R.T.M. Nagpur University, Nagpur
Four Year B.Tech. Course
(Revised curriculum as per AICTE Model Curriculum)
B.Tech. VII Semester (Computer Technology) Scheme

Cryptography and Network Security	
Total Credits: 4	Subject Code: BTCT701T
Teaching Scheme : Lectures: 3 Hours/Week Tutorials: 1 Hours/Week Practical: 2 Hours/Week	Examination Scheme : Duration of University Exam: 03 Hrs. College Assessment : 30 Marks University Assessment:70 Marks

Course Objectives :

1. To develop the student's ability to understand the concept of security goals in various applications and learn classical encryption techniques.
2. To apply fundamental knowledge on cryptographic mathematics used in various symmetric and asymmetric key cryptography.
3. To develop the student's ability to analyze the cryptographic algorithms.
4. To develop the student's ability to analyze the cryptographic algorithms.

Course Outcomes:

1. To understand basics of Cryptography and Network Security and classify the symmetric encryption techniques.
2. Understand, analyze and implement the symmetric key algorithm for secure transmission of data.
3. Acquire fundamental knowledge about the background of mathematics of asymmetric key cryptography and understand and analyze asymmetric key encryption algorithms and digital signatures.
4. Analyze the concept of message integrity and the algorithms for checking the integrity of data.
5. To understand various protocols for network security to protect against the threats in the networks.

Unit I **(08 Hrs)**

Introduction : Attributes of security, OSI Security Architecture**,** Model for network security. Mathematics of cryptography: modular arithmetic, Euclidean and extended Euclidean algorithm. Classical encryption techniques: substitution techniques-Caesar cipher, Vigenère's ciphers, Hill ciphers, Playfair ciphers and transposition techniques.

Unit II **(07 Hrs)**

Symmetric key cryptography: Block Cipher Principles, Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES), RC4, Key Distribution.

Unit III **(07 Hrs)**

Asymmetric key cryptography: Euler's Totient Function, Fermat's and Euler's Theorem, Chinese Remainder Theorem, RSA, Diffie Hellman Key Exchange, ECC, Entity authentication: Digital signature.

Unit IV **(07 Hrs)**

Message Integrity and authentication: Authentication Requirements and Functions, Hash Functions, MD5, Kerberos, Key Management, X.509 Digital Certificate format.

Unit V **(07 Hrs)**

Network Security: PGP, SSL, Firewalls, IDS, Software Vulnerability: Phishing, Buffer Overflow, SQL Injection, Electronic Payment Types,

Text Books:

1. William Stallings, “Cryptography and Network Security: Principles and Standards”, Prentice Hall India, 7th Edition, 2017.
2. Bernard Menezes, “Network Security and Cryptography”, Cengage Learning, 2010.

References:

1. Nina Godbole, “Information System Security”, Wiley India Publication, 2008.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network security, private communication in a public world", Second Edition, Prentice Hall, 2002.
3. Christopher M. King, Curtis Patton and RSA press, "Security architecture, Design Deployment and Operations", McGraw Hill Publication, 2001.
4. Robert Bragge, Mark Rhodes, Heithstraggberg "Network Security, The Complete Reference", Tata McGraw Hill Publication, 2004.
5. Behrouz A. Forouzan, “Cryptography and Network Security”, McGraw-Hill publication, 2nd Edition, 2010.

Cryptography and Network Security(PR)	
Total Credits: 1	Subject Code: BTCT701P
Teaching Scheme : Lectures: 0 Hours/Week Tutorials: 0 Hours/Week Practical: 2 Hours/Week	Examination Scheme : Duration of University Exam: College Assessment : 25 Marks University Assessment: 25 Marks

Minimum ten experiments should be conducted based on the Theory Syllabus.