UNIVERSITY OF LONDON

BSc Computer Science

Module Specification

Key Information			
Module title	Computer Security		
Level	5	Credit value	15
Member Institution	Goldsmiths	Notional study hours and duration of course	150
Module lead author/ Subject matter expert	Robert Zimmer		
Module co-author	Matthew Yee-King		

Rationale for the module

With the increasing value of data stored on computer systems and the prevalence of viruses, malware and hacking, computer security has become a crucial part of the work of computer scientists. With an understanding of the modern security landscape, you will be able to write better, more secure software. The module will prepare you to think about security issues in your further studies and professional work.

Aims of the module

This module aims to provide you with an understanding of the need for computer security and the technologies that support it. It has both a theoretical component that will teach you mathematical underpinnings of security systems and a practical element that will help you discover the pitfalls of security design and to comprehend the mathematics underlying the protocols by programming small examples.

Topics covered in this module:

The topics listed here are an approximation of what will be covered. The topics presented may be slightly revised to ensure currency and relevance. Students will be advised of any changes in advance of their study.

1. Security threats
2. Social Issues in Computer Security
3. Access Control and Authentication
4. Security Models
5. Operating System Security
6. Network security
7. Cryptography
8. Cryptographic protocols and key management
9. Public Key Cryptography
10. Blockchain protocols

Approximately 10-12 hours of study will be required per topic. The remaining study time is intended for coursework and examination preparation.

Learning outcomes for the module

Students who successfully complete this module will be able to:

1. Explain several ways in which computer systems can be attacked and how defences can be implemented
2. Understand and describe the role that cryptography plays within the broader subject of computer security and how it is used in blockchain technology
3. Implement simple cryptographic algorithms
4. Assess the security needs given a particular situation
5. Design and break security systems
6. Analyse case studies and problems for given situations

Assessment strategy, assessment methods

Summative and Formative Assessments
The module will contain a range of summative and formative assessments. Summative assessments are assessments which contribute directly towards your final grade. Formative assessments do not count directly towards your final grade. Instead, they provide you with opportunities for low stakes practice, and will often provide some sort of feedback about your progress. For example, a practice quiz might provide you with feedback about why a particular answer was wrong.

Assessment Activities
The table below lists the assessment activity types you might encounter taking the module. It also states if that type of assessment can be automatically graded. For example, multiple choice quizzes can be automatically graded, and so can some programming assignments. It also states if that type of assessment will be found in the summative coursework and the summative examination. More details about the summative assessments are provided below.

Assessment activity type	Can it be automatically graded with feedback in some cases?	Coursework	Examination
Quiz Writing task	X	X X	X X
Simulation task	X	X	
Peer review task		X	

Pass Mark

In order to pass this module, you must achieve at least 35% in each element of summative assessment and an overall weighted average of 40%, subject to the application of rules for compensation. Please refer to the programme regulations for more information.

Summative Assessment Elements

As this is a module that has a significant amount of theory it is assessed as a theory-based module. This means that the summative assessment is composed of two elements, whose weightings are listed in the table below.

Summative Assessment Component	Percentage of final credit	Deadline
Coursework	50%	Mid session
Examination	50%	End of session

The coursework comprises a variety of practical exercises and quizzes which in total will take up to 25 hours of study time to complete. The examination will be two hours long, and consist of written answer and multiple choice questions.

Learning resources

The module will draw on a number of different, largely web-based, public resources as well as the resources produced as bespoke material for this module. The standard text book(s) for the module will be:

William Stallings. *Cryptography and Network Security: Principles and Practice, Global Edition*. Pearson 2016

Keith Martin. *Everyday Cryptography: Fundamental Principles and Applications*. Oxford 2017