

SARDAR PATEL UNIVERSITY
Programme: B.Sc (Information Technology)
Semester: VI
Syllabus with effect from: November - 2013

Paper Code: US06CINT05	Total Credit: 3
Title of Paper: Information Security	

Unit	Description in detail	Weightage (%)
I	Introduction of Security & Cryptography Attacks, services and mechanism. Security attacks. Security services. A model for network security. Introduction of Cryptography Conventional encryption principles. Basic terms : plaintext, ciphertext, cryptography, cryptanalysis. Substitution Ciphers. Transposition Ciphers. Quantum Cryptography. Fundamental Cryptographic Principles.	25%
II	Symmetric–Key Algorithms & System Security Introduction to DES – Data Encryption Standard. Introduction to AES – Advanced Encryption Standard. Cipher Modes. Crypto analysis. Substitution ciphers vs. transposition ciphers. Types of attack on encrypted messages. Introduction to public key cryptography. Applications for public-key cryptosystems. Intruders. Viruses and related threats : trap doors, logic bombs, trojan horses, viruses, worms, bacteria. The nature of viruses. Types of viruses. Antivirus approaches : detection, identification and removal.	25%
III	Network Security Security Services. Message Confidentiality. Message Integrity. Message Authentication. Digital Signature. Entity Authentication. Key Management.	25%
IV	Security in the Internet Firewalls : introduction, design principles, characteristics, types, configuration. IP Security. Secure Sockets Layer (SSL). Transport Layer Security (TLS). Pretty Good Privacy (PGP).	25%



Basic Text & Reference Books:

- William Stallings : Network Security Essentials (Applications and Standards), Pearson Education India, Third Edition
- Data Communications and Networking by Behrouz A. Forouzan

