1. **Title of the module**

COMP6340 (CO634) - Computer Security and Cryptography

1. **Division or partner institution which will be responsible for management of the module**

Division of Computing, Engineering, Mathematical Sciences (CEMS)

1. **The level of the module (Level 4, Level 5, Level 6 or Level 7)**

Level 6

1. **The number of credits and the ECTS value which the module represents**

15 credits (7.5 ECTS)

1. **Which term(s) the module is to be taught in (or other teaching pattern)**

Autumn or Spring

1. **Prerequisite and co-requisite modules**

Pre-requisite:

COMP3240 Computer Systems or COMP3370 Computers and the Cloud

COMP5270 Operating Systems and Architecture or COMP5570 Computer Systems

Module not to be taken by students having already taken COMP5580 Introduction to Cyber Security

1. **The courses of study to which the module contributes**

BSc Computer Science (all variants), Business Computing, BEng Computer Systems Engineering, Business Information Technology, Information Technology, and Year in Industry variants.

1. **The intended subject specific learning outcomes.  
   On successfully completing the module students will be able to:**

8.1 have an understanding of the algorithms used in cryptography and be able to perform implementations of selected algorithms in this area [A2][C1];

8.2 have an understanding of the threats faced by computer operating systems, applications and networks and the various countermeasures that can be used [A1][A3];

8.3 be able to make informed choices of the appropriate security measures to put into place for a given network and/or operating system [C2][B5];

8.4 have an understanding of how cryptography can be used for providing security within applications.

1. **The intended generic learning outcomes.  
   On successfully completing the module students will be able to:**

9.1 be able to apply relevant mathematical techniques [D4].

9.2 be able to analyse a problem specification and to design and implement a solution [B3][B4][D3].

9.3 to be aware of the relevant professional, ethical and legal issues in this subject area [B6].

9.4 be able to develop their own time management and organisational skills. [D5].

1. **A synopsis of the curriculum**

Security has always been an important aspect of computing systems but its importance has increased greatly in recent years. In this module you learn about areas where security is of major importance and the techniques used to secure them. The areas you look at include computer operating systems (and increasingly, distributed operating systems), distributed applications (such as electronic commerce over the Internet) and embedded systems (ranging from smart cards and pay-TV to large industrial plant and telecommunications systems).

1. **Reading list (Indicative list, current at time of publication. Reading lists will be published annually)**

Charles P. Pfleeger , "Security in Computing ", 2nd ed. , September 1996, Prentice Hall William Stallings, "Cryptography and Network Security : Principles and Practice", 2nd ed. , July 1998, Prentice Hall

Rita C. Summers, "Secure Computing : Threats and Safeguards", January 1997, McGraw Hill

Bruce Schneier , "Applied Cryptography : Protocols, Algorithms, and Source Code in C", 2nd ed., December 1995, John Wiley & Sons

Jonathan Knudsen , "Java Cryptography", May 1998, O'Reilly & Associates

Scott Oaks, "Java Security", May 1998, O'Reilly & Associates

Ingemar Cox, Matthew Miller & Jeffrey Bloom, “Digital Watermarking: Principles and Practice”, 2003, Morgan Kaufman.

1. **Learning and teaching methods**

Total contact hours: 30

Private study hours: 120

Total study hours: 150

1. **Assessment methods**
   1. Main assessment methods

2 hour written exam (70%)

Coursework (30%):

Security Concepts and Threat Analysis (15%)

Cryptography (15%)

* 1. Reassessment methods

Like for like.

1. **Map of module learning outcomes (sections 8 & 9) to learning and teaching methods (section12) and methods of assessment (section 13)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Module learning outcome** | *8.1* | *8.2* | *8.3* | *8.4* | *9.1* | *9.2* | *9.3* | *9.4* |
| **Learning/ teaching method** |  |  |  |  |  |  |  |  |
| Lectures | x | x | x | x | x | x | x | x |
| *Private study* | x | x | x | x | x | x | x | x |
| **Assessment method** |  |  |  |  |  |  |  |  |
| *Modular Arithmetic* | x | x | x | x | x | x | x | x |
| *Decryption* | x | x | x | x | x | x | x | x |
| *Security concepts and threat analysis* | x | x | x | x | x | x | x | x |
| *Cryptography* | x | x | x | x | x | x | x | x |
| *Authentication* | x | x | x | x | x | x | x | x |
| *Examination* | x | x | x | x | x | x | x | x |

1. **Inclusive module design**

The School recognises and has embedded the expectations of current equality legislation, by ensuring that the module is as accessible as possible by design. Additional alternative arrangements for students with Inclusive Learning Plans (ILPs)/declared disabilities will be made on an individual basis, in consultation with the relevant policies and support services.

The inclusive practices in the guidance (see Annex B Appendix A) have been considered in order to support all students in the following areas:

a) Accessible resources and curriculum

b) Learning, teaching and assessment methods

1. **Campus(es) or centre(s) where module will be delivered**

Canterbury

1. **Internationalisation**

The topics addressed by this module relate to a field which is of international importance, given the global role of computers in today's technological innovation. The topics covered by this module are international in nature, being identical worldwide and independent of traditional spoken language.

**DIVISIONAL USE ONLY**

**Revision record – all revisions must be recorded in the grid and full details of the change retained in the appropriate committee records.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date approved | Major/minor revision | Start date of delivery of revised version | Section revised | Impacts PLOs (Q6&7 cover sheet) |
| 10/12/2020 | Minor | September 2021 | 1,6,7,16 | No |
|  |  |  |  |  |