COURSE SPECIFICATION FORM

DEPARTMENT OF: Mathematics				**Academic Session: 2020-21**	
Course Code:	MT5462	**Course Value:**	200 h	**Status:** *(ie:Core, or Optional)*	Mandatory for MCC MSc
Course Title:	Cryptography I			**Availability:** *(state which teaching terms)*	Term 1
Prerequisites:	UG courses in linear algebra and probability			**Recommended:**	
Co-ordinator:					
Course Staff					
Learning Objectives:	The module introduces symmetric key cipher systems and public key cryptography and gives students a working knowledge of the theory and practice of cryptography.				
Learning Outcomes:	On completion of this module, a student will be able to define and analyse a range of abstract and practical cryptosystems, including stream ciphers based on Linear Feedback Shift Registers and a modern block cipher. They will also have a basic understanding of Public Key Cryptography including Diffie–Hellman key exchange and the RSA Cryptosystem. They should be able to understand the concepts of authentication, identification and signature and be familiar with techniques that provide these; they should be able to understand the problems of key management and be aware of key distribution techniques The student should be able to demonstrate a breadth of understanding appropriate for an M-level course.				
Teaching & Learning Methods:	40 hours of lectures. 160 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 assessment in the form of 8 problem sheets. The students will receive feedback as written comments on their attempts.				
Summative Assessment:	**Exam** (%) A two-hour written exam: 85% **Coursework** (%) Set exercises: 15%				

Updated December 2019