RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

CSE-Artificial Intelligence and Machine Learning/ Artificial Intelligence and Machine Learning, VI-Semester

Open Elective AL604 (B) Information Security & Management

UNIT-I

Introduction: Needs for Security; Basic security terminologies e.g. threats, vulnerability, exploit etc.; Security principles(CIA), authentication, nonrepudiation; security attacks and their classifications; Mathematical foundation - Prime Number; Modular Arithmetic; Fermat's and Euler's Theorem; The Euclidean Algorithms; The Chinese Remainder Theorem; Discrete logarithms**.**

UNIT-II

Symmetric Key Cryptography: Classical cryptography – substitution, transposition and their cryptanalysis; Symmetric Cryptography Algorithm – DES, 3DES, AES etc.; Modes of operation: ECB, CBC etc.; Cryptanalysis of Symmetric Key Ciphers: Linear Cryptanalysis, Differential Cryptanalysis.

UNIT-III

Asymmetric Key Cryptography: Key Distribution and Management, Diffie-Hellman Key Exchange algorithm; Asymmetric Key Cryptography Algorithm– RSA, ECC etc.; Various types of attacks on Cryptosystems.

UNIT-IV

Authentication & Integrity – MAC, Hash function, SHA, MD5, HMAC, Digital signature and authentication protocols; Authorization; Access control mechanism; X.509 Digital Certificate**.**

UNIT-V

E-mail, IP and Web Security: E-mail security – PGP, MIME, S/MIME; IP security protocols; Web security – TLS, SSL etc.; Secure Electronic Transaction(SET); Firewall and its types; Introduction to IDPS; Risk Management; Security Planning.

TEXT BOOKS RECOMMENDED:

1. Michael E. Whitman, Herbert J. Mattord, "Principles of Information Security", 6th Edition, Cengage Learning.

2. Stallings William, "Cryptography and Network Security - Principles and Practice", 7th Edition, Pearson.

REFERENCE BOOKS:

1. Roberta Bragge, Mark Rhodes, Keith Straggberg, "Network Security the Complete Reference", Tata McGraw Hill Publication,