UNIVERSITY OF LONDON

Programme Regulations 2022–2023

Information Security

MSc
PGDip
Individual modules

Important document – please read
This document contains important information that governs your registration, assessment and programme of study

Contents

Important information regarding the Programme Regulations

About this document

Last revised 29 March 2022

As a student registered with the University of London you are governed by the current General Regulations and Programme Regulations associated with your programme of study.

The Programme Regulations are designed and developed by Royal Holloway, University of London which is responsible for the academic direction of the programme. The regulations take account of any associated arrangements at Royal Holloway. Programme Regulations, together with the Programme Handbook, will provide the detailed rules and guidance for your programme of study.

In addition to Programme Regulations you will have to abide by the General Regulations. These regulations apply to all students registered for a programme of study with the University of London and provide the rules governing registration and assessment on all programmes; they also indicate what you may expect on completion of your programme of study and how you may pursue a complaint, should that be necessary. Programme Regulations should be read in conjunction with the General Regulations.

The relevant General Regulations and the Programme Regulations relating to your registration with us are for the current year and not the regulations for the year in which you initially registered, nor regulations in the intervening years.

On all matters where the regulations are to be interpreted, or are silent, our decision will be final.

Further information about your programme of study is outlined in the Programme Specification which is available on the relevant Course page of the website. The Programme Specification gives a broad overview of the structure and content of the programme as well as the learning outcomes students will achieve as they progress.

Terminology

The following terminology is specific to the Information Security programme:

Module: Individual units of the programme are called modules. Each module is a self-contained, formally-structured learning experience with a coherent and explicit set of learning outcomes.

Mandatory modules: Modules which you are required to study.

Throughout the regulations, ‘we’ ‘us’ and ‘our’ mean the University of London; ‘you’ and ‘your’ mean the student, or where applicable, all students.

Final intake to Information Security

Due to the launch of a new MSc Cyber Security programme in October 2022 (subject to final approval), there will not be an intake of new students to Information Security from 2022–2023 onwards and notice of closure is given. The final assessments will take place in 2027; after this point it will no longer be possible to take or retake an assessment for Information Security.

Changes to Information Security Programme Regulations 2022–2023

There are no changes to the Information Security Programme Regulations for 2022–2023.

Alternative assessments during the Coronavirus (COVID-19) outbreak

In line with our current General Regulations, the University may offer you alternative assessments where necessary. This includes holding online timed assessments in place of written examinations, which are usually held at examination centres. Please note that this statement replaces any published information relating to assessments or written examinations in any of our materials including the website. Previously published materials relating to examinations should therefore be read in conjunction with this statement.

The University of London continues to work towards supporting the academic progression of all its students. The University also continues to be mindful of the health and wellbeing of its students during this pandemic, whilst protecting the academic standards of its awards.

1 Structure

Appendix B gives the module outlines.

Qualifications

1.1

The following named qualifications are awarded under the Information Security programme:

- MSc Information Security
- Postgraduate Diploma in Information Security

Qualification structure

1.2

The MSc Information Security consists of three elements:

- the Core element, comprising four mandatory modules (20 credits each) plus
- the Options element, comprising two modules (20 credits each) chosen from a list of options plus
- a compulsory Project (60 credits).

1.3

The Postgraduate Diploma (PGDip) in Information Security consists of two elements:

- the Core element, comprising four mandatory modules (20 credits each) plus
- the Options element, comprising two modules (20 credits each) chosen from a list of options.

1.4

The Postgraduate Certificate (PGCert) in Information Security is only available as an exit qualification.

Mixed mode

1.5

If you are registered for the MSc or PGDip Information Security, you may be permitted to study up to two modules on campus at Royal Holloway, University of London, through mixed-mode study.

Mixed-mode study enables students to study some modules by distance learning and others on campus at Royal Holloway, University of London. Whilst on campus, students may study a module over a single term, or over a concentrated period of time (normally one week) which is termed block mode. Full details on mixed-mode study can be obtained from the Programme Director.

Individual modules

1.6

All modules from the Information Security degree programme except for the Project are available to study on a stand-alone basis.

1.7

We may decide that you must successfully complete either one or two modules on a stand-alone basis before we will consider your application to register for the PGDip or MSc Information Security.

2 Programme redevelopment and withdrawal

2.1

It is no longer possible to register for the Information Security programme.

3 Registration

Effective date of registration

3.1

Your effective date of registration is 1 September in the year that you initially registered.

Period of registration

See the Programme Specification for the minimum and maximum periods of registration applicable to this programme.

3.2

The minimum and maximum periods of registration to complete the programme are counted from your effective date of registration.

Final assessments for Information Security will take place in 2026–2027, after which the programme will close. It will not be possible to take or re-take any assessments after this.

Code of conduct

See the website for the Virtual Learning Environment (VLE) code of conduct.

3.3

During virtual seminars and during all other online contributions, you must observe the code of conduct for online behaviour.

4 Recognition of prior learning and credit transfer

These regulations are to be read in conjunction with the General Regulations, Section 3.

Recognition of prior learning

4.1

Where prior learning is recognised, the decision to award credit (known as Accreditation of prior learning (APL)) shall be made by an academic appointed by the Programme Director.

Generally no more than 40 credits can be accredited for prior learning. Note that NCSC certification will generally not apply to a degree where APL has been granted.

For any queries regarding recognition and accreditation of prior learning, contact us using the *ask a question* button in the Student Portal.

Credit transfer

4.2

If you are a student or graduate of the University of London we will consider an application to transfer credit to the PGDip or MSc Information Security on a discretionary basis.

4.3

If you undertake any modules on campus through mixed-mode study, any credits achieved will be recorded as credit transfer, up to the maximum permitted modules.

See Section 1 for more information on mixed-mode study.

5 Module selection

Appendix A provides details of the programme structures and module titles.

Changing modules

5.1

You will only be allowed to change your choice of module after the registration deadline in exceptional circumstances and with the approval of the Programme Director. An administrative charge is payable for this. Once you have notified us that you intend to enter the examination for a module, we will not consider your application to change modules until all of the results for that session are published.

5.2

We will not allow you to change your choice of module if you have taken any element of the assessment for that module.

5.3

If you change your choice of options modules we may charge you a transfer fee.

Individual modules

5.4

You may take up to four credit bearing modules (80 credits) on a stand-alone basis without being registered for the MSc or PGDip. If you apply to progress to the MSc or PGDip and this is approved, you may be credited with any individual modules successfully completed.

See Section 8 for more information on transferring from an individual module to the PGDip or MSc.

6 Assessment for the programme

In line with our current General Regulations, the University may offer you alternative assessments where necessary. This includes holding online timed assessments in place of written examinations, which are usually held at examination centres. Please refer to Programme Specification for details on equipment that may be required for alternative assessments.

Assessment methods

Online seminars for modules are not compulsory, but you are strongly encouraged to participate.

6.1

Each module, except 'An introduction to cryptography and security mechanisms' IYM002 and the 'Project' IYM011, will be assessed by one two-hour unseen written examination.

6.2

'An introduction to cryptography and security mechanisms' IYM002 will be assessed by two elements: one two-hour unseen written examination (75%) and by coursework (25%).

6.3

The **'**Project' IYM011 will be assessed by two elements: one two-hour written examination (0%) and one dissertation (100%).

The examination is marked on a pass/fail basis and must be passed in order to pass the module. There is not a mark assigned to the examination element and the overall module mark will be based solely on the mark awarded to the dissertation.

Date of examinations

6.4

Written examinations take place in May each year.

See the General Regulations for the Rules for taking written examinations and for information about mitigating circumstances.

See the Portal for the list of examination centres.

Dates and requirements for the assessment for An introduction to cryptography and security mechanisms IYM002

6.5

The coursework for IYM002 should be submitted in the same academic year in which you take the written examination for IYM002.

6.6

The coursework for IYM002 must be submitted according to the instructions and deadlines given on the Virtual Learning Environment (VLE).

6.7

Coursework for IYM002 received after the deadline will not be marked, will not receive feedback from tutors, and will not count towards the overall mark for IYM002. This does not count as an attempt.

6.8

If you submit coursework for IYM002 but do not attempt the written examination, the mark you receive for the coursework will stand and be used to calculate the overall mark for the module when you take the written examination.

6.9

You must make an attempt at the written examination for IYM002 before we will permit you to make a second attempt at the coursework, even if you failed at your first attempt at the coursework.

6.10

If you do not submit coursework for IYM002, or if we receive it after the due date, you could still attempt the written examination for the module. However, the coursework will not receive a mark and you will therefore lose 25% of the total mark available for that module.

Where we have accepted your mitigating circumstances application, you may be permitted to sit your examination in a later session to that in which you submit the coursework.

Dates and requirements for the Project IYM011

6.11

The Project's written examination and dissertation must be attempted and submitted in the same academic year.

6.12

If you start the Project in one academic year, and do not submit the dissertation by 31 March in the same academic year, you will be deemed to have interrupted the Project. You are required to take the exam in the same year that you submit your project report.

6.13

Once you have been assigned a supervisor for the Project you must submit the Project dissertation and sit the Project written examination within three years. If you fail to do so, you will be deemed to have failed the Project module and you will be considered for the award of Postgraduate Diploma.

6.14

For the Project, you must submit an *outline plan* of the dissertation for approval to the Programme Director not later than 31 October in the academic year of submission of the dissertation.

6.15

For the Project, you must submit one *progress report* via your supervisor to the Programme Director by 31 January in the year in which the dissertation is to be submitted. The progress report will not form part of the final assessment, but is an essential study requirement. If you do not submit the progress report you may not be permitted to submit the dissertation.

6.16

You must submit an electronic version of the completed dissertation to arrive not later than 31 March (BST) in the academic year of submission. The electronic submission is via the VLE unless otherwise agreed. In the case of an interruption of the Project the dissertation should normally be submitted in the following year.

7 Retaking an assessment

Maximum number of attempts

7.1

The maximum number of attempts permitted at any element of assessment for a module is two. Elements of assessment include written examinations, coursework, project examinations and project dissertations.

When you can retake an assessment

7.2

If you obtain less than 50% in any module (the combined weighted mark for the elements of assessment for 'An introduction to cryptography and security mechanisms' IYM002) at a first attempt and have not yet satisfied the criteria for the award, you may choose to make a second attempt at the failed element of assessment, except for the 'Project' IYM011 where you must retake both elements of assessment.

7.3

If you obtain an overall mark of 50% or more (the combined weighted mark for 'An introduction to cryptography and security mechanisms' IYM002) in any module you will not be permitted to make a second attempt at any of the assessment elements for that module.

Capping

7.4

If you obtain less than 50% in any module at the first attempt and subsequently pass a resit you will receive a capped mark of 50% for that module.

7.5

For modules that have more than one element of assessment (IYM002 and IYM011) if you obtain a combined weighted mark of less than 50% at the first attempt, or receive a fail mark for IYM011 despite passing the dissertation, and subsequently pass at re-entry you will receive a capped mark of 50% for that module. This capping applies to the combined weighted mark for the module and not to the individual marks given for the written examination, dissertation or coursework.

Failure at a second attempt

See also details of the Progression within the programme in Section 8 and the Schemes of award in Section 9 for rules on satisfying the requirements of the degree and exit qualifications.

7.6

If you receive the result of 'Fail' on your second attempt at the assessment for a module, and you are still eligible to progress, then the highest mark for that module may be carried forward and considered for classification. However if you are no longer able to satisfy the requirements for the PGDip or MSc degree then your registration will cease and the Board of Examiners will consider whether you are eligible for an exit qualification.

Mark used for classification

7.7

If you retake the assessment for any module you will carry forward the higher of the two Fail marks achieved. The higher mark achieved will be used for classification purposes.

Retaking An introduction to cryptography and security mechanisms IYM002

7.8

If you are awarded marks for the coursework and written examination that together result in a mark of:

- 50% or above (Pass) you cannot make a further attempt at the assessments for the module, even if one of the elements has been given a mark of fail;
- 40–49% (Condonable Fail) you may choose to progress with the existing condonable mark or make a second attempt at the element(s) of the assessment that was failed. Only elements of the assessment that were failed may be re-attempted;
- 0–39% (Fail) you must make a second attempt at the assessment for the module if you wish to progress. Only elements of the assessment that were failed may be re-attempted.

Retaking the Project IYM011

7.9

If you receive the result of 'Fail' for the project report, with a mark of 40–49%, we will normally allow you to resubmit the project report with minor adjustments by the date specified in our response. The resubmitted project report will be considered the second and final attempt.

7.10

If you retake the Project you must retake all assessed elements of the Project.

7.11

An interrupted Project can be resumed the following year and, depending on how much supervision you have received in the academic year the Project was started, the amount of supervision when the Project is resumed will be limited to the unused supervision time. A new supervisor will be appointed if the original supervisor is no longer available.

7.12

If you interrupt your Project in two successive years you will have used up all your due supervision and will have the following options:

- to keep the same Project topic and make another attempt with no further supervision;
- to keep the same Project topic (or a related topic) and make another attempt with reduced supervision;
- to start again with a new Project topic and full supervision.

7.13

If you retake the Project module you have the following options:

- to keep the same Project topic and make another attempt with no further supervision, normally recommended for students who receive a mark of 40-49% on their first attempt at the project report
- to keep the same Project topic (or a related topic) and make another attempt with reduced supervision
- to start again with a new Project topic and full supervision.

7.14

If you submit a Project dissertation report you will be considered to have made an attempt at the Project.

If registered for an Individual module

7.15

If you are registered for an individual module and you receive the result of 'Fail' on your second attempt at the assessment for the module, then the highest mark for that module will count as the final result. If you apply to progress to the related PGDip or degree and this is approved, this mark will be taken into account for classification purposes.

8 Progression within the programme

See Section 6 for method of assessment.

8.1

In any one year you may attempt examinations in up to a maximum of six modules, excluding resits.

8.2

If you are registered for the MSc Information Security you must have completed the Core element, obtained at least 40% in all examined modules and not have more than two module marks below 50% before proceeding to the Project.

Transfer from the PGDip Information Security to the MSc Information Security

8.3

If you successfully complete the PGDip Information Security you will normally be permitted to transfer your registration to the MSc Information Security and receive appropriate credits.

8.4

To progress to the MSc Information Security you must have qualified for the award of the PGDip Information Security, and received a recommendation from the Board of Examiners that you may register for the Project element for the MSc degree. If you satisfy these requirements and wish to progress you must do so in the same year that you qualify for the PGDip. There is no automatic progression.

Transfer from the MSc Information Security to the PGDip Information Security

8.5

If you are registered for the MSc Information Security you may transfer to the PGDip at any time providing you are able to satisfy the conditions for that award.

Transfer from Individual modules

8.6

A mark or grade awarded for completion of an individual module may not be used to replace any mark or grade for a degree or diploma already awarded.

8.7

We will consider the transfer from an individual module to the PGDip or MSc on a case-by-case basis upon receiving a request to this effect.

You can request to transfer from an individual module to the PGDip or MSc by logging an enquiry via the *ask a question* button in the Student Portal.

Previous study recommended for Options modules

8.8

Students with relevant professional experience are not required to have completed the following previous study before taking Options modules, but are recommended to have done so:

Options module	Recommended previous study
Application security	Security management An introduction to cryptography and security mechanisms Network security
Advanced cryptography	An introduction to cryptography and security mechanisms
Cybercrime	None
Smart cards/tokens security and applications	An introduction to cryptography and security mechanisms
Digital forensics	Network security Computer security
Security testing: theory and practice	Network security Computer security
Human aspects of information security and privacy	None

9 Schemes of award

The date of award for Information Security will be 1 August in the year of the last assessment that contributes to the award.

MSc Information Security

9.1

To be considered for the award of the MSc, you must have attempted the examinations and dissertation for all three elements of the degree:

- the Core element [comprising four mandatory core modules];
- the Options element [comprising two modules chosen from a list of options];
- the Project element [comprising one examination and one dissertation].

9.2

To pass the MSc you must achieve an overall weighted average of at least 50%. Failure marks between 40–49% can be condoned in modules which constitute up to a maximum of 40 credits, provided that the overall weighted average is at least 50%, but a failure mark (i.e. below 50%) in the Project cannot be condoned. A mark of less than 40% in any of the modules cannot be condoned.

9.3

To be considered for an award with *distinction* for the MSc Information Security, you must have obtained an overall average of at least 70% (using the same weighting as applies in 8.1).

9.4

To be considered for an award with *merit* for the MSc Information Security, you must have obtained an overall average of at least 60% (using the same weighting as applies in 8.1).

9.5

A candidate for the award of the MSc who satisfies both the following criteria will automatically be raised into the next class of award:

(a) the overall weighted average mark must fall within 2% of one of the classification boundaries in paragraphs 8.2, 8.3 and 8.4, and

(b) the mark for the dissertation is above the classification boundary.

PGDip Information Security

9.6

To be considered for the award of the PGDip, you must have attempted the examinations for both elements of the PGDip:

- the Core element [comprising of four mandatory modules];
- the Options element [comprising two modules chosen from a list of options].

9.7

The PGDip may be awarded if a student achieves an overall weighted average of at least 50%, with no mark in any taught module which counts towards the final assessment falling below 50%. Failure marks between 40–49% are not usually condoned for the award of a PGDip, but if they are, such condoned fails would be in modules which do not constitute more than 40 credits.

9.8

To be considered for an award with *distinction* for the PGDip Information Security, you must have obtained an overall average of at least 70%.

9.9

To be considered for an award with *merit* for the PGDip Information Security, you must have obtained an overall average of at least 60%.

9.10

A candidate for the award of the PGDip who satisfies both the following criteria will automatically be raised into the next class of award:

(a) the overall weighted average mark must fall within 2% of one of the classification boundaries in paragraphs 8.7, 8.8 and 8.9, and

(b) the mark for at least 60 credits counting towards the award is above the classification boundary. The dissertation may be included in these 60 credits.

PGDip Information Security as an exit qualification

9.11

If you registered for the MSc Information Security you may be awarded the PGDip as an exit qualification if you are unable to complete the requirements of the MSc degree but you have attempted all assessment components and obtained at least 120 credits, which may include the Project.

9.12

The PGDip may be awarded if a student achieves an overall weighted average of at least 50%, with no mark in any taught module which counts towards the final assessment falling below 50% and has either chosen not to proceed to the Project, or has failed the Project on either the first or second attempt. Failure marks between 40–49% are not usually condoned for the award of a PGDip, but if they are, such condoned fails would be in modules which do not constitute more than 40 credits.

9.13

The PGDip Information Security as an intermediate or exit qualification may be awarded with merit or with distinction. If the Project element has been taken, this too can be considered for grading purposes by the Board of Examiners along with the core and options modules.

PGCert Information Security as an exit qualification

9.14

We may award the PGCert Information Security as an exit qualification if you do not complete the requirements of the PGDip or MSc degree, but do pass (with a mark of at least 50%) taught (i.e. non-Project) modules to the value of at least 60 credits. Marks leading to the award of a PGCert may not be condoned.

9.15

The Board of Examiners will decide if you can be awarded the PGCert Information Security. The Board of Examiners must be satisfied that the qualification represents a coherent programme of study.

9.16

To be considered for an award with distinction for the PGCert Information Security, you must have obtained an overall average of at least 70%.

9.17

To be considered for an award with merit for the PGCert Information Security, you must have obtained an overall average of at least 60%.

9.18

All assessments for the PGCert are marked and graded according to the assessment criteria for the degree in Information Security.

9.19

If we award you the PGCert Information Security you may not subsequently be awarded the PGDip or MSc Information Security.

Appendix A – Structure of the programmes

The syllabus for each module is provided in Appendix B.

Postgraduate Diploma in Information Security

Core element

Four mandatory modules:

Security management [IYM001] *(20 credits)*

An introduction to cryptography and security mechanisms [IYM002] *(20 credits)*

Network security [IYM003] *(20 credits)*

Computer security [IYM004] *(20 credits)*

+

Options element

Two modules chosen from the following:

Application security [IYM005] *(20 credits)*

Advanced cryptography [IYM008] *(20 credits)*

Cybercrime [IYM010] *(20 credits)*

Smart cards/tokens security and applications [IYM012] (*20 credits)*

Digital forensics [IYM015] *(20 credits)*

Security testing – theory and practice [IYM016] (*20 credits)*

Human aspects of information security and privacy [IYM017] *(20 credits)*

Note

1. The examination numbers are appended to the module titles in Appendix B and these numbers should be used when completing examination entry forms.
2. For mixed-mode study options see also regulation 1.5.

MSc in Information Security

Core element

Four mandatory modules:

Security management [IYM001] *(20 credits)*

An introduction to cryptography and security mechanisms [IYM002] *(20 credits)*

Network security [IYM003] *(20 credits)*

Computer security [IYM004] *(20 credits)*

+

Options element

Two modules chosen from the following:

Application security [IYM005] *(20 credits)*

Advanced cryptography [IYM008] *(20 credits)*

Cybercrime [IYM010] *(20 credits)*

Smart cards/tokens security and applications [IYM012] *(20 credits)*

Digital forensics [IYM015] *(20 credits)*

Security testing – theory and practice [IYM016] *(20 credits)*

Human aspects of information security and privacy [IYM017] *(20 credits)*

+

Project element

Project [IYM011] *(compulsory) (60 credits)*

Note

1. The examination numbers are appended to the module titles in Appendix B and these numbers should be used when completing examination entry forms.
2. For mixed-mode study options see also regulation 1.5.

Appendix B – Module outlines

Core element

Security management [IYM001]

Aims

This module will emphasise 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 those problems.

Objectives

On completion of the module, the student will appreciate the complexities of security management, and have seen how some companies attempt to solve these problems.

Assessment

One two-hour unseen written paper.

An introduction to cryptography and security mechanisms [IYM002]

Aims

The approach of this module is non-technical. The main objective is to introduce the students to the main types of cryptographic mechanism, to the security services which they can provide, and to their management, including key management. The mathematical content of this module is minimal. Support materials for the elementary mathematics needed for this module will be provided.

Objectives

On completion of this module students will have gained an understanding of the use of, and services provided by, the main types of cryptographic scheme. They should also have gained an appreciation of the need for good key management. This will include an appreciation of the general nature of: encryption techniques for providing confidentiality services (including stream ciphers, block ciphers and public key techniques), mechanisms for providing data integrity and origin authentication, including MACs and digital signatures, message exchanges to provide entity authentication and/or key establishment, and the use of Trusted Third Parties, such as Certification Authorities (CAs), to provide and support Public Key Infrastructures.

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

Assessment

One two-hour unseen written paper (75%) and coursework (25%).

Network security [IYM003]

Aims

This module is concerned with the protection of data transferred over commercial information networks, including computer and telecommunications networks. After an initial brief study of current networking concepts, a variety of generic security technologies relevant to networks are studied, including user identification techniques, authentication protocols and key distribution mechanisms. This leads naturally to consideration of security solutions for a variety of types of practical networks, including LANs, WANs, computer networks, mobile networks and 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.

Assessment

One two-hour unseen written paper.

Computer security [IYM004]

Aims

This module deals with the more technical means of making a computing system secure. This process starts with defining the proper security requirements, which are usually stated as a security policy. Security models formalise those policies and may serve as a reference to check the correctness of an implementation. The main security features and mechanisms in operating systems will be examined as well as security related issues of computer architecture. Specific well-known operating systems are then studied as case studies. Other areas investigated include the security of middleware, software protection and web security.

Objectives

On completion of this module 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 which are generally used to implement security policies;
- provide examples of the implementation of such features and mechanisms within particular operating systems;
- display a breadth of knowledge of the security vulnerabilities affecting computer systems;
- demonstrate an understanding of the main issues relating to Web security in the context of computer systems.

Assessment

One two-hour unseen written paper.

Options element

Application security [IYM005]

Aims

This module analyses the role of security from the perspective of business application design. The aim is to learn the fundamental processes that need to be incorporated into the application development lifecycle, and thus how to integrate security as a core component within an application architecture. This module uses case studies to support the learning of these fundamental application security design skills, to understand what decisions need to be made to both meet business requirements and to mitigate information security risks.

Objectives

On completion of the module the students should be able to:

- recognise a variety of security issues that arise in applications;
- review how the various security issues in a particular application relate to one another;
- understand how and why businesses address specific security concerns in their applications;
- appreciate the various aspects of integrating security into the application development lifecycle;
- analyse how security aims are met in a particular application;
- evaluate the effectiveness of security mechanisms in the technical and business context of the case studies.

Assessment

One two-hour unseen written paper.

Advanced cryptography [IYM008]

Aims

This module follows on from the introductory cryptography module (IYM002). In that module, cryptographic algorithms were introduced according to the properties they possessed and how they might fit into a larger security architecture. In this unit we look inside some of the most popular and widely deployed algorithms and we highlight design and cryptanalytic trends over the past twenty years. This module is, by necessity, somewhat mathematical and some basic mathematical techniques will be used. However, despite this reliance on mathematical techniques, the emphasis of the module is on understanding the more practical aspects of the performance and security of some of the most widely used cryptographic algorithms.

Objectives

On completion of this module, students will gain a broad familiarity of the inner-workings of many of today's most widely deployed cryptographic algorithms. Students will also develop a more detailed understanding of some of the most prominent algorithms.

Assessment

One two-hour unseen written paper.

Cybercrime [IYM010]

Aims

This module complements other modules by examining the subject from the criminal angle and presenting a study of cybercrime and the cyber 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 cybercrime through the experiences of victims and law enforcement and look at the motives and attitudes of hackers and other cyber criminals.

Objectives

On completion of the module students should be able to:

- follow trends in cyber crime;
- relate cyber security methodologies to criminal methods;
- detect criminal activity in a computerised environment;
- apply the criminal and civil law to cyber criminality;
- understand how viruses, logic bombs and hacking are used by criminals;
- appreciate the views of business, governments, and the media to instances of cyber crime;
- understand the need to gather and preserve digital evidence correctly so that legal actions can be brought.

Assessment

One two-hour unseen written paper.

Smart cards/tokens security and applications [IYM012]

Aims

This module will:

- provide an overview of smart cards/tokens and their properties;
- introduce various applications that exploit smart cards/tokens;
- examine benefits, threats and attacks;
- consider systems for the development, manufacture and management of smart cards/tokens;
- review smart card standards and security evaluation methodologies.

Objectives

On completion of this module students will be able to:

- identify constituent components, analyse strengths and weaknesses and identify new applications of smart cards;
- identify the steps in the manufacturing/personalisation processes, analyse and evaluate potential risks, and compare security safeguards;
- identify and compare the systems in use, analyse their strengths and weaknesses, and evaluate interoperability and security issues;
- analyse the range of capabilities of SIM/USIM cards and apply them to new service ideas, and evaluate the possible range of services and security measures;
- understand the main standards and applications of smart cards for banking and finance, compare them with earlier card solutions, and analyse strengths and weaknesses of the approaches;
- analyse the key role of the smart card for passports, IDs and satellite TV, and evaluate the security measures that have protected past and current cards;

- identify and describe new technologies, including TPMs, apply them to new applications and evaluate the likely suitability/success of such approaches;
- explain how Common Criteria may affect smart card design/development, analyse the different approaches and compare them with less formal methods;
- identify and describe the classes of attack and notable methods within each class, analyse countermeasures and evaluate practicality of attacks;
- identify, compare and evaluate different methods of developing applications for smart cards, and understand the development cycle and the use of practical tools;
- analyse the issues concerning smart card lifestyle management, and evaluate and compare methods of local and remote card management.

Assessment

One two-hour unseen written paper.

Digital forensics [IYM015]

Aims

The objective of this module is to introduce the foundations of digital forensics, from discovery to collection and analysis of evidence suitable for use in a court of law, or for purposes such as documenting compliance. This includes ways in which data is generated, stored, and transmitted in a number of settings including desktop and mobile environments as well as networks. Preserving the integrity of such evidence also in the presence of malware or explicit counter-forensic mechanisms as well as the means for discovering the presence of such mechanisms is also covered explicitly.

Objectives

On completion of the module students should be able to:

- have an understanding of audit and indirect dynamic activity records retained by operating systems, particularly in file systems;
- understand selected network protocols, collection and derivation of evidence allowing reconstruction of activities;
- be able to identify and apply sound forensic practices;
- be able to identify and counter obfuscation and counter-forensic techniques;
- have in-depth insight on retention characteristics of storage systems for desktop, mobile, and non-standard computing systems.

Assessment

One two-hour unseen written paper.

Security testing – theory and practice [IYM016]

Aims

This module provides the foundation and theoretical underpinning which aims to give an understanding of the way in which IT systems can be attacked and penetrated by circumventing security or exploiting vulnerabilities in the system.

This foundation forms the basis of a methodical approach to surveying and auditing systems, and prepares candidates to design secure systems, identify vulnerabilities, and defend systems against intrusion.

Objectives

On completion of this module students will have:

- gained an understanding of common approaches and methodologies used for carrying out and managing security and penetration testing, as well as an understanding of the legal aspects involved in such audits;
- gained a detailed understanding of some typical network protocols, relevant computer system architectures, and web application systems;
- gained an understanding of the vulnerabilities in some existing protocols, systems, and applications, and some common forms of attack; in addition, 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.

Assessment

One two-hour unseen written paper.

Human aspects of information security and privacy [IYM017]

Aims

This module engages with the psychological, perceptional, cultural, societal, political and ethical implications of information security and privacy. Information is a vital element of modern society. Every day, individuals and organisations generate an increasing amount of information that is automatically processed and stored. In most cases, these processes require some human intervention. Actions such as accepting an unfair privacy policy or opening a malicious email attachment cannot always be controlled by technical means, although they have a direct impact on the security and privacy of individuals and organisations. In fact, as stated by the '2015 Information Security Breaches Survey' commissioned by the UK Government, 50 per cent of the worst breaches suffered by UK companies were caused by inadvertent human error. In this module we will seek to move away from the technical aspects of the field and instead tackle the issues directly.

Objectives

- Understand how people fulfil information security goals.
- Explain the need of privacy in a computerised world.
- Identify biases that may affect an individual when making security or privacy decisions.
- Detect human vulnerabilities that may be present on a computer system.
- Understand the 'art and science' behind social engineering and develop social engineering penetration tests.
- Analyse cultures of risk within and beyond organisational settings to better understand how these cultures influence policy development and implementation.
- Examine the different biases and heuristics that affect risk perception and, therefore, security and privacy related decisions.

- Identity personality traits that affects individual security behaviours.
- Carry out privacy impact assessments, develop privacy policies and implement the appropriate privacy preserving controls.
- Develop, implement security awareness programs.

Assessment

One two-hour unseen written paper.

Project element

Project [IYM011]

Aims

The Project is a major individual piece of work. It can be of academic nature and aimed 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.

Objectives

The student will write a comprehensive dissertation on an information security topic. 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; and
- produce a well-structured report, including introduction, motivation, analysis, and appropriate references to existing work.

Supervisor

Each student will be assigned an academic project supervisor who may give advice on the choice of the project and will monitor its progress. However, it is primarily the responsibility of the student to define, plan and implement the MSc project.

Assessment

One two-hour unseen written paper and a submitted dissertation.

Appendix C – Assessment criteria

Where examinations feature essay-style questions, the following grade description criteria apply:

%	No specific marks are awarded for spelling, punctuation or grammar. However, any significant weaknesses in these areas which result in the examiner having difficulty comprehending an answer may result in less credit being awarded.
85+	Outstanding levels of accuracy and technical competence; deep understanding; near-comprehensive knowledge; exceptional independence of thought; exceptionally well-organised and original answers; high levels of ability in analysis of information; coherent structure; completely addresses all aspects of the question. As good as could be expected under examination conditions.
70-84	Very high levels of accuracy and technical competence; deep understanding; detailed knowledge; may show some originality in interpretation or analysis; high degree of creativity and independence of thought; high levels of ability in the analysis of quantitative or qualitative information; coherent structure; completely addresses all aspects of the question.
60-69	Good degree of accuracy and technical competence; clear understanding; good breadth of knowledge; some evidence of creativity and independence of thought; generally effective analysis of quantitative or qualitative information; coherent structure; arguments are well constructed; addresses most key aspects of the question.
50-59	Satisfactory degree of competence and technical accuracy; sound understanding and knowledge; familiarity with correct strategies for analysis of quantitative or qualitative information, but possibly with limitations in the process of analysis; adequate structure; there may be some omissions, limited clarity of expression and partial or incomplete understanding of some areas of the topic; addresses some key aspects of the question.
Pass at 50	
40-49	There are some significant omissions or technical inaccuracies; some general understanding and knowledge; weaknesses in detail; the essay may not be fully focused on the question asked; familiarity with correct strategies for analysis of quantitative or qualitative information, but with significant errors in the process of analysis; simple structure.
Condonable 40	
20-39	There are serious technical errors and/or omissions that indicate poor understanding; there may be a failure to address the question asked; information largely erroneous or has little or no relevance to the question; significant confusion over appropriate analysis of quantitative or qualitative information; analytical work incomplete and erroneous; inadequate structure, with no sense of logical argument.

0-19	The answer shows a clear lack of understanding with major technical errors and omissions; there is little attempt to address the question; information erroneous or has no relevance to the question; substantial error and confusion over appropriate analysis of quantitative or qualitative information; complete inability to analyse information; incomplete, fragmentary or chaotic structure. Individual marks may be gained for individual accurate facts.

Grade description for Dissertation

%	
85+	Exceptional understanding of subject area; exceptional depth of content; outstanding technical accuracy and competence; significant originality in the construction of its research aims and questions; penetrating analysis and critical evaluation; ability to make informed judgements and develop original insights; ability to establish original lines of inquiry; employ different approaches to provide solutions to highly complex and novel problems. Professionally presented; written in an incisive and fluent style with few or no errors; clearly publishable standard of referencing. A high level distinction dissertation should be publishable with editing and minor revision.
70–84	Authoritative understanding of subject area; high degree of depth of content; very high technical accuracy and competence; some originality in statement and fulfilment of aims; ability to analyse critically and formulate questions; excellent research potential; ability to employ different approaches to the solution of complex and novel problems. Excellent presentation; written in a fluent and incisive style with no significant errors; close to publishable standard of referencing. A distinction dissertation should demonstrate professional standards of research.
60–69	Convincing display of understanding of subject area; good all round depth of content; good technical accuracy and competence; very satisfactory fulfilment of aims; challenging in parts; ability to analyse critically; clear evidence of the potential to undertake original research given appropriate guidance and support; ability to solve complex, though not entirely original problems. Well-presented and structured; written in a fluent style, with few errors; good referencing standard.

50–59	Sound knowledge and understanding of subject area; satisfactory depth of content; satisfactory sufficiency of content; satisfactory technical accuracy and competence; aims and objectives represent an acceptable challenge; satisfactory fulfilment of aims and objectives; ability to construct coherent and relevant answers to questions; few signs of originality and independence of thought; adequately presented and structured; straightforward presentational style with some errors; adequate referencing standard.
Pass at 50	
40–49	Basic knowledge and understanding of subject area; basic depth of content; borderline sufficiency of content; lack of clarity and accuracy in technical competence; aims fall just below an acceptable standard *and/or* failure to fulfil stated aims; answers are either incomplete or not entirely coherent; little evidence of independent thought; weak presentation *or* limited structure; presentation lacks clarity; significant errors of spelling, punctuation or grammar; weak referencing *and/or* inadequate bibliography.
20–39	Fragmentary knowledge and understanding of subject area; limited depth of content; limited sufficiency of content; little or fragmentary accuracy of technical content; no clear aims or questions asked; answers show only a limited degree of understanding; almost no evidence of independent thought. Poorly presented *and/or* inadequate structure; consistent lack of clarity throughout; significant errors of spelling, punctuation or grammar; little or no referencing and inadequate bibliography.
0–19	Entirely lacking in knowledge and understanding of subject area; totally inappropriate depth of content; totally inappropriate sufficiency of content; entirely lacking accuracy of technical content; no aims or questions asked; totally devoid of independent thought; poorly presented and/or inadequate structure; confused and incoherent; substantial errors of spelling, punctuation or grammar; no references and absent bibliography.