

COURSE DEFINITION

DEPARTMENT OF MATHEMATICS (INFORMATION SECURITY GROUP)					
Course Code:	IY2760	Course Value:	0.5	Status:	Core for BSc in Computer Science (Information Security)
Course Title:	Information Security			Availability:	Term 1
Prerequisites:				Recommended:	
Co-ordinator:	Professor Chris Mitchell				
Course Staff	Professor Chris Mitchell				
Aims:	<p>Information storage, communication, processing and management is probably the core application of computer technology, and the successful management of information resources is fundamental to the success of business both now and in the future. The significance of information to commercial enterprises means that securing this information is of fundamental importance.</p> <p>This course is concerned with providing a general introduction to the subject of Information Security as a whole. The key technologies are introduced, and, after taking this course, the student will be equipped with the necessary background knowledge to go on and gain an in-depth understanding of specialised topics within the subject area.</p>				
Learning Outcomes:	<p>On successful completion of this course, students will be able to:</p> <ul style="list-style-type: none"> • demonstrate an understanding of the successful and secure management of information resources; • apply the background knowledge gained to further study of the specialised topics within the subject area. 				
Course Content:	<p>The course will cover the following topics:</p> <ul style="list-style-type: none"> • <i>Introduction:</i> What is security (covering notions of Confidentiality, Integrity, and Availability)? Security threats and risks. Security management (ISO/IEC 17799). Data Protection legislation. • <i>Elements of cryptography:</i> Ciphers (DES/AES). Message Authentication codes (MACs). Public key ciphers and digital signatures (RSA). • <i>Identity verification:</i> Use and storage of conventional passwords. Dynamic password schemes. Biometric techniques. Use of tokens (dumb and intelligent), including the use of smart cards. • <i>Access control:</i> Access Control Lists, capabilities, security labels (MAC and DAC), and role-based access control. • <i>Personal computer security:</i> Viruses, spyware, restricting access. • <i>CASE STUDY I:</i> Electronic payments (EMV). • <i>Network security concepts:</i> The concepts of security services and security mechanisms (as in ISO 7498-2). Firewalls. • <i>Authentication and key distribution:</i> The importance and relatedness of the concepts of key management and entity authentication in a network. Objectives of an entity authentication protocol. Some fundamental protocols (e.g. Kerberos). Using authentication protocols for key distribution, and other approaches to key establishment (including public key certificates and X.509). • <i>Software security.</i> • <i>CASE STUDY II:</i> Web security. 				
Teaching & Learning Methods:	110 hours, made up of 33 hours of lectures and 77 hours of non-assessed coursework and private study.				
Key Bibliography:	<p>The main recommended text for this course is: D. Gollmann, <i>Computer Security</i>, John Wiley & Sons, 2005 (2nd edition).</p> <p>Useful background:</p> <ul style="list-style-type: none"> • C. P. Pfleeger and S. L. Pfleeger, <i>Security in Computing</i>, Prentice Hall, 2006 (4th edition). • W. Ford, <i>Computer Communications Security</i>, 1994. • R. Anderson, <i>Security Engineering</i>, John Wiley and Sons, 2008 (2nd edition). • N. Ferguson and B. Schneier, <i>Practical cryptography</i>, 2003. • W. Stallings, <i>Cryptography and network security - principles and practice</i>, Prentice Hall, 2006 (4th edition). 				
Formative Assessment & Feedback:	This module will contain mandatory non-assessed coursework which students will be expected to complete and complete. Answers will be marked and returned with feedback.				
Summative Assessment:	<p>Exam 100%: 2 hours (answer 4 questions from a total of 6) – calculators will not be permitted. This course will be assessed solely by written examination.</p> <p>Deadlines: The written examination will be held in the summer term.</p>				