indistinguishability and adaptive chosen-ciphertext attack.; be able to critically analyse cryptosystems; have experience with implementing cryptosystems and cryptanalytic methods using a computer algebra package such as Mathematica. 				
Course Content:	<p>Background: Integers modulo n; Chinese remainder theorem; finite fields; fast exponentiation; public key cryptography and security; complexity theory.</p> <p>RSA/Rabin: Key generation; implementation; encryption and signatures; OAEP; the RSA problem and relationship with factoring; square roots modulo a prime; Hastad attack; Wiener attack.</p> <p>Discrete logarithms: Diffie-Hellman; ElGamal encryption; Schnorr signatures; Diffie-Hellman problem and decision Diffie-Hellman; methods to solve discrete logarithms such as baby-step-giant-step, Pollard rho and lambda, index calculus.</p> <p>Lattices: Definition of a lattice; GGH cryptosystem; LLL algorithm; lattice attacks on knapsack cryptosystems and variants of RSA.</p> <p>Elliptic curves: Group law; Hasse bound; group structure; point counting; ECC protocols; Maurer equivalence of DH and DL.</p>				
Teaching & Learning Methods:	<p>33 hours of lectures and examples classes. 167 hours of private study, including work on problem sheets and examination preparation. This may include discussions with the course leader if the student wishes.</p>				
Key Bibliography:	<p>Cryptography: an introduction – Nigel Smart (McGraw Hill) 001.5436 SMA Cryptography theory and practice – Doug Stinson (CRC press, 2nd ed.) 001.5436 STI</p>				
Formative Assessment & Feedback:	<p>Formative assignments in the form of 8 problem sheets. The students will receive feedback as written comments on their attempts.</p>				
Summative Assessment:	<p>Exam (%) Four questions out of five in a two-hour paper: 100% Coursework (%) None Deadlines: n/a</p>				

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department's policy of continuous improvement and development. Every effort will be made to notify you of any such changes.

COURSE SPECIFICATION FORM

DEPARTMENT OF: Mathematics					
Course Code:	MT5485	Course Value:	0.5	Status: <i>(ie: Core, or Optional)</i>	Optional
Course Title:	Applications of Field Theory			Availability: <i>(state which teaching terms)</i>	Term 1
Prerequisites:	An undergraduate course covering the elementary theory of groups, rings and fields.			Recommended:	None
Aims:	To introduce some of the basic theory of field extensions, with special emphasis on applications in the context of finite fields.				
Learning Outcomes:	<p>On completion of the course, students should be able to:</p> <ul style="list-style-type: none"> • understand simple field extensions of finite degree; • classify finite fields and determine the number of irreducible polynomials over a finite field; • state the fundamental theorem of Galois theory; • compute in a finite field; • understand some of the applications of fields. 				
Course Content:	<p>Extension theory: Polynomial factorisation. Field extensions. Simple extensions. The degree of an extension. Applications to ruler and compass constructions.</p> <p>Classifying finite fields: The number of irreducible polynomials. Existence and uniqueness of finite fields of a given size. Concrete representations of a finite field.</p> <p>The structure of finite fields: Roots of irreducible polynomials and the Frobenius automorphism. Cyclotomic polynomials. The Galois correspondence for finite fields. An indication of Galois correspondence for general fields. The norm and trace of an element. Applications to m-sequences. Dual and self-dual bases. Normal bases and the normal basis theorem. Applications to multiplication in finite fields.</p> <p>Discrete logarithms: The discrete log problem and its applications. The Pohlig-Hellman and baby step, giant step algorithms.</p>				
Teaching & Learning Methods:	<p>33 hours of lectures and examples classes. 167 hours of private study, including work on problem sheets and examination preparation. This may include discussions with the course leader if the student wishes.</p>				
Key Bibliography:	<p>Introduction to Finite Fields and their Applications – R. Lidl and H. Niederreiter (Cambridge UP 1994); <i>Library reference 512.4 LID.</i> Galois Theory – I. Stewart (Chapman and Hall 2003); <i>Library reference 512.4 STE.</i></p>				
Formative Assessment & Feedback:	Formative assignments in the form of 8 problem sheets. The students will receive feedback as written comments on their attempts.				
Summative Assessment:	<p>Exam (%) Four questions out of five in a two-hour paper: 100%</p> <p>Coursework (%) None</p> <p>Deadlines: n/a</p>				

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department's policy of continuous improvement and development. Every effort will be made to notify you of any such changes.