DEPARTMENT OF MATHEMATICS
CENTRAL UNIVERSITY OF JAMMU

TEACHING PLAN	
Course Title: Cryptography	**Duration of Examination: 3 hours**
Course Code: MAMT- 404	**Maximum Marks: 100**
Course Instructor : Dr. Deep Singh	
Lecture 1	Introduction to cryptography: private and public key cryptography
Lecture 2	Classical cryptography, substitution ciphers
Tutorial	Assignment/discussion/exercises
Lecture 3	Divisibility and greatest common divisors in Z
Lecture 4	The Euclidean algorithm and extended Euclidean algorithm
Tutorial	Assignment/discussion/exercises
Lecture 5	Modular arithmetic, prime numbers and unique factorization
Lecture 6	Fundamental theorem of arithmetic
Tutorial	Assignment/discussion/exercises
Lecture 7	Fermat's little theorem, primitive root theorem
Lecture 8	Symmetric ciphers, Encoding schemes, asymmetric ciphers
Tutorial	Assignment/discussion/exercises
Lecture 9	Origin of public key cryptography
Lecture 10	topic contd.
Tutorial	Assignment/discussion/exercises
Lecture 11	Discrete logarithm problem
Lecture 12	Deffie-Hellman key exchange
Tutorial	Assignment/discussion/exercises
Lecture 13	The El-Gamal public key crptosystem
Lecture 14	topic contd.
Tutorial	Assignment/discussion/exercises
Lecture 15	A collision for discrete logarithm problem
Lecture 16	The chinese remainder theorem
Tutorial	Assignment/discussion/exercises
Lecture 17	Integer factorization and the RSA crptosystem
Lecture 18	Euler's formula, roots modulo pq
Tutorial	Assignment/discussion/exercises
Lecture 19	The RSA public key crptosystem and its implementation and security issues
Lecture 20	Topic contd.
Tutorial	Assignment/discussion/exercises
Lecture 21	Primarily testing, Miler-Rabin test for composite numbers
Lecture 22	The prime number theorem, Riemann-zeta function
Tutorial	Assignment/discussion/exercises
Lecture 23	Riemann hypothesis, AKS primality test
Lecture 24	Pollard's p-1 factorization algorithm
Tutorial	Assignment/discussion/exercises
Lecture 25	Quadratic residues and quadratic reciprocity
Lecture 26	Quadratic residue modulo p and its properties
Tutorial	Assignment/discussion/exercises
Lecture 27	Legendre symbol, quadratic reciprocity

Lecture 28	Jacobi symbol, probabilistic encryption
Tutorial	Assignment/discussion/exercises
Lecture 29	The Goldwasser-Micali cryptosystem
Lecture 30	Information theorey: perfect secrecy, entropy, redundancy
Tutorial	Assignment/discussion/exercises
Lecture 31	Entropy of natural language, algebra of secrecy systems
Lecture 32	Complexity theory and P versus NP
Tutorial	Assignment/discussion/exercises
Lecture 33	Digital signatures: Definition and examples
Lecture 34	Components of digital signature scheme
Tutorial	Assignment/discussion/exercises
Lecture 35	RSA digital signatures
Lecture 36	topic contd.
Tutorial	Assignment/discussion/exercises
Lecture 37	ElGamal digital signatures
Lecture 38	Digital signature algorithm (DSA)
Tutorial	Assignment/discussion/exercises
Lecture 39	GGH lattice-based digital signatures
Lecture 40	NTRU digital signatures
Tutorial	Assignment/discussion/exercises