COURSE SPECIFICATION FORM

for new course proposals and course amendments

Department/School:	**Mathematics**	**Academic Session:**	**2017-18**
Course Title:	Public Key Cryptography	**Course Value:** (UG courses = unit value, PG courses = notional learning hours)	0.5 unit
Course Code:	MT3660	**Course JACS Code:** (Please contact Data Management for advice)	G100
Availability: (Please state which teaching terms)	Term 2	**Status:**	Optional Condonable
Pre-requisites:	MT2630, MT3110 & MT3620	**Co-requisites:**	-
Co-ordinator:	-		
Course Staff:	-		
Aims:	To introduce some of the mathematical ideas essential for an understanding of public key cryptography, such as discrete logarithms, lattices and elliptic curves; To introduce several important public key cryptosystems, such as RSA, Rabin, ElGamal Encryption, Schnorr signatures; To discuss modern notions of security and attack models for public key cryptosystems.		
Learning Outcomes:	1. be familiar with the RSA and Rabin cryptosystems, the hard problems on which their security relies and certain attacks on them; 2. have a basic knowledge of finite fields and elliptic curves over finite fields, and the discrete logarithm problem in these groups; be familiar with cryptosystems based on discrete logarithms, and some algorithms for solving the discrete logarithm problem; 3. know the definition of a lattice and be familiar with the LLL algorithm and some applications of lattices in cryptography and cryptanalysis; 4. be able to define security notions and attack models relevant for modern theoretical cryptography, such as indistinguishability and adaptive chosen ciphertext attack.; be able to critically analyse cryptosystems; 5. have experience with implementing cryptosystems and cryptanalytic methods using a computer algebra package such as Mathematica.		
Course Content:	Background: Integers modulo n; Chinese remainder theorem; finite fields; fast exponentiation; public key cryptography and security; complexity theory. RSA/Rabin: Key generation; implementation; encryption and signatures; OAEP; the RSA problem and relationship with factoring; square roots modulo a prime; Hastad attack; Wiener attack. Discrete logarithms: Diffie-Hellman; ElGamal encryption; Schnorr signatures; Diffie-Hellman problem and decision Diffie-Hellman; methods to solve discrete logarithms such as baby-step-giant-step, Pollard rho and lambda, index calculus. Lattices: Definition of a lattice; GGH cryptosystem; LLL algorithm; lattice attacks on knapsack cryptosystems and variants of RSA. Elliptic curves: Group law; Hasse bound; group structure; point counting; ECC protocols; Maurer equivalence of DH and DL.		
Teaching & Learning Methods:	The total number of notional learning hours associated with this course are 150. 3 hours of lectures a week over 11 weeks. 33 hours total. 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: 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 assignments in the form of 8 problem sheets. The students will receive feedback as written comments on their attempts.		
Summative Assessment:	**Exam:** 100% Written exam. A two hour paper. **Coursework:** None		

Updated September 2017

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.