Second Year B.C.A. (Science) Semester IV

(To be implemented from Academic year 2017-18)

Course Code: BCA 403 Course Name: Advanced Networking and Network Security

Total Contact Hours: 48hrs. Total Credits: 04

Total Marks: 100 Teaching Scheme: Theory- 05 Lect./Week

Unit No.	Contents	No. of Lectures
1	**Transport Layer** 1.1. Process-to-Process Delivery Client Server Paradigm, Multiplexing and De-multiplexing, Connectionless Vs Connection-Oriented Service, Reliable Vs Unreliable 1.2. User Datagram Protocol(UDP) Datagram Format, Checksum, UDP operations, Use of UDP 1.3. Transmission Control Protocol (TCP) TCP Services –Process to-Process Communication, Stream Delivery Service, sending andReceivingBuffers,Segments,Full–Duplex Communication, Connection oriented service, Reliable service 1.4. TCP Features –Numbering System, Byte Number, Sequence Number, Acknowledgement Number, Flow Control, Error Control, Congestion Control 1.5. TCP Segment Format	8
2	**Computer Security** 2.1. Introduction 2.2. Need for security 2.3. Principles of Security 2.4. Types of Attacks 2.5. Cryptography 2.6. Plaintext and Cipher Text 2.7. Substitution techniques 2.8. Caesar Cipher 2.9. Mono-alphabetic Cipher 2.10. Polygram, Poly alphabetic Substitution 2.11. Play fair 2.12. Hill Cipher 2.13. Transposition techniques, 2.14. Encryption and Decryption, 2.15. Symmetric and Asymmetric Key Cryptography 2.16. Steganography	10

	2.17. Key Range and Key Size 2.18. Possible Types of Attacks ,Attacks on cipher text	
3	**Symmetric Key Algorithm** 3.1. Algorithms 3.2. Types and modes 3.3. Overview of Symmetric key Cryptography 3.4. Data Encryption Standard (DES),Types of DES 3.5. Diffie Helman Key Exchange Algorithm	8
4	**Asymmetric Key Algorithm** 4.1. Brief history of Asymmetric Key Cryptography 4.2. Overview of Asymmetric Key Cryptography 4.3. RSA algorithm 4.4. Symmetric and Asymmetric key cryptography 4.5. Digital Signature 4.6. Message Digest and its uses 4.7. Problems with the public key exchange	12
5	**Internet Security Protocols** 5.1 Digital Certificates 5.2 Basic concepts of Internal security 5.3 Secure Socket Layer (SSL) 5.4 Transport Layer Security (TLS) 5.5 Secure Hyper Text Transfer Protocol (SHTTP) 5.6 Time Stamping Protocol (TSP)	6
6	**Network Security Firewalls and Virtual Private Networks** 6.1. Brief Introduction to Firewalls, IP Security, Virtual Private Networks (VPN) 6.2. Intrusion 6.3. User Authentication: 6.3.1 Authentication basics 6.3.2 Passwords, Authentication, Tokens 6.3.3 Biometric Authentication 6.3.4 Image-Base Authentication	12

Reference Books:-

1. Cryptography and Network Security by Atul Kahate, 3rd Edition, Tata McGraw Hill
2. Cryptography and Network Security by William Stallings, Fifth Edition, Pearson Education.
3. Cryptography: Theory and Practice by Douglas Stinson, CRC Press, CRC Press LLC.