

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:	<p>This course will:</p> <ul style="list-style-type: none"> • 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:	<p>On successful completion of this module students will:</p> <ul style="list-style-type: none"> • 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:	<ul style="list-style-type: none"> • The role of cryptography and its place in the security infrastructure. Classification of different cryptographic algorithms and cryptographic attacks • <i>Block Ciphers</i>: Design criteria, Testing, DES, AES and some other algorithms. Assessment of block ciphers; Linear and differential cryptanalysis. • <i>Stream Ciphers</i>: System-theoretic and other approaches, LFSRs, Linear equivalence and other measures of complexity; Combining functions; Non-linear generators; Correlation attacks. • <i>Asymmetric Cryptosystems</i>: Finite fields, Factoring and discrete logarithms, Prime generation and testing. El Gamal, RSA, Digital signatures, DSS, Elliptic curve cryptography. Provable Security. • <i>Quantum Cryptography and Quantum Computing</i> 				
Teaching & Learning Methods	<ul style="list-style-type: none"> • 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:	<p><i>Understanding Cryptography</i>: C. Paar and J. Pelzl. Springer. <i>The Handbook of Applied Cryptography</i>: A. Menezes, P. Van Oorschot and S. Vanstone. CRC Press. <i>Cryptography: Theory and Practice</i>: D. Stinson. Chapman and Hall / CRC Press.</p>				
Formative Assessment and Feedback:	Question sheets. Answers will be discussed in tutorials				
Summative Assessment:	<p>Exam 100(%) This course is assessed solely by written examination consisting of a two-hour-exam. (3 out of 5 questions) Coursework 0(%) Coursework does not contribute to the final assessment for this course.</p> <p>Deadlines: The written examination will be held in the Summer term</p>				

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.