ROYAL HOLLOWAY
University of London

PROGRAMME SPECIFICATION

This document describes the **Master of Science and Postgraduate Diploma in Mathematics of Cryptography and Communications**. This specification is valid for new entrants from **September 2006**.

The aims of the MSc in Mathematics of Cryptography and Communications are to:

- provide a suitable mathematical foundation for undertaking research or professional employment in cryptography and/or communications;
- provide students with the appropriate background in information theory and coding theory to enable them to understand and be able to apply the theory of communication through noisy channels;
- provide students with the appropriate background in algebra and number theory to develop an understanding of modern public key cryptosystems;
- provide students with a critical awareness of problems in information transmission and data compression, and the mathematical techniques which are commonly used to solve these problems;
- provide students with a critical awareness of problems in cryptography and the mathematical techniques which are commonly used to provide solutions to these problems;
- give students the opportunity to carry out an independent research investigation into the mathematics of cryptography and/or communications;
- provide students with a range of transferable skills appropriate to progression to PhD studies or employment, including experience with independent research and managing the writing of a dissertation.

The aims of the Postgraduate Diploma (PGDip) in Mathematics of Cryptography and Communications are as above, with the exception of those aspects relating to the research investigation and the writing of a dissertation, which is a major piece of independent study of between 12,000 and 15,000 words.

The programme is delivered over one year of full-time study (52 weeks) or two years of part-time study (104 weeks). It provides in-depth training and research experience entirely at Masters level. Students receive training in generic scientific and discipline-specific research skills.

Royal Holloway is internationally regarded as a centre of excellence in cryptography research and this programme complements the extremely successful MSc in Information Security which has been running for over ten years. The MSc is taught by members of the Mathematics Department and the Information Security Group and students have the opportunity to be supervised by researchers covering a wide range of research topics.

Further information

This document provides a summary of the main features of the programme(s), and of the outcomes which a student might reasonably be expected to achieve if full advantage is taken of the learning opportunities provided. Further information is contained in the College prospectus, the College Regulations and in various handbooks issued to students upon arrival. Whilst Royal Holloway keeps all its information for prospective applicants and students under review, programmes and the availability of individual courses are necessarily subject to change at any time, and prospective applicants are therefore advised to seek confirmation of any factors which might affect their decision to follow a specific programme. In turn, Royal Holloway will inform applicants and students as soon as is practicable of any substantial changes which might affect their studies.

Learning outcomes

Teaching and Learning in the programme are closely informed by the active research of staff. In general

terms, the programme provides opportunities for students to develop and demonstrate the following learning outcomes:

Knowledge and understanding of:
- the principles of information transmission, data compression and information theory;
- the principles of communication through noisy channels using coding theory;
- the principles of cryptography as a tool for securing data;
- the algebra and number theory behind public key cryptography;
- the mathematics behind symmetric key cipher systems;
- the principles of cryptanalysis and experience with some of the algorithms used to break cryptosystems;
- the role and limitations of mathematical ideas in information security.

Skills and other attributes:
- demonstrate a high level of ability in subject specific skills, including algebra and number theory;
- ability to clearly formulate problems and express technical content and conclusions in written form;*
- time management;*
- self-motivation, flexibility and adaptability;*
- computer skills;*
- ability to critically analyse the strengths and weaknesses of solutions to problems in cryptography and communications.

Skills and other attributes (MSc only):
- synthesise information from a number of sources with critical awareness;*
- evaluate research critically;*
- preparation of an MSc dissertation.*

* transferable skills

Back to top

Teaching, learning and assessment

For the taught courses, teaching is mainly by lectures, supported by weekly written coursework assignments. Learning is augmented by occasional computer projects and independent private study using books, course notes and the internet. For the dissertation, learning is by independent research and private study, supported by research supervision. Students receive regular feedback on their performance on coursework for taught courses; their detailed research proposal (end of examinations term); and dissertation drafts near the completion of the project. Completion of tasks is monitored centrally to ensure students experiencing difficulty can be identified and provided with appropriate support.

Assessment is mainly by examination in May for the taught courses. Some courses may also require extended essays, reports, computer programming or oral examinations. The dissertation is submitted at the end of the summer, approximately two weeks before the beginning of the next academic year. For details of the assessment of the main project see the Programme Handbook. Full details of the assessments for individual courses can be obtained from the Department.

Back to top

Details of the programme structure(s)

The MSc programme comprises six weighted taught courses, up to two supplementary courses, and the MSc dissertation. The two supplementary courses appear on students' transcripts but do not contribute to the final degree classification. Students decide towards the end of the second term which courses are to be considered as supplementary. The six weighted taught courses will normally comprise the four core courses and two options courses. 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 options course). At the discretion of the Programme Director, a student may attend up to one course (as a supplementary course) from the third or fourth year of the undergraduate programme in Mathematics, for example to fill a gap in their knowledge from undergraduate study. Students are encouraged to divide their courses

equally between the two terms, or over two years in the case of part-time students.

The brief outline of the programme is shown below; however students can obtain further details from the Programme Handbook. Where weightings are indicated in brackets, these refer to weightings within the MSc. The programme structure for the PGDip is as below, with the exception that students will not undertake the dissertation. Weightings for courses within the PGDip are proportionate, but exclude the dissertation.

Students must take the following four core courses (apart from exceptions mentioned above):

MT5441	Channels	(12.5%)
MT5461	Theory of Error Correcting Codes	(12.5%)
MT5462	Advanced Cipher Systems	(12.5%)
MT5466	Public Key Cryptography	(12.5%)

and take the Dissertation course:

MT5400	The MSc Project	(25%)

plus choose two options courses (25%) and two supplementary courses (non-weighted) from a list of courses offered by the Department.

Please note that the list of available courses offered is subject to change and not all courses run each year. A full list of current courses can be obtained from the Department.

Part-time arrangements

Part-time Masters students are typically expected to take four courses in their first year (typically the core courses would be taken in the first year) and complete the remaining courses and the dissertation in the second year. They will only be permitted to proceed to the second year if they pass at least three courses by the end of the first year. Part-time students will be encouraged to begin work on their dissertation during the summer between their first and second years.

Back to top

Progression and award requirements

The assessment is based on the courses and dissertation listed above.

- 75% of the assessment is taken to be the average mark of the six weighted taught courses. The six weighted taught courses over which the marks are averaged must all be of Masters level and must include at least three core courses.
- 25% of the assessment is on the written dissertation.

To pass the **MSc** programme a student must achieve an overall weighted average of at least 50.00%, with no mark in a weighted taught course or the dissertation falling below 50%. Failure marks between 40-49.99% can be condoned in courses which do not constitute more than 25% of the final assessment, provided that the overall weighted average is at least 50.00%, but a failure mark (i.e. below 50%) in the dissertation cannot be condoned.

The MSc degree with Merit may be awarded if a student achieves an overall weighted average of 65.00% or above, with no mark in a weighted taught course or the dissertation falling below 50%.

The MSc degree with Distinction may be awarded if a student achieves an overall weighted average of 70.00% or above, with no mark in a weighted taught course or the dissertation falling below 60%. A Distinction will not normally be awarded if a student re-sits or re-takes any element of the programme. In exceptional circumstances a viva may be held for a student at the request of the Examiners.

The **Postgraduate Diploma** may be awarded if a student:

- achieves an overall weighted average of at least 50.00%, with no mark in a weighted taught course falling below 50%; *or*
- has failure marks in the region 40-49.99% in courses which do not constitute more than 25% of the final assessment and which therefore may be condoned;

and has either chosen not to proceed to the dissertation, or has failed the dissertation on either the first or second attempt.

The Postgraduate Diploma with Merit may be awarded if a student achieves an overall weighted average of 65.00% or above, with no mark in a weighted taught course falling below 50%.

The Postgraduate Diploma with Distinction may be awarded if a student achieves an overall weighted average of 70.00% or above, with no mark in a weighted taught course falling below 60%. A Distinction will not normally be awarded if a student re-sits or re-takes any element of the programme. In exceptional circumstances a viva may be held for a student at the request of the Examiners.

Back to top

Student support and guidance

- Programme Director: The Programme Director meets the students during the induction meeting at the beginning of the academic year (if not earlier during the application and admissions process). The Programme Director acts as a point of contact for pastoral support and any questions about the programme throughout the year.
- MSc dissertation supervisor: By the end of term 2 each student's supervisor will have been determined. Students should meet their supervisor regularly to discuss all matters relating to their dissertation.
- Personal adviser: All students are allocated a personal adviser, with whom they meet at least once a term, and more regularly if required, to discuss all matters relating to their programme and for pastoral support.
- Representation on the Postgraduate Student Committee.
- Each lecture course includes regular homework problem sheets to be attempted by the student. The coursework is marked and returned to the student with feedback on their performance. This formative assessment is valuable for both students and staff.
- All academic staff are available and accessible through an open-door policy or by operating an office hours system.
- Programme Handbook.
- Supporting materials and learning resources in the Department, College libraries and Computer Centre.
- College Careers Service.
- Access to all College and University support services, including Student Counselling Service, Health Centre and the Education Support Office (for students with special needs).
- Secretarial and technical support staff as detailed in the handbook.

Back to top

Admission requirements

Admission to the programme normally requires a First or Upper Second Class Honours Degree in Mathematics. However, the Department also has considerable flexibility in its admissions and offers policy and strongly encourages applications from non-standard applicants (such as those with degrees in other subjects like Physics or Computer Science). Students whose first language is not English may also be asked for a qualification in English Language at an appropriate level. For further details please refer to the Prospective Students web page. It may also be helpful to contact the Admissions Office for specific guidance on the entrance requirements for particular programmes.

Back to top

Further learning and career opportunities

The programme prepares students for future careers in mathematical research and/or development in the general area of communications and information security. The programme also develops students' generic skills. After obtaining this degree, students would be well prepared to begin doctoral studies, for a technical role in the certain industries (e.g., communications), or for employment in any area where good numeracy, computer skills and general mathematical knowledge are valued. Information on career opportunities is provided by talks on careers and higher degree opportunities, organised by the Careers Service. For further details on further learning and career opportunities please refer to the Careers Service.

Back to top

Indicators of quality and standards

Royal Holloway's position as one of the UK's leading research-intensive institutions was confirmed by the results of the most recent Research Assessment Exercise (RAE 2008) conducted by the Higher Education Funding Council (HEFCE). The new scoring system for the RAE 2008 measures research quality in four categories, with the top score of 4* indicating quality that is world-leading and of the highest standards in terms of originality, significance and rigour. 60% of the College's research profile is rated as world-leading or internationally excellent outperforming the national average of 50%. The College is ranked 16th in the UK for research of 4* standard and 18th for 3* and 4* research.

Back to top

List of programmes

The programme is taught entirely by staff at Royal Holloway, University of London and leads to an MSc award of the University of London. The Postgraduate Diploma leads to an award of Royal Holloway and Bedford New College. Programmes in Mathematics of Cryptography and Communications are not subject to accreditation by a professional body. The Banner programme codes are given in parentheses.

Master of Science Degree programme in Mathematics of Cryptography and Communications

MSc in Mathematics of Cryptography and Communications (2130)

Postgraduate Diploma in Mathematics of Cryptography and Communications

PG Diploma in Mathematics of Cryptography and Communications (2131)

Back to top