INFORMATION SECURITY GROUP
Course Specification 2013-14

Code:	IY5502	**Course Value:**	0.5	**Status:**	Core A / Core B
Title:	**Introduction to Cryptography and Security Mechanisms**			**Availability:**	Autumn term
Prerequisites:	None			**Recommended:**	None
Co-ordinator:	Keith Martin				
Course Staff	Keith Martin, Colin Walter, Michelle Kendall				
Aims:	This course will • introduce the main types of cryptographic mechanism • explain how different cryptographic mechanisms provide different security services • identify some key issues relating to the management of these services				
Learning Outcomes:	Successful completion of the course will enable students to: • Explain exactly what cryptography can be used for. • Describe several basic cryptographic mechanisms for providing each of the core security services. • Appreciate the differences between various types of cryptographic mechanism 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. • Identify the limitations of cryptography and how to support it within a full security architecture.				
Course Content:	This course is divided into three parts: 1. Setting the scene: • core security services provided by cryptography • basic model of a cipher system and use of cryptography • historical algorithms • security in theory and practice 2. Cryptographic Toolkit • symmetric and public key encryption • data integrity • entity authentication • digital signatures • cryptographic protocols 3. Practical aspects • key management • cryptographic applications				
Teaching & Learning Methods	• Eleven three-hour presentations with exercise sheets and handouts • Tutorials: weekly mathematics support tutorials; two small group tutorials; pre-examination tutorial • Moodle course space with forums and electronic resources • One laboratory session • Private study				
Key Bibliography:	**Essential reading:** K. M. Martin, Everyday Cryptography, Oxford University Press (2012). **Highly recommended:** N. Ferguson, B. Schneier and T. Kohno, **Cryptography Engineering**, Wiley (2010).				
Formative Assessment and Feedback:	Three sets of exercises containing exam-style questions are accepted for submission with feedback provided.				
Summative Assessment:	**Exam** 100(%) This course is assessed solely by written examination consisting of a two-hour-exam. *(1 compulsory question, 2 out of a further 4 questions)* **Coursework** 0(%) Coursework does not contribute to the final assessment for this course. **Deadlines:** The written examination will be held in the Summer term				

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department's policy of continuous improvement and development. Every effort will be made to notify you of any such changes.