RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

Computer Science and Engineering, VII-Semester

Open Elective – CS703 (A) Cryptography & Information Security

COURSE OUTCOMES:

CO1: Understanding of the basics of Cryptography and Network Security and working knowledge of Mathematics used in Cryptology.
CO2: Understanding of previous attacks on cryptosystems to prevent future attacks from securing a message over an insecure channel by various means.
CO3: Knowledge about how to maintain the Confidentiality, Integrity and Availability of a data.
CO4: Understanding of various protocols for network security to protect against the network threats.
CO5: Getting hands-on experience of various Information Security Tools.

UNIT I:

Mathematical Background for Cryptography: Abstract Algebra, Number Theory, Modular Inverse, Extended Euclid Algorithm, Fermat's Little Theorem, Euler Phi-Function, Euler's theorem.
Introduction to Cryptography: Principles of Cryptography, Classical Cryptosystem, Cryptanalysis on Substitution Cipher (Frequency Analysis), Play Fair Cipher, Block Cipher. Data Encryption Standard (DES), Triple DES, Modes of Operation, Stream Cipher.

UNIT II:

Advanced Encryption Standard (AES), Introduction to Public Key Cryptosystem, Discrete Logarithmic Problem, Diffie-Hellman Key Exchange Computational & Decisional Diffie-Hellman Problem, RSA Assumptions & Cryptosystem,RSA Signatures & Schnorr Identification Schemes, Primarily Testing, Elliptic Curve over the Reals, Elliptic curve Modulo a Prime., Chinese Remainder Theorem.

UNIT III:

Message Authentication, Digital Signature, Key Management, Key Exchange, Hash Function. Universal Hashing, Cryptographic Hash Function, MD, Secure Hash Algorithm (SHA), Digital Signature Standard (DSS), Cryptanalysis: Time-Memory Trade-off Attack, Differential Cryptanalysis. Secure channel and authentication system like Kerberos.

UNIT IV:

Information Security: Threats in Networks, Network Security Controls–Architecture, Wireless Security, Honey pots, Traffic Flow Security, Firewalls – Design and Types of Firewalls, Personal Firewalls, IDS, **Email Security:** Services Security for Email Attacks Through Emails, Privacy-Authentication of Source Message, Pretty Good Privacy(PGP), S-MIME. **IP Security**: Overview of IPSec, IP& IP version 6 Authentication, Encapsulation Security Payload ESP, Internet Key Exchange IKE, **Web Security:** SSL/TLS, Basic protocols of security. Encoding –Secure Electronic Transaction SET.

UNIT V:Cryptography and Information Security Tools: Spoofing tools**:** like Arping etc., **Foot printing Tools** (ex-nslookup, dig, Whois,etc..), **Vulnerabilities Scanning Tools** (i.e. Angry IP, HPing2, IP Scanner, Global Network Inventory Scanner, Net Tools Suite Pack.), NetBIOS Enumeration Using NetView Tool, **Steganography** Merge Streams, Image Hide, Stealth Files, Blindsideusing:**STools, Steghide, Steganos**.Stegdetect, Steganalysis - Stego Watch- Stego Detection Tool, **StegSpy**.**Trojans Detection Tools**(i.e. Netstat, fPort, TCPView, CurrPorts Tool, Process Viewer), Lan Scanner Tools (i.e.look@LAN, Wireshark, Tcpdump). **DoS Attack Understanding Tools-** Jolt2, Bubonic.c, Land and LaTierra, Targa, Nemesy Blast, Panther2, Crazy Pinger, Some Trouble, UDP Flood, FSMax.

Recommended Text:

1. Cryptography and Network Security Principles and Practice Fourth Edition,William Stallings, Pearson Education.
2. Network Security Essentials: Applications and Standards, by William Stallings.Prentice Hall.
3. Behrouz A Ferouzan, “Cryptography and NetworkSecurity” Tata Mc Graw Hills, 2007
4. Charles PPfleeger, Shari Lawrence Pfleeger “Security in Computing”, 4th Edition Prentice Hall of India, 2006.
5. Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell, Chapman and Hall/CRC