COURSE SPECIFICATION FORM

for new course proposals and course amendments

<table>
<tr><td colspan="3">DEPARTMENT OF MATHEMATICS</td><td colspan="3"></td></tr>
<tr><td>Course Code:</td><td>MT5462</td><td>Course Value:</td><td>200hr</td><td>Status:
(ie:Core, or Optional)</td><td>Core for MfA and MCC MScs</td></tr>
<tr><td>Course Title:</td><td colspan="3">Advanced Cipher Systems</td><td>Availability:
(state which teaching terms)</td><td>Term 1</td></tr>
<tr><td>Prerequisites:</td><td colspan="3">UG courses in linear algebra and probability</td><td>Recommended:</td><td>none</td></tr>
<tr><td>Aims:</td><td colspan="5">To introduce and study the mathematical and security properties of both symmetric key cipher systems and public key cryptography, covering methods for obtaining confidentiality and authentication.</td></tr>
<tr><td>Learning Outcomes:</td><td colspan="5">On completion of the course the student should be able to:
Understand the concepts of secure communications and cipher systems;
Understand and use statistical information and the concept of entropy in the cryptanalysis of cipher systems;
Understand the main properties of Boolean functions, and their applications and use in cryptographic algorithms;
Understand the structure of stream ciphers and block ciphers;
Know how to construct as well as have an appreciation of desirable properties of keystream generators, and understand and manipulate the concept of perfect secrecy;
Understand the main mathematical and statistical properties of Feedback Shift Registers, and of FSR-based stream ciphers;
Understand the modes of operation of block ciphers and their properties;
Understand the main design principles and cryptographic techniques of modern symmetric cryptography algorithms;
Understand the concept of public key cryptography, including the details of the RSA and ElGamal cryptosystems, both in the description of the schemes and in their cryptanalysis;
Understand the concepts of authentication, identification and signature, be familiar with techniques that provide these, including one-way functions, hash functions and interactive protocols, and the Fiat-Shamir scheme;
Understand the problems of key management, and be aware of key distribution techniques.</td></tr>
<tr><td>Course Content:</td><td colspan="5">Cipher systems: An introductory overview of the aims and types of ciphers. Methods and types of attack. Information theory. Boolean functions. Statistical tests.
Stream ciphers: The one-time pad. Pseudo-random key streams – properties and generation. Mathematical and statistical properties of feedback shift registers. Berlekamp-Massey algorithm. Design principles and cryptanalytic techniques of modern stream ciphers.
Block ciphers: Confusion and diffusion. Iterated block ciphers – substitution/permutation. SP-networks. The Feistel principle. DES, AES. Modes of operation. Linear and differentiable cryptanalysis, and related cryptographic techniques.
Public key ciphers: Discussion of key management. Diffie-Hellman key exchange. One-way functions and trapdoors. RSA, ElGamal cryptosystem.
Authentication/identification: Protocols. Challenge/response. MACs. Zero-knowledge protocols; Fiat-Shamir protocol.
Digital signatures: Digital signature methods. Hash functions – design and analysis techniques. DSS. Digital certificates.</td></tr>
</table>

Teaching & Learning Methods:	44 hours of lectures and examples classes. 156 hours of private study, including work on problem sheets and examination preparation. This may include discussions with the course leader if the student wishes.
Key Bibliography:	Codes and Cryptography – D Welsh (Oxford 1988) *001.5436 WEL* Cipher Systems – H J Beker and F C Piper (Van Nostrand 1982) *001.5436 BEK*
Formative Assessment & Feedback:	Formative assignments in the form of 8 problem sheets. The students will receive feedback as written comments on their attempts.
Summative Assessment:	**Exam** (%) Four questions out of five in a two-hour paper: 100% **Coursework** (%) None **Deadlines:** n/a