MMA-E415
CRYPTOGRAPHIC MATHEMATICS

MM : 100 Sessional : 30
Time : 3 hrs ESE : 70
L T P Pass Marks : 40
5 2 0

NOTE: The question paper shall consist of two sections (Sec.-A and Sec.-B). Sec.-A shall contain 10 short answer type questions of six marks each and student shall be required to attempt any five questions. Sec.-B shall contain 8 descriptive type questions of ten marks each and student shall be required to attempt any four questions. Questions shall be uniformly distributed from the entire syllabus. The previous year paper/model paper can be used as a guideline and the following syllabus should be strictly followed while setting the question paper.

Division algorithm, relatively prime numbers, greatest common divisor(gcd), Euclidean algorithm, modular arithmetic operation, extended Euclidean algorithm, Fermat's theorem, Euler's totient function, Euler's theorem, Miller-Rabin's primality testing algorithm, Chinese remainder theorem(CRT), Pollard rho method, primitive roots for prime numbers, discrete logarithm and modular arithmetic logarithm, discrete logarithm problem(DLP).

Introduction to cryptography, cryptanalysis and cryptology; ingredient of cryptography, types of cryptography, requirements for public key cryptography(PKC), easy and hard problems, applications of PKC, substitution techniques, Caesar cipher, Play fair cipher, Hill cipher, Polyalphabetic ciphers, one-time pad(OTP), rail fence transportation technique, stream cipher and block cipher (definition only), RSA, time complexity of an algorithm, big-O notation, security of RSA, Diffie-Hellman(DH) key exchange algorithm, man-in-the-middle attack, Elgamal cryptographic system, elliptic curves over finite fields, arithmetic operation in the set of elliptic curve points, elliptic curve cryptography(ECC),elliptic curve Diffie-Hellman algorithm(ECDHA), ECDLP, security of ECC, digital signatures, requirements for digital signatures, digital signature algorithm(DSA), Elgamal DSA (EDSA), Schnorr DSA (SDSA), elliptic curve DSA (ECDSA).

Row and column vectors; inner, outer and tensor (Kronecker) products of vectors; inner product of two vectors having components as complex numbers, norm of a vector, Hilbert space, Dirac (bra and ket) notations for vectors, representation of column vectors of an identity matrix as smallest ket vectors $|0\rangle$, $|1\rangle$, $|2\rangle$, ... etc, standard basis for a Hilbert space, change of basis, projection of a vector along another vector, representation of a vector using its projections on basis vectors, orthogonal projections, Gram-Schmidt orthogonalization method; Hermitian, unitary and rotational matrices; qubit, qutrit, ququart, qudit, multiple qubits, quantum states and quantum superposition principle, Bloch sphere representation of qubit states, separable (non-entangled) and non-separable quantum states, Einstein-Podolsky-Rosen(EPR) paradox, Bell states, pure and mixed quantum states, Pauli operators, quantum operations, joint quantum operations, quantum gates and circuits, quantum measurement.

Text /Reference Books

1. William Stallings, Cryptography and Network Security, Pearson Education, 2011. (ISBN 0-13-03221-0).
2. Steven D. Galbraith, Mathematics of Public Key Cryptography, Cambridge University Press, Version 2.0, 2018.
3. Martin Laforest, The Mathematics of Quantum Mechanics, University of Waterloo, 2015. (Unit-IV and V).
4. Michael A. Nielsen & Isaac L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, N. Y., 2010. [ISBN 978-1-107-00217-3](Unit-IV and V).
5. James S. Kraft and Lawrence C. Washington, An Introduction to Number Theory with Cryptography, Second Edition, CRC Press, Taylor & Francis Group , N. W., 2018. (ISBN-13: 978-1-1380-6347-1).
6. Lawrence C. Washington, Elliptic Curves Number Theoryand Cryptography, Second Edition, Chapman & Hall/CRC Press, Taylor & Francis Group, N.W., 2008. (ISBN-13: 978-1-4200-7146-7)[with Computer Packages : Pari, Magma and SAGE]