COURSE SPECIFICATION FORM

DEPARTMENT OF: Mathematics				**Academic Session: 2017-18**	
Course Code:	MT3620	**Course Value:**	0.5	**Status:** *(ie:Core, or Optional)*	Optional
Course Title:	Cipher Systems			**Availability:** *(state which teaching terms)*	Term 1
Prerequisites:	MT1820 and some probability			**Recommended:**	
Co-ordinator:					
Course Staff					
Aims:	To introduce both symmetric key cipher systems and public key cryptography covering methods of obtaining the two objectives of privacy and authentication.				
Learning Outcomes:	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 structure of stream ciphers and block ciphers; • know how to construct as well as have an appreciation of desirable properties of key stream generators, understand and manipulate the concept of perfect secrecy; • understand the modes of operation of block ciphers and their properties; • understand the concept of public key cryptography, including 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, including the Fiat-Shamir scheme; • understand the problems of key management, be aware of key distribution techniques.				
Course Content:	**Cipher systems:** An introductory overview of the aims and types of ciphers. Methods and types of attack. Information theory. Statistical tests. **Stream ciphers:** The one time pad. Pseudo-random key streams - properties and generation. **Block ciphers:** Confusion and diffusion. Iterated ciphers - substitution/ permutation. The Feistal principle, DES, AES, Modes of operation. **Public key ciphers:** Discussion of key management. Diffie-Hellman key exchange. One-way functions and trap-doors. RSA; ElGamal cryptosystem. **Authentication/Identification:** Protocols. Challenge/response. MACs. Zero-knowledge protocols; Fiat-Shamir protocol. **Digital signatures:** Digital signature methods. Hash functions. DSS. Certificates.				
Teaching & Learning Methods:	33 hours of lectures and examples classes. 117 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:	Cryptography : theory and practice (3rd edition) - D. Stinson (Chapman & Hall/CRC, 2006) Library ref: 001.5436 STI Introduction to cryptography: with coding theory - W. Trappe and L.C. Washington (Pearson Prentice Hall, 2006) Library ref: 001.5436 TRA				
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** (%) A two-hour paper: 100% **Coursework** (%) None				

Updated September 2017