INFORMATION SECURITY GROUP

Course Specification 2013-14

Code:	IY5603	**Course Value:**	0.5	**Status:**	Option
Title:	**Advanced Cryptography**			**Availability:**	Spring Term
Prerequisites :	Introductory Cryptography course			**Recommended:**	
Co-ordinator:	Sean Murphy				
Course Staff	Sean Murphy				
Aims:	This course will: • introduce students to commonly used cryptographic algorithms • explain the need for different algorithms with different properties • cover a wide variety of algorithms and their analysis • study the performance and security trade-offs between different kinds of algorithms • develop an appreciation of the role of cryptographic algorithms as part of a solution.				
Learning Outcomes:	On successful completion of this module students will: • be able to describe in detail and explain a wide range of different cryptographic algorithms • be able to comment on the differences between algorithms and critically compare their properties • have a comprehensive understanding of the current state of the art with regards to the performance and cryptanalysis of a wide-range of different algorithms • have a critical appreciation of some of the newer research trends that are likely to influence cryptographic algorithm work in the coming years				
Course Content:	• The role of cryptography and its place in the security infrastructure. Classification of different cryptographic algorithms and cryptographic attacks • *Block Ciphers:* Design criteria, Testing, DES, AES and some other algorithms. Assessment of block ciphers; Linear and differential cryptanalysis. • *Stream Ciphers:* System-theoretic and other approaches, LFSRs, Linear equivalence and other measures of complexity; Combining functions; Non-linear generators; Correlation attacks. • *Asymmetric Cryptosystems:* Finite fields, Factoring and discrete logarithms, Prime generation and testing. El Gamal, RSA, Digital signatures, DSS, Elliptic curve cryptography. Provable Security. • *Quantum Cryptography and Quantum Computing*				
Teaching & Learning Methods	• Eleven three-hour presentations • Questionnaires and exercise sheets • Pre-examination tutorial • Module web site contains materials and details of sources for further study				
Key Bibliography:	*Understanding Cryptography*: C. Paar and J.Pelzl. Springer. *The Handbook of Applied Cryptography*: A. Menezes, P. Van Oorschot and S. Vanstone. CRC Press. *Cryptography: Theory and Practice*: D. Stinson. Chapman and Hall / CRC Press.				
Formative Assessment and Feedback:	Question sheets. Answers will be discussed in tutorials				
Summative Assessment:	**Exam** 100(%) This course is assessed solely by written examination consisting of a two-hour-exam. *(3 out 5 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				