MSc in Information Security

Royal Holloway
University of London
Royal Holloway is widely recognised on the world stage as one of the UK’s leading teaching and research university institutions. One of the larger colleges of the University of London, we are strong across the sciences, social sciences, arts and humanities. Our 8,000 students work with internationally renowned scholars in 18 academic departments. The University of London degree gained by our talented, high-achieving graduates is valued the world over.

As a cosmopolitan community, with students from over 130 countries, we focus on the support and development of the individual. Our friendly campus, just 19 miles west of central London, provides a unique environment for university study.

We aim to provide an understanding of the modern world and equip students with the skills necessary to succeed in the careers of the future.
This brochure describes the MSc in Information Security offered by the Information Security Group (ISG) at Royal Holloway, which is one of the largest groups of academic information security researchers in the world. The MSc is an interdisciplinary course taught by the ISG and security experts from industry.

Contents
Introduction 2
Information Security at Royal Holloway 3
Course duration and structure 4
Admissions 5
Programme overview 6
Degree classification scheme 9
Other information 10

The Course:
Security Management 12
Introduction to Cryptography & Security Mechanisms 13
Network Security 14
Computer Security (Operating Systems) 15
Security Technologies 16
Legal & Regulatory Aspects of Electronic Commerce 17
Application & Business Security Developments 18
Standards & Evaluation Criteria 19
Advanced Cryptography 20
Database Security 21
Computer Crime 22
Software Security 23
Smart Cards / Tokens Security & Applications 24
Digital Forensics 26
Security Testing Theory & Practice 27
MSc Project 28

Academic staff 30
Visiting Professors and Senior Visiting Fellows 36
Consultants 39
Our location 40

Contact details
Information Security Group Secretary
Royal Holloway, University of London
Egham, Surrey,
TW20 0EX
United Kingdom

T: +44 (0)1784 443093
F: +44 (0)1784 430766
E: isg-secretary@rhul.ac.uk
www.isg.rhul.ac.uk

This brochure is printed on Evolution 100 Premium Silk, a high quality FSC certified silk coated paper, made from 100% de-inked post consumer waste and produced without the use of chemical bleaching.
Introduction

The electronic handling of information is a defining technology of our age. Enormous volumes of information are routinely stored and transmitted worldwide – indeed, most aspects of our daily lives would come to a halt should the information infrastructure fail.

The field of Information Security, namely the study of countermeasures to real and serious threats to information security, has grown very rapidly in recent years. The subject embraces technologies such as cryptography, computer security, network security, digital forensics and fraud detection, as well as considering the management of security and the many trade-offs and subjective issues that need to be addressed when implementing information security within an organisation.

This MSc is a non-mathematical course. The programme, which can be studied full-time or part-time (day release or block mode) or by distance learning, provides students with a systematic understanding and critical awareness of current threats to the security of electronic information and the measures available to counteract these. It is designed to introduce all technical, legal and commercial aspects of Information Security and is intended as a foundation, or a building block, for a career in the field.

Students come from a variety of backgrounds, ranging from new graduates through to very senior security managers (often from blue chip enterprises). They are seeking a formal qualification in Information Security on a course that is well respected and well-known as the first of its kind in the world. To date more than 1,500 students from over 40 countries have completed the course.
Information Security at Royal Holloway

Research environment

The ISG is an interdisciplinary research group of computer scientists, mathematicians and social scientists. It is one of the largest academic information security groups in the world (with visiting professors and fellows, research assistants, support staff and around 60 PhD students complementing the core team of 17 academic staff). It has strong links with a number of industrial and government institutions and, in 1992, it introduced the MSc in Information Security, the first course of its kind in the world.

The Group holds a regular seminar series with considerable industrial participation and sponsorship, and the annual Hewlett-Packard Security Colloquium is held at Royal Holloway. As well as conducting several research projects funded by government and industry, the information Security Group is active in the European Union research programme ECRYPT and contributes to the International Technology Alliance programme supported by the MoD and DoD.

The ISG incorporates the Smart Card Centre, a venture established by Royal Holloway, Giesecke & Devrient and Vodafone as a venue for research and teaching on smart cards and tokens and their applications. For more details visit www.scc.rhul.ac.uk.

The lab facilities that are available to students allow security investigations and research to be performed in a realistic (but protected) environment. This includes a virtual penetration testing environment.

Queen’s Anniversary Prize

The Queen’s Anniversary Prizes for Higher and Further Education recognise and reward the outstanding contribution that universities and colleges in the UK make to the intellectual, economic, cultural and social life of the nation. The prizes are awarded within the national honours system. In 1998, Royal Holloway was awarded a Queen’s Anniversary Gold Prize in recognition of the Information Security Group’s work. Since then our international reputation has increased dramatically.

Our MSc has very large numbers of alumni from all over the world. Our theme of Academia and Industry in Harmony has flourished and more than 100 industrialists have lectured on our MSc. We have five visiting professors from industry and ISG members are continuously in demand to give keynote addresses at both academic and commercial conferences.

In recognition of the continuing contributions made by the ISG, the group was awarded the industry prize of the Best Information Security Team (government) at the 2007 SC Professional Awards. And on a slightly more humorous note, let us not forget about Dan Brown’s research activities for the Da Vinci Code that identified the ISG as (the?) leading IS group in the world!

“This pioneering Group provides a unique national resource for the training of information security specialists and the development of highly secure communications and computer systems. It offers world-leading independent expertise in a field of national importance where trust and integrity are paramount.”

Queen’s Anniversary Prize, 1998
The design and delivery of the MSc programme in Information Security draws extensively upon the research activities and expertise of staff of the Information Security Group (ISG).

<table>
<thead>
<tr>
<th></th>
<th>Full-time</th>
<th>Part-time</th>
<th>Block mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>one full academic year (50 weeks)</td>
<td>two full academic years (100 weeks)</td>
<td>one week (five day) courses over two academic years</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Distance Learning</td>
<td>two to four years</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Project Submission</td>
<td>September (week 50 of the academic year)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Autumn Term</th>
<th>Spring Term</th>
<th>Summer Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full-time</td>
<td>4 core modules</td>
<td>2 or 3 option modules</td>
<td>Independent Project</td>
</tr>
<tr>
<td>Part-time (day release)</td>
<td>1 day per week 2 core modules (Year 1 &amp; 2)</td>
<td>1 day per week 2 or 3 option modules (Over Year 1 &amp; 2)</td>
<td>Independent Project (Year 1 or 2)</td>
</tr>
<tr>
<td>Part-time (block mode)</td>
<td>1 week (5 day) courses</td>
<td>1 week (5 day) courses</td>
<td>Independent Project (Year 1 or 2)</td>
</tr>
<tr>
<td>Distance Learning</td>
<td>Modules and Independent Project are studied over the Autumn and Spring Terms</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
by studying modules either through the normal day release scheme, or through block mode, or through distance learning. Mixing the above modes of study offers a truly flexible way of completing the MSc programme.

Extra curricular activities
Through our excellent industry links, we are able to offer free industrially focused courses that are highly valued by the students. For example we provide a 2-day revision course for the CISSP exam which is also held on-campus, a 2-day course on Security in Banking delivered by a CISO from a major UK bank, a 2-day Foundstone Ultimate Web Hacking course, a one day KPMG Hacker bootcamp course, and a 2-day commercial firewall configuration course.

Admissions
Students are normally expected to have at least a Second Class Honours degree in a relevant discipline, or an equivalent qualification acceptable to the University of London. A relevant discipline includes, but is not restricted to, computer science, electronics, information systems and mathematics.

Applications from mature students, who do not possess a degree but have appropriate industrial or commercial experience, are also welcomed. For students for whom English is not the first language, a high level of competence in the English language will be required, typically a minimum IELTS of 7.0 in writing and 6.0 in other areas, or a TOEFL score of 600. All ‘non-standard’ applications are viewed sympathetically, each case being considered individually on its merits.

For an overview of the application process please visit: www.rhul.ac.uk/Graduate-School/apply.html

For specific queries about the Information Security Group and postgraduate admissions, please contact:

Pauline Stoner
Information Security Group Administrator
T: +44 (0)1784 443101 E: p.stoner@rhul.ac.uk
The MSc can be studied through two distinct pathways

- Technical Pathway
- Secure Digital Business Pathway

The Technical Pathway through the MSc places considerably more emphasis on Computer and Network Security, whereas the Secure Digital Business Pathway focuses on security infrastructures and legal aspects. Each Pathway has its own set of prescribed (core) modules.

The MSc degree is taught in course modules. Each module usually consists of three hours of lectures per week, sometimes with tutorials and practical work. Lectures are generally held on the same day. Part-time students can attend classes one day per week, which equates to a total of 44 days of lectures spread over two years (block mode students only attend five-day blocks). The curriculum for the MSc degree consists of six or seven taught modules and a project.

Of the taught modules, four are mandatory core modules and the others are optional modules chosen by the student from a list of options. The four core modules will be taught in the Autumn Term, and the optional modules will be taught in the Spring Term. Note that the two pathways share two modules, namely Security Management and Introduction to Cryptography and Security Mechanisms. Furthermore, several modules are not available in block mode, namely Legal & Regulatory Aspects of Electronic Commerce, Security Technologies, Advanced Cryptography, Digital Forensics, and Penetration Testing. For a list of modules that are available through Distance Learning, you should refer to the External Programme (www.londonexternal.ac.uk).

1. The Secure Digital Business Pathway is not available to Distance Learning students and is also not available through block mode.

2. Note that the block mode timetable operates on a two-year cycle, with half the core delivered in one year, and the remaining half in the other year.
For assessment purposes the MSc is broken down into three separate elements (core, options, and project).

Students on the Technical Pathway take the following four core modules:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IY5501</td>
<td>Security Management</td>
</tr>
<tr>
<td>IY5502</td>
<td>Introduction to Cryptography and Security Mechanisms</td>
</tr>
<tr>
<td>IY5511</td>
<td>Network Security</td>
</tr>
<tr>
<td>IY5512</td>
<td>Computer Security</td>
</tr>
</tbody>
</table>

Students on the Secure Digital Business Pathway take the following four core modules:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IY5501</td>
<td>Security Management</td>
</tr>
<tr>
<td>IY5502</td>
<td>Introduction to Cryptography and Security Mechanisms</td>
</tr>
<tr>
<td>IY5521</td>
<td>Legal and Regulatory Aspects of Electronic Commerce</td>
</tr>
<tr>
<td>IY5522</td>
<td>Security Technologies</td>
</tr>
</tbody>
</table>

Students on the Technical Pathway select two (or optionally three) of the following modules:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IY5521</td>
<td>Legal and Regulatory Aspects of Electronic Commerce</td>
</tr>
<tr>
<td>IY5601</td>
<td>Application and Business Security Developments</td>
</tr>
<tr>
<td>IY5602</td>
<td>Standards and Evaluation Criteria</td>
</tr>
<tr>
<td>IY5603</td>
<td>Advanced Cryptography</td>
</tr>
<tr>
<td>IY5604</td>
<td>Database Security</td>
</tr>
<tr>
<td>IY5605</td>
<td>Computer Crime</td>
</tr>
<tr>
<td>IY5606</td>
<td>Smart Cards/Tokens Security and Applications</td>
</tr>
<tr>
<td>IY5607</td>
<td>Software Security</td>
</tr>
<tr>
<td>IY5609</td>
<td>Digital Forensics</td>
</tr>
<tr>
<td>IY5610</td>
<td>Security Testing Theory and Practice</td>
</tr>
</tbody>
</table>

All students take the following compulsory element:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IY5500</td>
<td>Project</td>
</tr>
</tbody>
</table>

Students on the Secure Digital Business Pathway select two (or optionally three) of the following modules:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IY5501</td>
<td>Security Management</td>
</tr>
<tr>
<td>IY5502</td>
<td>Introduction to Cryptography and Security Mechanisms</td>
</tr>
<tr>
<td>IY5503</td>
<td>Advanced Cryptography</td>
</tr>
<tr>
<td>IY5504</td>
<td>Database Security</td>
</tr>
<tr>
<td>IY5505</td>
<td>Computer Crime</td>
</tr>
<tr>
<td>IY5506</td>
<td>Smart Cards/Tokens Security and Applications</td>
</tr>
<tr>
<td>IY5507</td>
<td>Software Security</td>
</tr>
<tr>
<td>IY5509</td>
<td>Digital Forensics</td>
</tr>
<tr>
<td>IY5510</td>
<td>Security Testing Theory and Practice</td>
</tr>
</tbody>
</table>
The Project is a significant piece of individual work assessed by a report of between 10,000 and 20,000 words. As a very rough guide, the project report should be around 50 pages long. This measure assumes fairly dense text, reasonable line spacing, font size (typically between 10 and 12) and the use of reasonable margins. The project has to be submitted in week 50 of the academic year (this always falls in the first half of September). Part-time students will normally submit their projects at the end of their second year of studies. For Distance Learning students the submission deadline is 31 March.

The Project and the optional modules give students the opportunity to pursue their own interests in more detail. The Project is a major individual piece of work. It can be of academic nature and aim at acquiring and demonstrating understanding and the ability to reason about some specific area of information security. Alternatively, the project work may document the ability to deal with a practical aspect of information security.

3. Except for Distance Learning students
To decide whether or not a student will be awarded the MSc degree, and also to decide whether or not a distinction will be awarded, the assessment results from each of the three programme elements (the core, options and project elements) will be used.

To pass the degree programme, the student will normally need to achieve each of the following:

- an average of at least 50 percent where the average is computed over the three elements, and where the core is given weight twice that given to the other two elements (i.e. so that the core element contributes 50 percent of the overall mark, and the other two elements 25 percent each);
- minimum of 50 percent for the core element;
- minimum of 40 percent for the options and project elements, and a minimum of 50 percent for at least one of these two elements.

To be awarded a distinction in the degree programme, the student will normally need to achieve each of the following:

- an average of at least 70 percent, where the average is computed over the three elements, and where the core is given weight twice that given to the other two elements (i.e. so that the core element contributes 50 percent of the overall mark, and the other two elements 25 percent each);
- a minimum of 60 percent in each of the three elements.

A student who fails the degree at the first attempt is normally allowed only one further attempt to re-sit or re-take any element for which an element mark of less than 50 percent was obtained. Any such attempts must be made at the next available opportunity. In the case of a failed core or options element, students will only be allowed to re-sit or re-take modules in which the un-weighted exam score was less than 50.

“The ISG MSc programme at Royal Holloway was extremely valuable to my professional career. To the best of my knowledge, both the structure and contents of the programme are unmatched anywhere else.”

Marc Sel, Director, PricewaterhouseCoopers Advisory Services, Belgium
Curriculum development
The basic structure of the MSc was widely discussed with more than 30 institutions. These included government departments, large IT companies and many financial organisations. This exercise has ensured that the overall structure of the MSc remains stable. To ensure that the course is completely up-to-date, most of the modules involve significant input from recognised security experts from industry.

The main Steering Committee for the course consists of all the members of the Information Security Group. Curriculum development is further enhanced by input from The ISG’s visiting professors.

Although this latter group has no formal powers, their opinions are highly regarded and all their suggestions are taken very seriously and acted upon. A curriculum committee regularly meets to consider input from the above areas and also from student feedback activities.

Student support and guidance
Students are encouraged to discuss any problems arising in their studies with any member of the ISG and are assigned to a member of staff who acts as an Advisor. Most members of staff can be contacted in their offices during the working day, although if there are problems in contacting individuals then arrangements for meetings may also be made via email or through the ISG secretary.

During the first term, tutorials are arranged to complement and reinforce the lectures and to provide any necessary background material, depending on the needs of the students. Examples of tutorials that might be arranged include a basic introduction to computer networks and operating systems, and elementary mathematics (as necessary to understand the concepts in cryptography).

Typically, each week there will be one day devoted to a particular module within small tutorial groups, and the module lecturer will conduct a series of tutorials during that day with MSc students. If required, additional lunchtime provision will also be made for part-time students.

The David Lindsay Prize
The British Computer Society (BCS) Computer Security Specialist Group awards the David Lindsay Prize for the project report that best addresses innovative applications of Information Security. All MSc and BSc projects in the area of Information Security are eligible for the prize. The final decision is made by the BCS Computer Security Specialist Group each year. This is a highly regarded prize.

A number of MSc projects are chosen to receive Search Security awards. The awards are given to those projects which best present research in an area of information security of interest to information security managers and professionals. These projects are re-written as short articles for a general audience and published online at SearchSecurity.co.uk.
Security Management

Status: Core (both Pathways)
Module code: IY5501

Aims
This module emphasises the need for good security management. Its aims are to identify the problems associated with security management and to show how various (major) organisations solve these problems.

Objectives
On completion of the module, the student will be able to evaluate security management requirements; critically analyse alternative security management strategies and methods; propose effective methods for solving security management problems, and compare and critically evaluate different approaches to security management.

Course content
There will be 11 sessions lasting about three hours. Most sessions will consist of a lecture given by an outside industrialist, including the opportunity for questions and answers on the topics discussed. Students are also expected to engage in appropriate private study and to take part in the online discussion forums.

The list of topics may vary slightly to reflect developments in the subject but examples of recently covered topics are:
  Richard Walton (Visiting Professor to the ISG)
- The Principles of Information Security and its Management
  John Austen (QCC)
- Internal Control, Audit and Security
  Chris Potter (Pricewaterhouse Coopers)
- Information Security, Governance and the Law
  Chris Sundt (Independent)
- IS 27001 – Information Security Management for Business Benefit
  Richard Mayall (Acuity Risk Management)
- The Role of Risk Analysis and Management in Effective InfoSec.
  Les Krause-Whiteing (Accenture)
- Security Management – Systems, Models and Frameworks
  Lizzie Coles-Kemp (Royal Holloway)
- Building a World-class Information Security Architecture
  David Lacey (Consultant)
- The Business of Trust
  Paul Dorey (BP)
- Information Security Management in the Real World
  Graham Edwards (HBOS)
- Business Continuity – the Wider Context of Information Security
  David Sutton (O2 UK)

Key bibliography

Further recommended texts can be found online.
Introduction to Cryptography & Security Mechanisms

Status: Core (both Pathways)
Module code: IY5502

Aims
The approach of this module is non-technical. The primary objectives are to explain why cryptography is needed, what it provides, how basic cryptographic mechanisms work and what issues need to be addressed when implementing cryptography. The mathematical content of this module is minimal. Tutorial support for the elementary mathematics needed for this part of the course will be provided for those who require it.

Objectives
At the end of this module, students should be able to: explain exactly what cryptography can be used for; appreciate the differences between various types of cryptosystems and in which situations they are most usefully employed; identify the issues that need to be addressed when assessing what types of cryptographic mechanism are necessary to “secure” an application; describe several basic cryptographic mechanisms for providing each of the core security services; identify the limitations of cryptography and how to support it within a full security architecture.

Students completing this module should not expect to be able to design algorithms.

Course content
This course is divided into three parts:
Setting the Scene: the need for cryptography; core security services provided by cryptography; basic model of a cryptosystem; historical cryptosystems; security in theory and practice
The Cryptographic Toolkit: symmetric encryption algorithms; hash functions; message authentication codes; entity authentication techniques; pseudorandom number generators; public key encryption algorithms; digital signatures; freshness techniques; cryptographic protocols
Cryptography in Practice: key management; public key infrastructures; legal aspects of cryptography; cryptographic applications

Key bibliography
Essential reading:
Aims
This module is concerned with the protection of data transferred over public information networks, including computer and telecommunications networks. After an initial brief study of current networking concepts, a variety of generic security technologies are studied, including user identification techniques, authentication protocols and key distribution mechanisms. This leads naturally to consideration of security solutions for a number of network types, including LANs, WANs and routing aspects, proprietary computer networks, mobile and wireless networks and higher-level applications as exemplified by electronic mail.

Objectives
At the end of the module, students should have gained an understanding of the fundamentals of the provision of security in information networks, as well as an appreciation of some of the problems that arise in devising practical solutions to network security requirements.

Course content
Introduction to Networking and Network Security; An Overview of Biometrics; Email security; GSM and UMTS Security; Wireless LAN Security; Introduction to Secure Protocols; Routing Security; Secure Protocols – IPSec, SSL/TLS, and SSH; Firewalls; Intrusion Detection Systems

Key bibliography
Aims
This course deals with security mechanisms in modern computer systems and will consider the core concepts of memory protections; authentication; important access control models and policies; how access control is implemented in commercial products; why operating systems and computer systems remain vulnerable to attack, and how vulnerable systems can be strengthened to increase resistance to attackers.

Objectives
On completion of the course, students should be able to: demonstrate an understanding of the importance of security models with reference to the security of computer systems; describe the features and security mechanisms that are generally used to implement security policies; provide examples of the implementation of such features and mechanisms within particular operating systems; display breadth of knowledge of the security vulnerabilities affecting computer systems, and demonstrate an understanding of the main issues relating to software security in the context of computer systems.

Course content
- Concepts and Terminology
- Hardware protection mechanisms
- Authentication
- Authorisation
- Vulnerabilities
- Software Security
- Case Studies

Key bibliography
Security Technologies

Status: Core module, Secure Digital Business Pathway
Module code: IY5522

Aims
This course will: provide an overview of the fundamental technologies underpinning computer and networked applications, along with the associated security issues; examine how maintaining security through separation is a key aspect of operating system design; provide an overview of the main types of authentication mechanisms used in computer systems; describe the fundamental types of access control mechanisms; overview the fundamental principles of secure protocol design, and how they are used in deployed security protocols; examine the security threats and vulnerabilities found in particular types of networks; assess mobile and wireless communication technologies in terms of their security vulnerabilities.

Objectives
On successful completion of the course students will be able to: demonstrate a systematic understanding of the construction of information networks, specifically the architecture and operation of the Internet Protocol suite; demonstrate a clear understanding of the construction of a modern computer system, specifically the different hardware and software components which support multiprocessing; explain the causes and potential effects of vulnerabilities that affect computer systems and identify appropriate countermeasures; demonstrate a comprehensive understanding of different types of user authentication mechanisms in use within modern computer systems; provide an overview of different access control mechanisms used within computer systems, and evaluate the suitability of different access control mechanisms for different security requirements; provide a clear understanding of how strong authentication protocols, key exchange protocols and key exchange mechanisms suitable for use on open networks can be constructed; demonstrate a clear understanding of how the design principles for secure protocols are applied to the Internet, focussing on SSL/TLS; identify the key security threats faced in network environments, and be able to specify appropriate countermeasures; explain the basic differences between different wireless technologies, and evaluate the security requirements according to the particular needs of different wireless networking technologies.

Course content
Introduction to Computer and Network Architecutres
Introduction to Security
Platform and Operating System Security
User Authentication Mechanisms
Security Models and Access Control Mechanisms
Malicious Code
Introduction to Security Protocols
Network Security Threats and Countermeasures
Web Security
Wireless (WLAN and GSM/UMTS) Security

Key bibliography
Aims
This course, which will be directed almost entirely to non-criminal law with an emphasis on legal obligations and liabilities between private parties, will consider fundamental legal concepts and rules which apply to e-commerce activities; legal risk management techniques for information security managers, and the most significant of the regulatory aspects which apply to secure electronic commerce.

Objectives
On completion of this module, students will have gained an understanding of the legal underpinnings and government regulations applying to the use of e-commerce, as well as an understanding of managing legal risk.

Course content
The module will be divided into three main parts and will involve lectures from a number of legal experts.

Part I: The rules – an introduction to the law
Introduction; basic liability for online activities; e-commerce and the law of contracts; dematerialization of documents; legal restrictions on the movement and use of cryptographic technology; digital signature and electronic signature law; international e-commerce and the law; discussion: revisiting issues in a multinational context, and electronic ‘money’.

Part II: The rules applied – an introduction to corporate legal risk management
Systems and service procurement; corporate re-organisation and the IT security manager; network acceptable use policies, and records retention policies in the era of dematerialization.

Part III: Regulatory aspects of e-commerce
Government control of security technology; regulation of CAs/TTPs; data privacy legislation, and taxation of e-commerce.

Key bibliography
Christopher Reed, Internet Law: Text and Materials, Butterworths, 2004
The precise list of security applications may vary slightly to reflect developments in the subject. However, the initial set of application domains are likely to include: payment and e-commerce applications; web applications, and identity management.

**Key bibliography**

There is no single text which covers this course. The following list provides a useful starting point. Further bibliographies can be found on the ISG website.


**Aims**

This module will provide an in-depth coverage of some of the current issues and technological developments relating to the security of business and e-commerce applications. It will consider the role of security in perspective and demonstrate how security techniques form part of an application system. It will also examine how a particular situation may make certain aspects of security important and how an entire system might fit together.

**Objectives**

On completion of the module, students should be able to: identify and analyse the security issues that arise in a variety of applications; understand how and why particular applications address specific security concerns; analyse the various security issues in a particular application and explain how they relate to one another, and review how the security aims are met in a particular application.

**Course content**

The main lectures in this module are delivered by ISG staff, although descriptions of individual case studies may be given by visiting experts in several security application areas who discuss their own specialist topic. There is opportunity for questions and discussion.
Aims
Over the last few years, international standards bodies have produced a variety of security-related standards. This module examines some of the most important of these in detail. In doing so, it illustrates how international standards now cover many aspects of the analysis and design of secure systems. The material covered also puts certain other aspects of the degree course in a more structured setting.

Objectives
At the end of the module, students should have a clear understanding and critical awareness of the need for standard information security techniques, and be aware of the various sources for these techniques; understand the role and basic framework for information security management proposed by ISO/IEC 27001 and ISO/IEC 27002; understand the risks and safeguards associated with delegating a security service to a third party; understand the differences between a security service and a security mechanism, and how security services and mechanisms are used in the context of the OSI communications architecture; analyse the security frameworks for key management, access control and authentication; understand the history and the latest encryption algorithms; be able to analyse and evaluate the different standardised methods for constructing MACs, hash functions and digital signature schemes from lower level primitives, and compare critically the usefulness of different algorithm choices in different situations; be able to analyse and evaluate a variety of standardised protocols for providing two parties with entity authentication and key agreement, and compare critically the usefulness of different protocols in different situations; be able to discuss the development of modern security evaluation criteria; and understand the Common Criteria framework for security evaluation.

Course content
The course consists of 11 lectures covering the following topics: introduction of cryptographic and information security standards; Security Management; Security Architectures; Security Algorithms; Security Protocols; and Evaluation Criteria.

Key bibliography
Advanced Cryptography

Status: Optional module
Module code: IY5603

Aims
This course will introduce students to commonly used cryptographic algorithms; explain the need for algorithms with different properties; cover a wide variety of algorithms and their analysis; study the performance and security trade-offs between different kinds of algorithms, and develop an appreciation of the role of cryptographic algorithms as part of a solution.

Objectives
On completion of this module, students will be able to: describe in detail and explain a wide range of different cryptographic algorithms; be able to comment on the differences between algorithms and critically compare their properties; have a comprehensive understanding of the current state of the art with regard to the performance and cryptanalysis of a wide range of different algorithms, and have a critical appreciation of some of the newer research trends that are likely to influence cryptographic algorithm work in the coming years.

Course content
The role of cryptography and its place in the security infrastructure. Classification of different cryptographic algorithms and cryptographic attacks.

Block Ciphers: Design criteria, Testing, DES, AES and other algorithms; assessment of block ciphers; linear and differential cryptanalysis.

Stream Ciphers: System-theoretic and other approaches, LFSRs, Linear equivalence and other measures of complexity; combining functions; nonlinear generators; correlation attacks.

Asymmetric Cryptosystems: Finite fields, Factoring and discrete logarithms, Prime generation and testing, ElGamal, RSA, Digital signatures, DSS, Elliptic curve cryptography, Quantum Cryptography and Quantum Computing.

Key bibliography
Aims
This module covers several aspects of database security and the related subject of concurrency control in distributed databases. We will discuss methods for concurrency control and failure recovery in distributed databases and the interaction between those methods and security requirements. We will also examine how access control policies can be adapted to relational databases.

Objectives
At the end of the module, students should: understand how multi-level security can be preserved within a database whilst still permitting the concurrent execution of transactions; understand why confidentiality is so difficult to achieve within a statistical database, and understand the implications that security and its administration have in the context of commercial databases such as Informix and Oracle.

Course content
Transaction Processing
Serialisability Theory
Two Phase Locking
Centralised Recovery
Distributed Recovery
Security and Security Models
Relational Database Security
Statistical Database Security
Concurrency Control and Multi-Level Security
Oracle Security

Key bibliography


Aims
This module complements other modules by examining the subject from the criminal angle and presenting a study of computer crime and the computer criminal. We will discuss its history, causes, development and repression through studies of surveys, types of crime, legal measures, and system and human vulnerabilities. We will also examine the effects of computer crime through the experiences of victims and law enforcement and look at the motives and attitudes of hackers and other computer criminals.

Objectives
On completion of the module, students should be able to:
- follow trends in computer crime; relate computer security methodologies to criminal methods; detect criminal activity in a computerised environment; apply the criminal and civil law to computer criminality; understand how viruses, logic bombs and hacking are used by criminals, and appreciate the views of business, governments and the media to instances of computer crime.

Course content
- Introduction: Types of computer crime, history, surveys, statistics and global connections
- Legal Measures: Computer Misuse, Criminal Damage, Software Piracy, Forgery, Investigative Powers
- Case Studies: Investigations into hacking, cases and PC misuse
- Social Engineering
- Spam, Phishing and Pharming
- Malware: The types, effects and investigations
- DoS and Distributed DoS: The causes, mechanisms, case studies and counter-measures
- Network Crimes: Hacking methodologies via the Internet and attacks to other networks
- Investigations, Incident Handling and Forensic Examination
- The Future: The expansion of the Internet, pornography and other unsuitable material
- Identity Theft and Fraud

Key bibliography

Hedley & Aplin, *Blackstone’s Statutes on IT and E-Commerce*, Oxford University Press

Aims
This course will identify the vulnerabilities that can be introduced into programs through language features and poor programming practice; discuss the generic techniques that can be applied to improve the security of programs and applications, and consider the specific support provided for developing secure applications in the .NET Framework and JAVA.

Objectives
On successful completion of the module, students will be able to: explain the importance of security in the development of applications, particularly in the context of distributed software and web services; be able to identify poor programming practice; appreciate the support for secure software development that has been made available to programmers in the .NET Framework and JAVA, and have a critical appreciation of some of the newer research trends that are likely to influence software security work in the coming years.

Course content
Vulnerabilities and Attacks
Countermeasures
Mobile Code
Case Study: JAVA Technology
Case Study: The .NET Framework
Web Application Programming
Web Services Security
Deployment and Configuration

Key bibliography
Michael Howard, Steve Lipner, The Security Development Lifecycle
Mark G. Graff, Kenneth R. Van Wyk O’Reilly, Secure Coding: Principles and Practises
Objectives
By the end of the module the students should: have a general understanding of smart cards, RFIDs and their underlying technologies; have an appreciation of the trusted production environment used to manufacture smart cards; know the various operating systems in use, plus associated interoperability and security properties; understand SIM/USIM cards and how security is provided for mobile telephony; have an overview of how smart cards are used for secure banking and finance; understand how smart cards are used for passports, IDs and satellite TV; be aware of new smart chip & token technologies (including TPM/NFC) for securing platforms and applications; understand common-criteria security applied to smart cards and tokens; be aware of the range of attacks used against smart cards/RFIDs and their countermeasures plus how smart cards are tested/evaluated; be familiar with smart card application development environments for JAVA and SIM Toolkit; appreciate real world deployment and management issues for transport card systems; understand remote communication with the SIM (OTA) and secure SIM lifecycle management, and be able to formulate their own informed opinions about the future for smart cards and tokens.

NOTE: If a student passes this module and his/her project was supervised by the ISG Smart Card Centre, the student is permitted to state that he/she “specialised/majored” in Smart Card and RFID Security Systems.
Course content

The following lectures will be delivered by industry experts plus ISG and Smart Card Centre staff. There will be practical demonstrations and quizzes set within lectures to be answered by the group within following lectures. During private study, students are encouraged to read the course book.

Introduction to Smart Cards and RFID
Smart Cards – Trusted Production Environment
Operating systems, Interoperability and Security
SIM/USIM Cards – Applications and Security for Mobile Telephony
Smart Cards for Secure Banking & Finance
Smart Cards in IDs and Passports
RFIDs Explained
Advances in Smart Chips and Tokens for Platform
Overview of Trusted Platform
Common Criteria and Smart Cards
Security Attacks, Countermeasures and Testing for Smart Cards
Application Development Environments for JAVA and SIM Toolkit
OTA and Secure SIM Lifecycle Management
The London Transport Oyster Card

Key bibliography

Course Book: Mayes and Markantonakis, Smart Cards, Tokens Security and Applications, Springer 2008
**Digital Forensics**

**Status: Optional module**  
**Module code:** IY5609

### Aims

The module provides a fast-paced overview of the field of digital forensics, covering approaches and techniques for gathering and analysing traces of human and computer-generated activity in such a way that it is suitable for presentation in a court of law. Beginning with legal and procedural aspects, the module encompasses live as well as conventional storage and network forensics with particular emphasis on the limitations and possible counter-forensics techniques employed by skilled adversaries. The module aims to help gain an appreciation of underlying first principles of ways in which data that can subsequently be used as evidence is generated, stored, and transmitted in different environments and mechanisms for both collection and analysis.

### Objectives

On completion of the module, students will have gained an understanding of key legal and procedural aspects of digital evidence and procedures required to safeguard these for use in a court of law. They will also have a well-grounded understanding of the loci in host operating systems and network components where human or computer-generated activity will produce traces which can be identified and analysed as well as the uncertainties associated with collecting such information. Particular emphasis will have been placed on ways in which such evidence may be contaminated or its acquisition obfuscated or disabled altogether by malicious software or counter-forensics mechanisms.

### Course content

The course will cover the following main topics:

- Introduction to Digital Forensics
- Windows Host Forensics Fundamentals
- Unix and Linux Host Forensics Fundamentals
- Network Forensics
- Malware
- Special Devices and Systems
- Steganographic Mechanisms and Covert Channels
- Alternative Storage Mechanisms

### Key bibliography

- B. Carrier, *File System Forensic Analysis*, Addison-Wesley, 2005
- C. Benvenuti, *Understanding Linux Network Internals*, O’Reilly, 2005
- D. Liu, *Cisco Router and Switch Forensics*, Syngress, 2009
- J. Zdziarski, *iPhone Forensics*, O’Reilly, 2008
Security Testing Theory and Practice

Status: Optional module
Module code: IY5610

Aims
The aim of this module is to provide the foundations and theoretical underpinnings for an understanding of the way in which IT systems can be attacked and penetrated by circumventing security or exploiting vulnerabilities in the system. This will form the basis of a methodical approach to surveying and auditing systems, and prepare candidates to design secure systems, identify vulnerabilities, and defend systems against intrusion.

Objectives
After completing this course, students will have: gained an understanding of the legal aspects of carrying out a penetration test and an approach to preparing and managing such an audit; gained an in-depth understanding of network protocols; computer system architectures; and application systems; gained an understanding of the vulnerabilities in existing protocols, systems, and applications; and an understanding of the security technologies designed to mitigate these vulnerabilities; gained practical experience of how these vulnerabilities may be exploited in practice to penetrate a system.

Course content
Introduction to security auditing, legal aspects of penetration testing, standards and certification.

Pen testing approaches, and how to prepare and manage an audit.

Technical aspects of network security covering standards, protocols, routing, firewalls showing the theoretical basis of vulnerabilities and how these may be exploited in practice.

Technical aspects of computer security covering operating systems, access control in windows and linux/unix, host based intrusion detection, escalation of privileges and how to exploit these vulnerabilities in practice and how to harden systems.

Technical aspects of Internet based applications, web services, protocols, languages (e.g. SQL) and how these may be exploited using for example SQL injection and cross-site scripting; how to exploit these vulnerabilities in practice, and how to harden the applications.

A survey of non-standard and emerging technologies and review of potential threats these may lead to.

Key bibliography
T. Wilhelm, Professional Penetration Testing, Syngress, 2010
S. Harris et al., Grey Hat Hacking, 2nd ed. McGraw Hill, 2007
Module: IY5500

Overview
This is a compulsory course that contributes 25 percent to the total marks for the determination of the degree classification.

Aims
A project is a major individual piece of work. It can be of academic nature and aim at acquiring and demonstrating understanding and the ability to reason about a specific area of information security. Alternatively, the project work may document the ability to deal with a practical aspect of information security.

Objectives
The student will write a comprehensive dissertation on the topic of the project. On completion of the project students should have demonstrated their ability to: work independently on a security-related project, for which they have defined the objectives and rationale; apply knowledge about aspects of information security to a particular problem, which may be of an engineering, analytical or academic nature; produce a well-structured report, with introduction, motivation, analysis and relevant references to existing work.

Each student will have an academic project supervisor who may give advice on the conduct of the project and will monitor its progress. However, it is primarily the responsibility of the student to define and plan the MSc project. Students may do their projects off-site but must maintain contact with their academic supervisor, for example, by having good Internet connectivity.

Some projects may be supported by industrial partners of the Information Security Group. Students are encouraged to seek placements with industrial sponsors of their projects and to collaborate with industry on them.

It is expected that, for full-time students, the topic of the project will be agreed upon at the beginning of the second semester, so that preliminary work can be done during the second term, and that students will concentrate on their project after the course examinations in May. For part-time students, this process may proceed at a slower pace or be delayed until the second year.

Assessment
Projects will be assessed on the basis of the written report, and possibly on the basis of a demonstration or evaluation of an artifact such as a computer program. An oral examination may take place at the discretion of the examiners.

Submission
TWO COPIES of the dissertation must be submitted by 4pm on the closing date for submission. These should be handed to the Departmental Office (Room 243 McCrea Building) and a receipt obtained. The closing date for submission is the Friday of week 50 of the academic year. Candidates are encouraged to submit upon completion of the dissertation.

Timetable for project work: First term
At the beginning of the first term each student is assigned a personal advisor. During the term, students should consider, in consultation with their advisor, the topic area in which they wish to do their project. The advisor may act as supervisor of the project or suggest other members of staff whom the student may approach to be their supervisor.

The number of students that any one member of staff may supervise is limited. Students are advised to consult members of staff to ascertain whether they would be able and willing to supervise their proposed project topic. Students may nominate a willing member of staff to be their supervisor in week nine of the first term. Students who do not do so by week 11 will be assigned a supervisor. It is possible to change supervisor (and topic) but such a change would need approval by all parties concerned and fall within the constraints on numbers of students supervised by each individual supervisor.

Second term
Each student should meet his/her supervisor to discuss the scope of the project; such meetings should normally continue through the life of the project. Should students be seeking an industrial placement, they should also meet prospective industrial collaborators.
Every student shall provide his/her supervisor with a completed Project Description form by the end of the second term. This form gives details of the project plan, including title, objectives, methods to be used, and work plan.

**June to September**

This is the main period during which work should be undertaken on the project, although some students may wish to start their project work earlier in the year. Advice should be sought from project supervisors, and any other appropriate sources, at all stages, and the supervisor should also be kept informed of progress. It is advised that students should show their supervisor an almost final draft of their project dissertation at least two weeks before the submission deadline.

**Guidance on structure and content of project dissertation**

Typically, the project dissertation will be a document of about 50 pages. It must be the work of the candidate, and should be a readable and coherent account of the chosen topic. It should provide an outline of the scope of the project and describe the extent to which the objectives of the project are met. It should also describe its relation to any industrial placement with which it may be associated.

It is important that the students show that they have extended their source material by including a critical analysis of their chosen subject area. A student may do this, for example, by elaborating the treatment as found in the sources, by comparing different approaches to solving a problem, or by performing practical experimentation to inform their analysis.

The students should also reference their source material appropriately and demonstrate that they appreciate how the topics discussed relate to one another and to the rest of the subject area concerned.
Academic staff

Professor Peter Wild BSc (Adelaide) PhD (London)
Director, Information Security Group

Peter Wild received his BSc (Hons) degree in Pure Mathematics in 1976 from the University of Adelaide and the PhD degree in Mathematics in 1980 from the University of London. He has worked at the Ohio State University, Columbus, Ohio, the University of Adelaide and with the CSIRO, Australia. In 1984, he joined Royal Holloway where he is currently employed as a Professor in Mathematics and is the Director of the Information Security Group. His research interests are in combinatorics, design theory, cryptography and coding theory. He has acted as a data security consultant for a number of companies offering advice in algorithm analysis, key management and user identification protocols.

Professor Fred Piper BSc PhD (London)
CEng CMath FIEE ARCS DIC FIMA M.InstISP

Fred Piper was appointed Professor of Mathematics at the University of London in 1975 and has worked in information security since 1979. In 1985, he formed a company, Codes & Ciphers Ltd, which offers consultancy advice in all aspects of information security. He has acted as a consultant to over 80 companies including a number of financial institutions and major industrial companies in the UK, Europe, Asia, Australia, South Africa and the USA. The consultancy work has been varied and has included algorithm design and analysis, work on EFTPOS and ATM networks, data systems, security audits, risk analysis and the formulation of security policies. He has lectured worldwide on information security, both academically and commercially, has published more than 100 papers and is joint author of Cipher Systems (1982), one of the first books to be published on the subject of protection of communications, Secure Speech Communications (1985), Digital Signatures – Security & Controls (1999) and Cryptography: A Very Short Introduction (2002).

Fred has been a member of a number of DTI advisory groups. He has also served on a number of Foresight Crime Prevention Panels and task forces concerned with fraud control, security and privacy. He is currently a member of the Board of Trustees for Bletchley Park and the Board of the Institute of Information Security professionals. He is also a member of (ISC)2’s European Advisory Board, the steering group of the DTI’s Cyber Security KTN, ISSA’s advisory panel and the BCS’s Information Security Forum.

In 2002, he was awarded an IMA Gold Medal for “services to mathematics” and received an honorary CISSP for “leadership in Information Security”. In 2003, Fred received an honorary CISM for “globally recognised leadership” and “contribution to the Information Security Profession”.

In 2005 he was elected to the ISSA Hall of Fame. He was named Professional of the Year at the Communications in Business Awards 2005. In 2008 he was elected to be a Fellow of (ISC)2. In 2008 he was the first person to be elected to the InfoSecurity Europe Hall of Fame. In 2008 he was elected to the International Advisory Board of IMPACT (the International Multilateral Programme Against Cyber Threats).

Dr Zbigniew ‘Chez’ Ciechanowicz BSc PhD (London)
A.Inst.ISP
MSc Programme Director, Information Security Group

Chez received his BSc (Hons) in Pure Mathematics in 1975 from the University of London, and his PhD degree in Mathematics (also from the University of London) in 1980. He then worked at the National Physical Laboratory for five years specialising firstly in compiler validation, then in cryptography and digital signatures. He ended his stay at the Laboratory holding the rank of Senior Scientific Officer. His next appointment was as a full-time lecturer in the Computer Science Department of Royal Holloway, his main area of interest being cryptography. Between 1999 and 2005 Chez worked as a consultant at Zergo Ltd, and his main areas of interest there were risk analysis and security management. Whilst at Zergo he performed numerous security reviews for large Government departments and industrial institutions throughout Europe and the States. He was a principal author of Zergo’s own risk analysis method. Between 1996 and 2003 he was the editor of the Elsevier Information Security Technical Report, and is currently still on the editorial board. For an extended period Chez went on secondment to the Information Security Group as a Teaching Fellow, and also as Programme Director for the MSc in Information Security. In 1997 he became a founder member of the British Computer Society’s
ISEB Information Security Management Certificate Board and sat on the Board until 2004. Chez became a permanent member of the Information Security Group in 2001. He has also served as a member of ISC2’s CBK Review Committee. Whilst at Royal Holloway, Chez has been involved in a number of high profile consultancy activities including security studies for TfL’s Oyster Card.

Professor Simon Blackburn BSc (Bristol) DPhil (Oxon)
Simon Blackburn received his BSc in Mathematics from Bristol University in 1989 and his DPhil in Mathematics from Oxford University in 1992. From 1992 to 1995, he was a Research Assistant in the Department of Mathematics at Royal Holloway, specialising in Stream Ciphers. From 1995 to 2000, he was an EPSRC Advanced Fellow. He is currently a Professor in Pure Mathematics. His research interests include combinatorics, group theory and cryptography.

Dr Carlos Cid BSc PhD (UnB, Brazil)
Carlos Cid received his PhD in Mathematics from the University of Brasilia, Brazil, in 1999. After working for a short period as a lecturer in Brazil, he spent a year as a postdoctoral researcher at RWTH-Aachen, Germany. Between 2001 and 2003, he worked as a software engineer for an Irish start-up where he was involved in the design and development of hardware security modules and network security appliances. He joined the Information Security Group in October 2003, and is currently Reader in Information Security. Carlos has a broad interest in the area of Information Security, in particular cryptography.

Dr Lizzie Coles-Kemp BA (Hons) MSc PhD (London)
Lizzie Coles-Kemp was awarded a BA (Hons) in Scandinavian Studies and Linguistics from the University of Hull in 1988. She then worked as a UNIX software trainer and translator for several years, specialising in applications adapted for variants of secure UNIX. In 1991 she joined the Swedish security software company, Dynamic Software AB, eventually becoming director of the UK subsidiary, DynaSoft Ltd, with responsibility for UNIX security and smart card projects across Europe and in the US. In 1997 Lizzie left DynaSoft to become global IT Security Officer for the British Council and completed the Information Security MSc at Royal Holloway. She was also a lead assessor for Lloyds Register Quality Assurance (LRQA) auditing organisations to ISO/IEC 27001 and tScheme. She now works for the ISG as a lecturer in information governance and security management for the BSc in Biomedical Informatics which is a collaborative programme between St George’s, University of London, Kingston University and Royal Holloway. Lizzie also contributes to the distance learning version of the Information Security MSc. Her academic research areas are organisational theories applied to design aspects of information security management systems and the visualisation of information security concepts. In 2008 Lizzie completed a PhD in information security management systems at King’s College, London. She is a Primary Investigator on the Visualisation and Other Methods of Expression (VOME) project which is joint research between Cranfield University, Salford University, Royal Holloway (University of London), Sunderland City Council and Consult Hyperion. The project is funded by The Technology Strategy Board, Engineering and Physical Sciences Research Council (EPSRC) and Economic and Social Research Council (ESRC).

Dr Jason Crampton BSc (Hons) MSc, PhD (London)
Jason Crampton was awarded a BSc (Hons) in Mathematics from the University of Manchester in 1986. He worked as a maths teacher for several years and then for a trade union developing software for the collection, recording and reporting of subscription income. He completed a part time MSc in Computer Science in 1996 and a PhD in 2002. His research interests include role-based access control and the application of partial order theory to access control. Jason was promoted to Reader in 2007.

Dr Alex Dent M.Maths. (Oxon), PhD (London)
Alex Dent received his undergraduate degree from St. Peter’s College, Oxford, in 1998 and his doctorate from Royal Holloway in 2001. At the end of his doctorate, he joined the staff of the Information Security Group as a research assistant for the NESSIE algorithm evaluation project. During this project, he was part of the team responsible for evaluating the security of a series of public-key cryptosystems and the result of his work directly influenced the contents of several security standards.

“A pioneering course that continues to provide students with the essential knowledge and understanding of information security, with many graduates going on to fill senior roles.”

Malcolm Marshall, Partner, KPMG London
In 2004, he was awarded an EPSRC Junior Research Fellowship, one of ten awards made that year, to continue his research on the theory of provable security in public-key encryption schemes. In 2006, he was employed as a full-time lecturer at Royal Holloway. His main research interests are in the theory of provable security and how this theory can be applied to public-key cryptosystems. Alex was promoted to Reader in 2009. He teaches the campus-based and distance-learning versions of the “Standards and Evaluation Criteria” MSc course.

Andreas Fuchsberger BSc MSc (London) EUR ING CEng MBCS CITP

Andreas Fuchsberger received a BSc (Hons) in Computer Science in 1992 and an MSc in Information Security in 1993, both from Royal Holloway. Andreas lectures in the areas of network, computer and software security. He has over 18 years of experience in teaching and running training classes in IT security architecture, design and programming. He has published articles on programming and network security, intrusion detection/prevention and vulnerability analysis. From 1999 until 2000, he was employed as a principal Consultant for ISS until he joined eSecurity Inc as Technical Manager for EMEA. He rejoined the ISG in 2003. Andreas holds CISSP and ISSAP credentials of (ISC)². He is a registered Chartered Engineer (CEng) of the Engineering Council UK as well as a EUR ING of Fédération Européenne d’Associations Nationales d’Ingénieurs (FEANI).

Dr Konstantinos Markantonakis BSc (Lancaster University) MSc MBA PhD (London)

Konstantinos Markantonakis received his BSc in Computer Science from Lancaster University in 1995, his MSc in Information Security in 1996, his PhD in Smart card Security in 2000 and his MBA in International Management in 2005 from Royal Holloway, University of London. His main research interests include smart card security and applications; secure cryptographic protocol design, Public Key Infrastructures, key management, mobile phone security, embedded systems, RFID security. Since completing his PhD, he has worked as an independent consultant in a number of information security and smart card related projects. He has worked as a Multi-application smart card Manager in VISA International EU, responsible for multi-application smart card technology for southern Europe. He was also working as a Senior Information Security Consultant for Steer Davies Gleave, responsible for advising transport operators and financial institutions on information security and smart card technology projects. He joined the Information Security Group as a lecturer in 2002, and was promoted to Reader in 2007. He is also a member of the IFIP Working Group 8.8 on Smart Cards. He continues to act as a consultant on a variety of topics including smart card security, key management, information security protocols, mobile devices, smart card migration program planning/project management for financial institutions, transport operators and technology integrators.

Professor Keith Martin BSc (Glasgow), PhD (London), CMath FIMA

Keith Martin joined the Information Security Group as a lecturer in January 2000. He received his BSc (Hons) in Mathematics from the University of Glasgow in 1988 and a PhD from Royal Holloway in 1991. Between 1992 and 1996, he held a Research Fellowship in the Department of Pure Mathematics at the University of Adelaide, investigating mathematical modeling of cryptographic key distribution problems. In 1996, he joined the COSIC research group of the Katholieke Universiteit Leuven in Belgium where he was primarily involved in an EU ACTS project concerning security for third generation mobile communications. He has also held visiting positions at the University of Wollongong, University of Adelaide, and Macquarie University. Keith’s current main research interests include cryptography, key management and wireless sensor network security. Keith is also interested in e-learning and is a co-developer of the distance learning MSc in Information Security.

Dr Keith Mayes BSc PhD (Bath) CEng FIET A.Inst.ISP

Keith Mayes received his BSc (Hons) in Electronic Engineering in 1983 from the University of Bath, and his PhD degree in Digital Image Processing in 1987. He is an active researcher/author with publications in numerous conferences, books and journals. His interests include mobile communications, the design of secure protocols, communications architectures and security tokens as well as associated attacks/countermeasures.
Chris Mitchell received his BSc (1975) and PhD (1979) degrees in Mathematics from Westfield College, London University. Prior to his appointment in 1990 as Professor of Computer Science at Royal Holloway, University of London, he was a Project Manager in the Networks and Communications Laboratory of Hewlett-Packard Laboratories in Bristol, which he joined in 1985. Between 1979 and 1985 he was at Racal-Comsec Ltd. (Salisbury, UK), latterly as Chief Mathematician. Since joining Royal Holloway in 1990 he has played a role in the development of the Information Security Group, and helped launch the MSc in Information Security in 1992. His research interests mainly relate to information security and the applications of cryptography. He has played an active role in a number of international collaborative projects, including Open Trusted Computing, a recently completed EU 6th Framework Integrated Project. Other completed projects include the Mobile VCE Core 2 and Core 3 programmes, four EU 5th Framework projects (SHAMAN and PAMPAS on mobile security, USB_Crypt dealing with novel security tokens, and the Finger_Card project combining smart cards and biometrics), and two EU ACTS projects on security for third generation mobile telecommunications systems (USECA and ASPeCT). He is currently convenor of Technical Panel 2 of BSI IST/33, dealing with security mechanisms and providing input to ISO/IEC JTC1/SC27, on which he has served as a UK Expert since 1992. He has edited ten international security standards and published well over 200 research papers. He is a member of the editorial boards of The Computer Journal, IEEE Communications Letters, Information Management and Computer Security, and the International Journal of Information Security, and a member of the accreditation board of Computer and Communications Security Abstracts. He has been a member of Microsoft’s Trustworthy Computing Academic Advisory Board since 2003, he served as a member of the DoCoMo Euro-Labs Advisory Board between 2005 and 2009, and he continues to act as a consultant on a variety of topics in information security.
Academic staff continued

Professor Sean Murphy BA (Oxon) PhD (Bath)
Sean Murphy received a BA in Mathematics from Oxford University in 1985 and a PhD in Mathematics from the University of Bath in 1989. He has been at Royal Holloway since 1988 and is currently a Professor of Mathematics. His research interests centre on cryptology. He was a member of the European NESSIE project for evaluating cryptographic standards and of the executive committee of ECRYPT, the European Network of Excellence in Cryptology. He is a co-author of the books Cryptography: A Very Short Introduction and Algebraic Aspects of the Advanced Encryption Standard.

Dr Siaw-Lynn Ng BSc (Adelaide) PhD (London)
Siaw-Lynn Ng was awarded a BSc (Hons) degree in Mathematics and Computer Science from the University of Adelaide in 1995 and a PhD in Mathematics from Royal Holloway in 1998. She was a post-doctoral research assistant at Royal Holloway from 1998 to 2001. Her research interests include combinatorics, finite geometry and their applications in information security. Siaw-Lynn was appointed as a lecturer in 2001.

Professor Kenny Paterson BSc (Glasgow) PhD (London) FIMA
Kenny Paterson obtained his BSc (Hons) in 1990 from the University of Glasgow and a PhD from the University of London in 1993, both in mathematics. He was a Royal Society Fellow at the Swiss Federal Institute of Technology, Zurich, from 1993 to 1994, investigating algebraic properties of block ciphers. After that, he was Lloyd’s of London Tercentenary Foundation Fellow at the University of London from 1994 to 1996, working on digital signatures. He joined the mathematics group at Hewlett-Packard Laboratories Bristol in November 1996, becoming project manager in 1999. His technical work there involved him in international standards setting, internal consultancy on a wide range of mathematical and cryptographic subjects, and intellectual property generation. He joined the ISG in 2001. Kenny’s research interests span a wide range of topics: cryptography and protocols, network security, sequences, coding theory and information theory. Kenny leads the ISG’s participation in the International Technology Alliance and was recently awarded a prestigious EPSRC Leadership Fellowship. He is a member of the editorial board of the Journal of Cryptology.

Dr Geraint Price BSc (London), PhD (Cantab)
Geraint Price obtained his BSc in Computer Science from Royal Holloway, University of London in 1994 and his PhD from University of Cambridge in 1999. His PhD dissertation analysed the interaction between Computer Security and Fault Tolerance. From 1999 to 2001, he was a Research Associate within the University of Cambridge, working on projects related to Denial of Service attacks in networks. In November 2001, he joined the Information Security Group (ISG) as a Research Assistant to work on a project funded by PricewaterhouseCoopers on the future of Public Key Infrastructures. From late 2002 to mid 2004, he worked on a research project funded by the PKI Club at Royal Holloway. In Sept 2004, Geraint was appointed as Lecturer in Information Security. His current research interests include Public Key Infrastructures, Authentication and Identity Management, Denial of Service attacks and resilient security.

Professor Ruediger Schack Diplom-Physiker, PhD (LMU Muenchen)
Professor Ruediger Schack received his Diplom degree in Theoretical Physics in 1986 and his PhD in Theoretical Physics in 1991, both at the University of Munich. Subsequently, he held postdoctoral positions at the University of Southern California, the University of New Mexico and Queen Mary and Westfield College. He joined Royal Holloway in 1995. His main research interest is quantum information theory.

Dr Allan Tomlinson BSc (Strathclyde) MSc, PhD (Edinburgh)
Allan Tomlinson received his BSc in Applied Physics from Strathclyde in 1981, his MSc in Microelectronics in 1987 and doctorate in 1991, both from Edinburgh. He then joined the Institute of Microelectronics at the National University of Singapore, working on secure NICAM broadcasting and video compression. In 1994, he moved to Gi in California to work on the Digicipher II Conditional Access system for digital video broadcasting. Before joining the Information Security Group, he was Principal Engineer at Barco Communications Systems where he was responsible for the development of the “Krypton” DVB Video Scrambler. He also served for a number of years on the DVB Simulcrypt committee. He is currently a
lecturer in the Information Security Group. He joined the ISG in 2003 where his research interests are distributed systems, security, mobile network security, and trusted computing, with particular interest in issues of trust and privacy in these areas.

**Professor Michael Walker OBE FREng BSc PhD (London) Dr rer nat habil (Tuebingen) CMath FIMA FIET**

Michael Walker was, until his retirement in September 2009, the Group Research and Development Director for the Vodafone Group of companies, with the responsibility for the Group’s research activities, intellectual property and technology standards worldwide. He also led technology innovation and managed engagement with start-up companies for Vodafone, and was a member of the board of Vodafone Ventures, the venture capital arm of the company. Michael is currently Executive Technical Advisor to Vodafone. Michael holds the Vodafone Chair in Telecommunications at Royal Holloway, University of London, as a part-time professor, is a visiting professor at the University of Surrey, and is Vice Chairman of the mobile VCE – a group of universities and industries researching mobile communications. He sits on scientific advisory boards for the Universities of Warwick and Surrey, and some start-up companies. He was a member of the UK Technology Strategy Board, and was a member of the academic advisory board of the University of Karlsruhe. He has held a number of positions with standards bodies, including chairmanship of the body responsible for the security aspects of UMTS. He is currently chairman of the Board of the European Telecommunications Standards Institute. Before joining Vodafone, Michael was Head of Mathematics at Racal Research, and prior to that an academic at the University of Tuebingen in Germany. Michael is a Fellow of the Royal Academy of Engineering and a member of Council of the Academy. He is the current President of the Institute of Mathematics and its Applications. He was appointed an OBE in June 2009 for his services to the telecommunications industry.

**Dr Colin Walter BSc (Edin) PhD (Cantab), Director of Distance Learning MSc**

Colin Walter graduated from Edinburgh University in 1972 with 1st class honours in Mathematics and was awarded a PhD from the University of Cambridge in 1976 for work in algebraic number theory under Prof. J.W.S. Cassels. He was a member of the Mathematics Department of UMIST, Manchester, from 1984 to 2002. He then joined the certificate authority Comodo where he was Head of Cryptography until coming to Royal Holloway as Director of the Information Security Distance Learning Programme in 2009. His research interests include side channel leakage from crypto implementations, exponentiation and modular multiplication algorithms, and trusted computing.

**Dr Stephen Wolthusen Dipl.-Inform., Dr.-Ing. (TU Darmstadt)**

Dr. Wolthusen received his degrees from TU Darmstadt, Germany, where he also lectured in the graduate programme from 1999 to 2005 and joined the Information Security Group in 2006 where he is currently a Reader. He also is Full Professor of Information Security (part-time) in the Department of Computer Science at Gjøvik University College, Norway and is retained as Senior Scientist by the Fraunhofer IGD institute in Darmstadt, Germany, where he was previously on the scientific staff. He holds visiting positions at both the Harbin Institute of Technology, China, and the Virginia Tech Advanced Research Institute, VA, USA. He is author and editor of several books, past Editor-in-Chief of the journal Computers&Security, and has published more than 80 peer-reviewed research articles. His main research interests range from models of interdependencies and vulnerabilities in critical infrastructures to network security, particularly in the tactical domain, and digital forensics with an emphasis on concurrent and distributed systems.
Visiting Professors & Senior Visiting Fellows

Professor Henry Beker BSc PhD (London) BA (Open University) FREng CEng CMath CStat CSci

In 1988, Henry J Beker founded Zergo Limited (which later became Baltimore Technologies plc) and, as Chairman and Chief Executive, steered the company through listings on both sides of the Atlantic and presided over its phenomenal growth. Prior to this, Henry Beker was Managing Director of Racal-Guardata Ltd, having previously held positions of Head of Mathematics Department, Racal Comsec Ltd., and Research Director at Racal Research Ltd. In addition to providing security systems to a number of financial institutions worldwide, Henry Beker has also been very actively involved within various Standards bodies. This includes the American National Standards Institute’s work on wholesale and retail banking and the Standards Association of Australia formulating their EFTPOS Standards. He is joint author of Cipher Systems (1982), one of the first books to be published on the subject of protection of communications, and Secure Speech Communications (1985). From 1987 to 1989, he was Vice-President of the IMA, and was appointed President in 1998. Having relinquished his roles at Baltimore Technologies plc of Chief Executive (in 1999) and Chairman (in 2000), Henry is now devoting more time to his academic, educational and business interests. Henry founded the e-Learning Foundation initiative to provide portable computers for every schoolchild in the UK and was instrumental in engaging governmental interest. Among his many business interests, Henry is Chairman of Bladerunner Limited, a company that manages more than 100 fitness centres for corporate and local government.

Robert Carolina BA (Dayton) JD (Georgetown) LLM (London) Attorney-at-Law (Illinois, USA) Solicitor (England & Wales)

Robert Carolina qualified as a lawyer in 1991 and became an in-house lawyer with an Internet software developer in the US. He then worked in the specialist information technology law practice of Clifford Chance, the world’s largest law firm. He was subsequently a Partner at Landwell, the legal services arm of PricewaterhouseCoopers. Robert is now a Principal with Origin Ltd, a solicitors’ firm regulated by the Law Society of England and Wales. The firm engages in patent prosecution, technology transfer, IP portfolio analysis and valuation, IP litigation and IT regulatory matters. Robert’s practice focuses on legal protection of information technology inventions, technology transfer deals and regulation of information technology systems. He represents inventors, users, purchasers, and vendors of IT and telecommunications products and services and advises on electronic commerce transactions and projects. His clients include early stage businesses, private and public IT and communications companies, as well as major multinational financial institutions, located in Europe and the US.

Professor Whitfield Diffie BSc (MIT) Dr.sc.techn. (hc, ETH Zurich)

Whitfield Diffie began his career in security as the inventor of the concept of public key cryptography, which underlies the security of Internet commerce. He has made fundamental contributions to many aspects of secure communications and was instrumental in the rise of a public cryptographic research community. In the 1990s he turned his attention to public policy and played a key role in opposing government key-escrow proposals and restrictive regulations on the export of products incorporating cryptography. Diffie recently retired from his position as Chief Security Officer at Sun Microsystems and is now studying the impact of web services and grid computing on security and intelligence. Prior to assuming his position at Sun, Diffie was Manager of Secure Systems Research at Northern Telecom throughout the 1980s. Diffie is a fellow of the Marconi Foundation. He is the recipient of the National Computer Systems Security Award given jointly by the National Institute of Standards and Technology and the National Security Agency, the Levy Prize of the Franklin institute, and other awards. His work and career are treated at length in the book Crypto by Steven Levy.

Witfield Diffie was awarded an Honorary Degree of the University of London conferred by Royal Holloway in 2008.

Professor Paul Dorey BSc PhD (Southampton) CISM M.Inst.ISP M.I.Biol

Paul Dorey has over 25 years management experience in information security gained as a senior security and risk executive at Morgan Grenfell/Deutsche Bank, Barclays Bank and BP. His work has encompassed information security management, operational risk management, business continuity planning and crisis management, privacy and
the security of process control systems. Paul has consulted to several governments in protecting critical national infrastructure, was a founder of the Jericho Forum, and is the Chairman of the Institute of Information Security Professionals (IISP). He currently sits as an independent expert on the Permanent Stakeholders Group of the European Network Information Security Agency (ENISA). His industry recognition includes being awarded Chief Security Officer of the Year (2006), IT Security Executive of the Year (2008) and his induction into the IT Security Hall of Fame (2009). His interests include the problem of establishing and communicating trust in IT systems, risk convergence (integrating IT Security with physical security and other risk disciplines) and demonstrating the value of security investment. In addition to his academic interests, he currently runs two consultancy firms specialising in developing commercial security strategies and building programmes to improve security team capability and knowledge sharing in the industry.

**Professor Dieter Gollmann Dipl.-Ing. Dr.tech. (Linz) Dr.habil. (Karlsruhe)**

Prof. Dieter Gollmann received his Dipl.-Ing. in Engineering Mathematics (1979) and Dr.tech. (1984) from the University of Linz, Austria, where he was a research assistant in the Department for System Science.

He was a Lecturer in Computer Science at Royal Holloway, University of London, and later a scientific assistant at the University of Karlsruhe, Germany, where he was awarded the ‘venia legendi’ for Computer Science in 1991. He rejoined Royal Holloway in 1990, where he was the first Course Director of the MSc in Information Security. He was a Visiting Professor at the Technical University of Graz in 1991, an Adjunct Professor at the Information Security Research Centre, QUT, Brisbane, in 1995, and has acted as a consultant for HP Laboratories Bristol. He joined Microsoft Research in Cambridge in 1998. In 2003, he took the chair for Security in Distributed Applications at Hamburg University of Technology, Germany. He is a Visiting Professor with the Information Security Group at Royal Holloway, a Visiting Professor with the School of Software at Tsinghua University, Beijing, and was an Adjunct Professor at the Technical University of Denmark.


**Professor David Naccache PhD (Paris)**

David Naccache is a computer science professor at the University of Paris II, Panthéon-Assas and a member of the Computer Science Laboratory of the Ecole normale supérieure (Paris) and of the Centre de recherche en informatique of the University of Paris I, Panthéon-Sorbonne. He is the director of the EEJSI masters diploma at the University of Paris II and currently supervises 16 PhD students. Before joining academia, David was Gemplus’ SVP Research & Innovation and the manager of Gemplus’ Applied Research & Security Centre (90 engineers and researchers). He is the author of more than 80 papers in information security and cryptography and 80 patent families totalling 340 applications – many of which were effectively used in commercial products. David served in nearly 70 program committees of scientific conferences and is currently member of the editorial boards of the following journals: IEEE Security & Privacy, Cryptologia, ACM Transactions on Information and System Security, The Small Scale Digital Device Forensics Journal and Communication Networks and a member of the board of reviewers of Computers & Security.

In the past, he served on the editorial board of IEEE IT Pro and IET Information Security and Security. Amongst David’s most noteworthy results are attacks against the signature standards ISO 9796–1 (the attack led to the withdrawal of this standard) and ISO 9796–2 (the attack led to an amendment of this standard) and PKCS#1 v1.5. Amongst other functions, David is a forensic expert by the Court of Appeal Paris, member of the Banque de France’s Smart Card Security Commission, scientific advisor to the French commissariat à l’énergie atomique (CEA Leti), scientific advisor to Ingenico, member of the Scientific Council of Thomson Technicolor and one of the elected directors of the IACR. David is an ex reserve major (RC) of the French Armée de Terre. His current areas of interest are handset forensics, hardware security, computer forensics, number theory, public key cryptography and side channel attacks. [www.naccache.fr/research](www.naccache.fr/research)
Visiting Professors & Senior Visiting Fellows
continued

Professor Nelson Stephens BSc PhD (Manchester)
Nelson Stephens was awarded his Ph.D. in 1965 on Conjectures concerning elliptic curves from the University of Manchester, UK. He has held academic appointments in UK universities at East Anglia, Oxford, Cardiff and London. He has held visiting research positions at the universities of Paris-Sud, Saarbrucken, Concordia in Montreal, Erasmus in Rotterdam, and at the Max-Planck Institute in Bonn. In 1988 he held an Industrial Fellowship with British Telecom. His research interests include cryptography, algorithms and number theory. He has authored over 60 papers in journals, books and refereed conference proceedings. He now works as a freelance consultant.

Richard Walton received his B.Sc. (Hons) and Ph.D. in Mathematics from the University of Nottingham in 1968 and 1971 respectively. He studied with the Open University during the 1980s taking mainly Electronics courses and received his B.A. (Hons) in 1987. From 1971–1973 he was a lecturer in Mathematics at the North Staffordshire Polytechnic before joining GCHQ as a Mathematician at the end of 1973. He was appointed Companion of the order of the Bath (CB) in the 2003 New Year Honours.

His GCHQ career culminated in his appointment in January 1999 to the GCHQ Board as Director CESG, the National Technical Authority for Information Assurance. He held this post until October 2002 when he was seconded to the Cabinet Office to initiate work on the production of a National Strategy on Information Assurance.

His earlier posts included Head of the Division employing most of the GCHQ Mathematicians (1996–1999) and Head of the Mathematical Services Group in CESG (1985–1991). In the 1980s he initiated many of the changes in CESG’s public profile as they started to engage in open fora, both national and international, during the early stages of the development of open standards for computer security. He was the first member of GCHQ to attend open cryptographic conferences (Eurocrypt in 1982, Crypto in 1985). His actions were instrumental in achieving the change of GCHQ policy to publish the early CESG work on Public Key Cryptography.

He retired from the Civil Service in May 2003 and undertakes occasional consultancy through his own company, Walton-Mackenzie Ltd. Since retirement, he has published several papers on topics concerned with information security and serves on the IT policy panel of the IET. He was appointed as an independent member of the Defence Scientific Advisory Council in April 2004.
Consultants, technical & administrative staff

**John Austen BA FBCS NEBSS**

John Austen is a director of QCC InfoSec Training Ltd and Course Director for the Royal Holloway Diploma in Information Security. He was the Head of the Computer Crime Unit, New Scotland Yard, until September 1996. He was a career detective for 30 years, investigating the first major UK computer crime in 1976 and founding the Computer Crime Unit in 1984 – the first of its type in the world. He was responsible for the first successful arrests and prosecutions against hackers, organised crime groups, and information brokers. He trained all of his own staff, officers from each of the UK Police Forces and latterly police from Eastern Europe on courses held at the National Police Staff College (in Bramshill, Hampshire). John was the first Chairman of the Interpol Computer Crime Committee, serving from 1991 to 1996, and was responsible for the worldwide standardisation of Police procedure. He is a Fellow of the British Computer Society and a member of its Security Committee. He is a consultant to the Government on Computer Security, the Computer Misuse Act, and British Standard 7799. He is a scientific expert to the Legal Affairs Committee, Council of Europe, Strasbourg, and a contributor to its Recommendation for Criminal Procedural Law on Computer Related Crime published in 1995. He has been an official advisor to the Governments of the Czech Republic, Poland and Croatia. During the last 10 years, he has presented lectures to Government committees and international conferences throughout the world.

**Dr Mick Ganley BSc PhD (London)**

Mick Ganley graduated from Royal Holloway College in 1968 with a BSc in Mathematics and obtained a PhD in Algebra and Geometry from Westfield College in 1971. He then held academic appointments in the Mathematics Departments at York University and Glasgow University, with time spent at Washington State University and the University of Western Australia. His primary research interests were in the areas of combinatorics, geometry, algebra and number theory. In 1987, Mick moved into industry, working for the cryptographic security division of Racal. Subsequently, he was made a Racal Senior Manager and appointed as Head of Consultancy and Security Analysis. His main functions included managing all security analysis, audit and consultancy activities carried out by the security division; liaising with other Racal companies and the central Racal product team on new security products and systems; providing security input from research work, new techniques and conference/press feedback; liaising with CESG and the DTI on various security issues relating to the company and carrying out research work, and presenting results in published papers and at conferences. During all of this time, he maintained close links with Royal Holloway. In 2000, Mick left Racal to take up the position of Director of Consultancy at Cylink Consultancy Ltd. He left the company in mid-2002 to work as a freelance security consultant. His current client list includes a number of major multinational organisations. He also has a part-time contract with the ISG, for the provision of various consultancy services including lecturing on the MSc in Information Security and helping with the development of Distance Learning material.

**Jon Hart BEng MEng (Brunel) MSc (London)**

Jon received a joint BEng and MEng in Electronic and Computer Engineering from Brunel University in 2003, and an MSc from Royal Holloway in 2009. He has over nine years’ experience in IT support and computer and network security, specialising in LINUX and UNIX platforms. Before joining the ISG as network manager, Jon worked in the defence industry for two years as a software engineer.

**Tristan Findley BSc (Portsmouth)**

Tristan graduated from the University of Portsmouth in 2006 with a BSc in Computer Network Management and Design. He has worked in the IT industry for over six years in various capacities. He is currently focusing on security and networking technologies. He joined the ISG in 2006 as systems administrator.

**Pauline Stoner – ISG Administrator**

**Jennifer Lee – Term Time Secretary**
Royal Holloway's location on the A30 between Englefield Green and Egham is just 19 miles from the centre of London, minutes from the M25 and M3, M4 and M40. London Heathrow Airport is 7 miles away and trains from Egham to Waterloo take 35 minutes. College buses run to and from Egham station during term.

The Information Security Group is set in the beautiful grounds of Royal Holloway at Egham, Surrey. The campus is famous for its Founder’s Building – one of the most spectacular university buildings in the world – which was officially opened by Queen Victoria in 1886.

Disclaimer: This brochure 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 modules 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.