COURSE SPECIFICATION FORM

for new course proposals and course amendments

Department/School:	**Mathematics**	**Academic Session:**	**2020-21**
Course Title:	Cryptography II	**Course Value:** (UG courses = unit value, PG courses = notional learning hours)	200 h
Course Code:	MT5466	**Course JACS Code:** (Please contact Data Management for advice)	G100
Availability: (Please state which teaching terms)	Term 2	**Status:**	Optional for MfA Mandatory for MCC Condonable
Pre-requisites:	MT5462	**Co-requisites:**	-
Co-ordinator:	-		
Course Staff:	-		
Learning Objectives:	This module introduces students to some of the mathematical ideas essential for an understanding of public key cryptography.		
Learning Outcomes:	Upon completion of this module, the student should be able to demonstrate an understanding of the key mathematical ideas that underpin public key cryptography; understand several important public key cryptosystems; understand modern notions of security and attack models for public key cryptosystems. The student should be able to demonstrate a breadth of understanding appropriate for an M-level course and demonstrate independent learning skills.		
Teaching & Learning Methods:	30 hours of lectures. 170 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: an introduction – Nigel Smart (McGraw Hill) 001.5436 SMA Cryptography theory and practice – Doug Stinson (CRC press, 2nd ed.) 001.5436 STI		
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: 75%. **Coursework:** Miniproject: 10% Set exercises: 15%.		