Royal Holloway, University of London
Course specification for a postgraduate award
MSc Mathematics of Cryptography and Communications (2130)

Section 1 – Introduction to your course

This course specification is a formal document, which provides a summary of the main features of your course and the learning outcomes that you might reasonably be expected to achieve and demonstrate if you take full advantage of the learning opportunities that are provided. Further information is contained in the College prospectus, and in various handbooks, all of which you will be able to access online. Alternatively, further information on the College's academic regulations and polices can be found here. Further information on the College's Admissions Policy can be found here.

The course is delivered over one year of full-time study (52 weeks). The course is also available part time; you would normally complete the course within 2 years (104 weeks) but College regulations permit up to five years of part-time study (260 weeks). It provides in-depth training and research experience entirely at Masters level. You 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 course 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 you have the opportunity to be supervised by researchers covering a wide range of research topics.

While Royal Holloway keeps all the information made available under review, courses and the availability of individual modules, especially optional modules are necessarily subject to change at any time, and you are therefore advised to seek confirmation of any factors which might affect your decision to follow a specific course. In turn, Royal Holloway will inform you as soon as is practicable of any significant changes which might affect your studies.

The following is brief description for some of the most important terminology for understanding the content of this document:

Degree course – Also referred to as 'course', this term refers to the qualification you will be awarded upon successful completion of your studies. 'Courses' were formerly known as 'programmes' at Royal Holloway.
Module – This refers to the credits you will study each year to complete your degree course. . Postgraduate taught degrees at Royal Holloway comprise 180 credits. On some degree courses a certain number of optional modules must be passed for a particular degree title. 'Modules' were formerly known as 'course units' at Royal Holloway.

Section 2 – Course details			
Date of specification update	October 2021	**Location of study**	Egham Campus
Course award and title	MSc Mathematics of Cryptography and Communications	**Level of study**	Postgraduate
Course code	2130	**Year of entry**	2022/23
Awarding body	Royal Holloway, University of London		
Department/ School	Department of Mathematics School of Engineering, Physical and Mathematical Sciences	**Other departments or schools involved in teaching the course**	N/A
Mode(s) of attendance	Full-time / Part-time	**Duration of the course**	One year (52 weeks) full-time Two to five years (104 - -260 weeks) part-time
Accrediting Professional, Statutory or Regulatory Body requirement(s)	N/A	**For queries on admissions:**	study@royalholloway.ac.uk.
Link to Coursefinder for further information:	https://www.royalholloway.ac.uk/studying-here/		

Section 3 – Degree course structure

3.1 Mandatory module information

The following table summarises the mandatory modules which students must take in each year of study

Module code	Module title	Credits	FHEQ level	Module status (see section 6)
MT5400	Main Project	60	7	MNC
MT5462	Advanced Cypher Systems	20	7	MC
MT5441	Channels	20	7	MC
MT5461	Theory of Error-Correcting Codes	20	7	MC
MT5466	Public Key Cryptography	20	7	MC

This table sets out the most important information for the mandatory modules on your degree course. These modules are central to achieving your learning outcomes, so they are compulsory, and all students on your degree course will be required to take them. You will be automatically registered for these modules. Mandatory modules fall into two categories; 'condonable' or 'non-condonable'.

In the case of mandatory 'non-condonable' (MNC) modules, you must pass the module to successfully graduate with a particular degree title, or before you can proceed to the next year of your course where studying part-time. In the case of mandatory 'condonable' (MC) modules, these must be taken but you can still progress or graduate even if you do not pass them (see Academic Regulations on condonable fails). Please note that although Royal Holloway will keep changes to a minimum, changes to your degree course may be made where reasonable and necessary due to unexpected events. For example; where requirements of relevant Professional, Statutory or Regulatory Bodies have changed and course requirements must change accordingly, or where changes are deemed necessary on the basis of student feedback and/or the advice of external advisors, to enhance academic provision.

3.2 Optional modules

In addition to mandatory modules, there will be a number of optional modules available during the course of your degree. The following table lists a selection of optional modules that are likely to be available. However, not all may be available every year. Although Royal Holloway will keep changes to a minimum, new options may be offered or existing ones may be withdrawn. For example; where reasonable and necessary due to unexpected events, where requirements of relevant Professional, Statutory or Regulatory Bodies (PSRBs) have changed and course requirements must change accordingly, or where changes are deemed necessary on the basis of student feedback and/or the advice of External Advisors, to enhance academic provision.There may be additional requirements around option selection, so it is important that this specification is read alongside your department's Student Handbook, which you can normally access via Moodle.

Optional modules.			
Module Title	**Credits**	**Module Title**	**Credits**
MT5485 Applications of Field Theory	20	MT5412 Computational Number Theory	20
MT5445 Quantum Information and Coding	20	MT5413 Complexity Theory	20
MT5414 Principles of Algorithm Design	20	MT5432 Inference	20
MT5448 Advanced Financial Mathematics	20	MT5491 Topology	20
MT5454 Combinatorics	20		

3.3 Optional module requirements

You must choose two optional modules (40 credits) and two supplementary modules (non-weighted) from a list of modules offered by the Department. The two supplementary modules appear on your transcript but do not contribute to the final degree classification.

A full list of current modules can be obtained from the Department.

Section 4 - Progressing through each year of your degree course

For further information on the progression and award requirements for your degree, please refer to Royal Holloway's Academic Regulations.

Progression throughout the year/s is monitored through performance in summative or formative coursework assignments. Please note that if you hold a Tier 4 (General) Student Visa and you choose to leave (or are required to leave because of non-progression) or complete early (before the course end date stated on your CAS), then this will be reported to UKVI.

To pass the Master's course you must achieve an overall weighted average of at least 50.00%, with no mark in any module which counts towards the final assessment falling below 50%. Failure marks between 40-49% can be condoned in modules which constitute up to a maximum of 40 credits, 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.

Part-time arrangements

Part-time Masters students are typically expected to take four modules (80 credits) in their first year (typically the mandatory modules would be taken in the first year) and complete the remaining modules and the dissertation in the second year**. Part-time students following the standard 2 year model will be encouraged to begin work on their dissertation during the summer between their first and second years.

** part time students are permitted under College regulations to complete their course of study over a period of up to 5 years. If you are unable to complete the course within the standard 2 year timeframe then you should liaise with the course director to agree a time frame for completion.

Section 5 – Educational aims of the course

The aims of this course are to:

- provide a suitable mathematical foundation for undertaking research or professional employment in cryptography and/or communications;
- provide you 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 you with the appropriate background in algebra and number theory to develop an understanding of modern public key cryptosystems;
- provide you 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 you with a critical awareness of problems in cryptography and the mathematical techniques which are commonly used to provide solutions to these problems;
- give you the opportunity to carry out an independent research investigation into the mathematics of cryptography and/or communications;
- provide you 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.

Section 6 – Course learning outcomes

In general terms, the courses provide opportunities for students to develop and demonstrate the following learning outcomes. (*Categories – Knowledge and understanding (K), Skills and other attributes (S), and Transferable skills (*)*)

1. the principles of information transmission, data compression and information theory**(K)**;
2. the principles of communication through noisy channels using coding theory **(K)**;
3. the principles of cryptography as a tool for securing data **(K)**;
4. the algebra and number theory behind public key cryptography **(K)**;
5. the mathematics behind symmetric key cipher systems **(K)**;
6. the principles of cryptanalysis and experience with some of the algorithms used to break cryptosystems **(K)**;
7. the role and limitations of mathematical ideas in information security **(K)**.
8. demonstrate a high level of ability in subject specific skills, including algebra and number theory **(S)** ;
9. ability to clearly formulate problems and express technical content and conclusions in written form **(S)**;*
10. time management**(S)** ;*
11. self-motivation, flexibility and adaptability**(S)** ;*
12. computer skills **(S)**;*
13. ability to critically analyse the strengths and weaknesses of solutions to problems in cryptography and communications **(S)** .
14. synthesise information from a number of sources with critical awareness **(S)**;*
15. evaluate research critically **(S)**;*
16. preparation of an MSc dissertation **(S)** *(MSc only)*.*

Section 7 - Teaching, learning and assessment
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. 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. You receive regular feedback on your performance on coursework for taught modules; your 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 modules. Some modules 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 Course Handbook. Full details of the assessments for individual modules can be obtained from the Department.

Section 8 – Additional costs
There are no single associated costs greater than £50 per item on this degree course.
These estimated costs relate to studying this particular degree course at Royal Holloway. General costs such as accommodation, food, books and other learning materials and printing etc., have not been included, but further information is available on our website.

Section 9 – Indicators of quality and standards	
QAA Framework for Higher Education Qualifications (FHEQ) Level	7
Your course is designed in accordance with the FHEQ to ensure your qualification is awarded on the basis of nationally established standards of achievement, for both outcomes and attainment. The qualification descriptors within the FHEQ set out the generic outcomes and attributes expected for the award of individual qualifications. The qualification descriptors contained in the FHEQ exemplify the outcomes and attributes expected of learning that results in the award of higher education qualifications. These outcomes represent the integration of various learning experiences resulting from designated and coherent programmes of study.	
QAA Characteristics Statement (Master's Degrees) – September 2015	https://www.qaa.ac.uk/en/quality-code/supporting-resources
Subject benchmark statements provide a means for the academic community to describe the nature and characteristics of courses in a specific subject or subject area. They also represent general expectations about standards for the award of qualifications at a given level in terms of the attributes and capabilities that those possessing qualifications should have demonstrated.	

Section 10 – Further information
This specification provides a concise summary of the main features of the course and the learning outcomes that a typical student might reasonably be expected to achieve and demonstrate when taking full advantage of the learning opportunities that are available. More detailed information on modules, including teaching and learning methods, and methods of assessment, can be found via the online module catalogue. The accuracy of the information contained in this document is reviewed regularly by the university, and may also be checked routinely by external agencies. Your course will be reviewed regularly, both by the university as part of its cyclical quality enhancement processes, and/or by your department or school, who may wish to make improvements to the curriculum, or in response to resource planning. As such, your course may be revised during the course of your study at Royal Holloway. However, your department or school will take reasonable steps to consult with students via appropriate channels when considering changes. All continuing students will be routinely informed of any significant changes.

Section 11 – Intermediate exit awards (where available)		
You may be eligible for an intermediate exit award if you complete part of the course as detailed in this document. Any additional criteria (e.g. mandatory modules, credit requirements) for intermediate awards is outlined in the sections below.		
Award	**Criteria**	**Awarding body**
PG Diploma	Passes in at least 120 credits, with fails of between 40% to 49% for up to 40 credits condonable (with the exception of any course specific requirements).	Royal Holloway and Bedford New College
PG Certificate	Passes in at least 60 credits with no condonable fails	Royal Holloway and Bedford New College

Section 12 - Associated award(s) with Banner Codes	
MSc in Mathematics of Cryptography and Communications (2130) PG Diploma in Mathematics of Cryptography and Communications (2131)	PG Certificate in Mathematics of Cryptography and Communications (3073)