

PEOPLE'S UNIVERSITY, BHOPAL

PROGRAMME: M Tech (Cyber Security)

SEM: II


Subject Title	Subject Code
Computer Forensics Science	MTCY 201

Unit	Contents (Theory)
I	Basics of Cyber forensics: need, illegal activities, principles of cyber forensics, Cyber crimes, where and when is it used, Cyber Law: Introduction, need, IT ACT, 2000, digital signatures, E-Governance, IT act-2008, Legal Perspective: searching for and seizing information's, introduction, information as contraband, instrumentally, information as evidence, privilege confidential information, searching for information
II	Digital Evidences: Introduction, Digital Evidence, Types of Digital Evidence, What is Digital Forensics. How to Identify Digital Evidence, How to treat digital evidences, Software Tools Data Imaging and Imaging Forensics: Imaging, Image Analysis, Image Running Tools, Restore Access to EFS-Encrypted Files
III	Recovering of Deleted Files and deleted partitions: Recycle Bin, Recover deleted files in Windows XP or Vista, Recovering deleted files from Deleted Partition, Introduction to mobile and PDA forensics, Forensic Tools, Handset Tools, PDA Forensic, FORENSICS with PDA, Password Cracking, Brute Force Intrusion, Dictionary intrusion, RAR Password Crackers, Password Guessing, CMOS Level Password Cracking, PDF Password Crackers, Password Cracking Tools, Common Recommendations for Improving Password Security, Standard Password Advice.
IV	Network Intrusions Investigation: Sniffer, Network Addressing Schemes, Tool: TCPDump, Network Sniffer, HTTP Sniffer, Ether Detect Packet Sniffer, Ethereal, Honey Pot Log, Honey Net Log, Web Application Intrusions Investigation, Vulnerability of web services, Vulnerabilities, Web Application Intrusions ,SQL Injection Intrusion, Price Manipulation, Cross-Site Scripting, Other Web Application Intrusion, Web Application Forensic, Tools,
V	Trademark and Copyright Infringement Issue: Introduction, Trademark, Copyright, Patent, Copyright Infringement, Report Generation, Importance of reports, REPORT PREPARATION, Stages of Report Preparation, Gathering the Data, Analyzing and Sorting the Results, Outlining the Report, Case Studies and references

References:

1. Jerry Hatchett, Computer Forensics: A Real World Guide, Jul 2009, Auerbach Publications.
2. John R. Vacca, Computer Forensics: Computer Crime Scene Investigation, 2009, Firewall.
3. Inda Volonino, Reynaldo Anzaldua, Jana Godwin, Computer Forensics: Principles and Practices, Aug 2006, Prentice Hall
4. Irons, Andersen, Laing, Computer Forensics, CI Emea Higher Education Warren G. Kruse, Jay G. Heiser, Computer Forensics: Incident Response Essentials, Sep 2001, Addison-wesley Professional.


CHAIRMAN


Registrar
People's University
Bhopal (M.P.)


DEAN
FACULTY OF ENGINEERING

PEOPLE'S UNIVERSITY, BHOPAL

PROGRAMME: M Tech (Cyber Security)

SEM:II

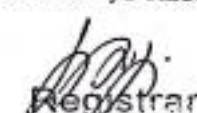
Subject Title	Subject Code
Mobile & wireless Security	MTCY 202

Unit	Contents (Theory)
I	Wireless Fundamentals: Wireless Hardware- Wireless Network Protocols- Wireless Programming WEP Security. Wireless Cellular Technologies – concepts – Wireless reality –Security essentials – Information classification standards - Wireless Threats: Cracking WEP -Hacking Techniques- Wireless Attacks – Airborne Viruses.
II	Standards and Policy Solutions – Network Solutions – Software Solutions – Physical Hardware Security- Wireless Security – Securing WLAN – Virtual Private Networks – Intrusion Detection System – Wireless Public Key infrastructure. Tools – Auditing tools – Pocket PC hacking –wireless hack walkthrough.
III	Security Principles – Authentication – Access control and Authorization – Non-repudiation privacy and Confidentiality – Integrity and Auditing –Security analysis process. Privacy in Wireless World – Legislation and Policy – Identify targets and roles analysis – Attacks and vulnerabilities – Analyze mitigations and protection.
IV	WLAN Configuration – IEEE 802.11 – Physical layer – media access frame format – systematic exploitation of 802.11b WLAN – WEP – WEP Decryption script – overview of WEP attack –Implementation - Analyses of WEP attacks.
V	Global Mobile Satellite Systems: case studies of the IRIDIUM and GLOBALSTAR systems. Wireless Enterprise Networks: Introduction to Virtual Networks, Blue tooth technology, Blue tooth Protocols. Server-side programming in Java, Pervasive web application architecture, Device independent example application

References:

1. Russel Dean Vines, "Wireless Security Essentials: Defending Mobile from Data Piracy", John Wiley & Sons, 1st Edition, 2002.
2. Cyrus, Peikari and Seth Fogie, "Maximum Wireless Security", SAMS Publishing 2002.
3. Yi-Bing Lin and Imrich Chlamtac, "Wireless and Mobile Networks Architectures", John Wiley & Sons, 2001.
4. Raj Pandya, "Mobile and Personal Communication systems and services", Prentice Hall of India, 2001.
5. Tara M. Swaminathan and Charles R. Eldon, "Wireless Security and Privacy- Best Practices and Design Techniques", Addison Wesley, 2002.
6. Bruce Potter and Bob Fleck, "802.11 Security", O'Reilly Publications, 2002.
7. Burkhardt, "Pervasive Computing", Pearson Education, India Edition, 2007.
8. J. Schiller, "Mobile Communication", Pearson Education, India Edition, 2002.


CHAIRMAN


Registrar
People's University
Bhopal (M.P.)


DEAN

FACULTY OF ENGINEERING

PEOPLE'S UNIVERSITY, BHOPAL

PROGRAMME: M Tech (Cyber Security)

SEM: II

Subject Title	Subject Code
Network Security	MTCY 203

Unit	Contents (Theory)
I	Introduction: The Security, functionality and ease of use Triangle, Essential Terminology, Elements of Security, Difference between Penetration Testing and Ethical Hacking, Deliverables ethics and legality, Computer Crimes and Implications.
II	Reconnaissance: Information Gathering Methodology, Locate the Network Range, Active and Passive reconnaissance. Scanning: Scanning, Elaboration phase, active scanning, scanning tools nmap, hping2. Enumeration, DNS Zone transfer.
III	Trojans and Backdoors: Effect on Business, Trojan?, Overt and Covert Channels, Working of Trojans, Different Types of Trojans, Different ways a Trojan can get into a system, Indications of a Trojan Attack, Some famous Trojans and ports used by them. Sniffers: Definition of sniffing, How a Sniffer works?, Passive Sniffing, Active Sniffing, Ethrealttool, Man-in-the-Middle Attacks, Spoofing and Sniffing Attacks, ARP Poisoning and countermeasures.
IV	Denial of Service: What is Denial of Service? , Goal of DoS (Denial of Service), Impact and Modes of Attack. Session Hijacking: Understanding Session Hijacking, Spoofing vs Hijacking, Steps in Session Hijacking, Types of Session Hijacking, TCP Concepts 3 Way and shake, Sequence numbers.
V	Network Security and Technologies and Protocols – AAA Protocols – Tunneling Protocols – Secured Routing Protocols – GRE- Generic Routing Encapsulation – IPSEC – Security architecture for IP – IPSECAH – Authentication Header – ESP – IKE – ISAKMP and Key management Protocol. IEEE 802.11 - Structure of 802.11 MAC – WEP- Problems with WEP – Attacks and Risk- Station security – Access point Security – Gate way Security – Authentication and Encryption

References:

1. William Stallings, "Cryptography and Network Security", Second edition, Prentice Hall, 1999.
2. Atul Kahate, "Cryptography and Network Security," TMH
3. William Stallings, "Cryptography and Network Security", Third Edition, Pearson Ed 4. Introduction to network security, Krawetz, Cengage
4. Behrouz A. Frouzan: Cryptography and Network Security, TMH
5. I. Jawin, "Networks Protocols Handbook", Jawin Technologies Inc., 2005


Registrar
People's University
Bhopal (M.P.)


DEAN

FACULTY OF ENGINEERING
PEOPLE'S UNIVERSITY, BHOPAL


CHAIRMAN

BOARD OF STUDIES (ENGINEERING)
PEOPLE'S UNIVERSITY, BHOPAL

PEOPLE'S UNIVERSITY, BHOPAL

PROGRAMME: M Tech (Cyber Security)

SEM: II

Subject Title	Subject Code
Applied Cryptography	MTCY 204


Unit	Contents (Theory)
I	Foundations – Protocol Building Blocks - Basic Protocols - Intermediate Protocols – Advanced Protocols - Zero-Knowledge Proofs - Zero-Knowledge Proofs of Identity - Blind Signatures - Identity-Based Public-Key Cryptography - Oblivious Transfer - Oblivious Signatures – Esoteric Protocols
II	Key Length - Key Management - Electronic Codebook Mode - Block Replay - Cipher Block Chaining Mode - Stream Ciphers - Self-Synchronizing Stream Ciphers - Cipher-Feedback Mode - Synchronous Stream Ciphers - Output-Feedback Mode - Counter Mode - Choosing a Cipher Mode - Interleaving - Block Ciphers versus Stream Ciphers - Choosing an Algorithm - Public- Key Cryptography versus Symmetric Cryptography - Encrypting Communications Channels - Encrypting Data for Storage - Hardware Encryption versus Software Encryption Compression, Encoding, and Encryption - Detecting Encryption – Hiding and Destroying Information.
III	Information Theory - Complexity Theory - Number Theory - Factoring - Prime Number Generation - Discrete Logarithms in a Finite Field - Data Encryption Standard (DES) – Lucifer - Madryga - NewDES - GOST – 3 Way – Crab – RC5 - Double Encryption - Triple Encryption - CDMF Key Shortening - Whitening.
IV	Pseudo-Random-Sequence Generators and Stream Ciphers – RC4 - SEAL - Feedback with Carry Shift Registers - Stream Ciphers Using FCSRs - Nonlinear-Feedback Shift Registers - System-Theoretic Approach to Stream-Cipher Design - Complexity-Theoretic Approach to Stream-Cipher Design - N- Hash - MD4 - MD5 - MD2 - Secure Hash Algorithm (SHA) - One- Way Hash Functions Using Symmetric Block Algorithms - Using Public-Key Algorithms - Message Authentication Codes
V	RSA - Pohlig-Hellman - McEliece - Elliptic Curve Cryptosystems -Digital Signature Algorithm (DSA) - Gost Digital Signature Algorithm - Discrete Logarithm Signature Schemes - Ongchnorr- Shamir -Cellular Automata - Feige-Fiat-Shamir -Guillou-Quisquater - Diffie-Hellman - Station-to-Station Protocol -Shamir's Three-Pass Protocol - IBM Secret-Key Management Protocol - MITRENET - Kerberos - IBM Common Cryptographic Architecture.

References:

1. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C"
2. John Wiley & Sons, Inc, 2nd Edition, 1996.
3. Wenbo Mao, "Modern Cryptography Theory and Practice", Pearson Education, 2004
4. Atul Kahate, "Cryptography and Network Security", Tata McGraw Hill, 2003.
5. William Stallings, "Cryptography and Network Security", 3rd Edition, Pearson education, 2003



CHAIRMAN



Registrar
People's University
Bhopal (M.P.)



DEAN

FACULTY OF ENGINEERING

PEOPLE'S UNIVERSITY, BHOPAL

PEOPLE'S UNIVERSITY, BHOPAL

PROGRAMME: M Tech (Cyber Security)

SEM: II

Subject Title	Subject Code
Information Security & quality assurance	MTCY 205


Unit	Contents (Theory)
I	Introduction: IT security and intrusion Combo, Essential Terminologies, Security and its need, Aspects of Security, need for enhanced security, Information Security & Law, IPR, Patent Law, Copyright Law, Legal Issues in Data mining Security, Building Security into Software Life Cycle
II	Why IT is security Necessary: IT security services life cycle, Operating system basics, objectives of operating system, Services provided by operating systems.
III	Data communication Basics: Networking basics, Data communication, OSI/ TCP models, Cyber Threats and Issues
IV	An approach towards intrusion: Intrusion basics, Intrusion methodology, types of intruders, challenges. Protecting your computer: Physical security, Laptop, Desktop, network components, Software security, Protecting against Intruders, viruses, spywares, unwanted e-mails,
V	Software security for portable computers: Social engineering, defending against social engineers, Phishers, Protecting Password, logging on safely and securely, tips for creating secure password, keeping password secure, selecting tools, safety rules. Case studies: Hack reports-2000, Reports-2005 to 2009, Picture into intrusion and cyber crimes-2009-2010, CERT-IN reports, security tools

References:

1. Randy Weaver, "Network Infrastructure Security", Cengage Learning
2. Merkov, Breithaupt, "Information Security", Pearson Education
3. Yadav, "Foundations of Information Technology", New Age, Delhi
4. Andrew S. Tanenbaum "Computer Networks", 4th Edition, Pearson Education, 2008
5. Behrouz A. Forouzan, "TCP/IP Protocol Suit", TMH, 2000.


CHAIRMAN

(ENGINEERING)


Registrar
People's University
Bhopal (M.P.)


DEAN

FACULTY OF ENGINEERING
PEOPLE'S UNIVERSITY, BHOPAL

PEOPLE'S UNIVERSITY, BHOPAL

Subject Title	Subject Code
LAB-III	MTCY 206

Set-1

1. Study of Cyber Forensics and Cyber Crime
2. Study of E-Governance
3. Study of Digit evidence
4. Study of restore and access to EFS-Encrypted files
5. Study of Password cracking tools
6. Study of Forensic Tools
7. Study of Network Sniffer and Intrusion detection system
8. Study of Trademark and copyright infringement
9. Study of Network addressing schemes
10. Study of cross site scripting

Set-2

1. To study the wireless hardware and protocol
2. To Study the wireless attack
3. To Study the process for for setup of basic WLAN
4. To study for installing the client adapter in the PC for wireless networking
5. To Study the virtual Private Network for WLAN
6. To Study the Intrusion detection system In Wireless Netowrk
7. To Implement wired network topology and wirelss network topology in ns2
8. To connect the computer WLAN
9. To Study the function of Wireless Network
10. To Study of IRIDIUM and GLOBALSTAR

References:

1. Jerry Hatchett, Computer Forensics: A Real World Guide, Jul 2009, Auerbach Publications.
2. John R. Vacca, Computer Forensics: Computer Crime Scene Investigation, 2009, Firewall.
3. inda Volonino, Reynaldo Anzaldua, Jana Godwin, Computer Forensics: Principles and Practices, Aug 2006, Prentice Hall
4. Russel Dean Vines, "Wireless Security Essentials: Defending Mobile from Data Piracy", John Wiley & Sons, 1st Edition, 2002.
5. Cyrus, Peikari and Seth Fogie, "Maximum Wireless Security", SAMS Publishing 2002.
6. Yi-Bing Lin and Imrich Chlamtac, "Wireless and Mobile Networks Architectures", JohnWiley & Sons, 2001.


CHAIRMAN

BOARD OF STUDIES (ENGINEERING)
PEOPLE'S UNIVERSITY, BHOPAL


Registrar
People's University
Bhopal (M.P.)


DEAN

FACULTY OF ENGINEERING
PEOPLE'S UNIVERSITY, BHOPAL

PEOPLE'S UNIVERSITY, BHOPAL

Subject Title	Subject Code
LAB-IV	MTCY 207

Set-1

1. Understanding DoS Attack Tools- Jolt2 , Bubonic
2. To Study of Scanning for vulnerabilities using Global Network Inventory Scanner, Net Tools Suite Pack
3. How to Detect Trojans by using – Netstat, fPort, TCPView
4. To Study of Session Hijacking
5. To Study AAA Protocol
6. To Study of IEEE 802.11
7. To Study Study of MAC Protocol
8. To Study of Sniffers and their working process
9. To Study Security architecture for IP
10. To Study of Lan Scanner using look@LAN, wireshark

Set-2


1. Write program for Mono alphabetic cipher
2. Implementation of Play Fair cipher
3. Implementation of Vigenere cipher (Polyalphabetic substitution)
4. Implement RSA asymmetric (public key and private key)-Encryption. Encryption key (e, n) & (d, n)
5. Generate digital signature using Hash code
6. Study of MD5 hash function and implement the hash code using MD5
7. Study of SHA-1 hash function and implement the hash code using SHA-1
8. Generate digital signature using MAC code
9. Program to implement Deffi-Hellman Algorithm
10. Study of KERBEROS, PGP, SSH, SRP, OPIE

References:

1. William Stallings, "Cryptography and Network Security", Second edition, Prentice Hall, 1999.
2. Atul Kahate, "Cryptography and Network Security," TMH
3. William Stallings, "Cryptography and Network Security", Third Edition, Pearson Ed 4. Introduction to network security, Krawetz, Cengage
4. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C"
5. John Wiley & Sons, Inc, 2nd Edition, 1996.
6. Wenbo Mao, "Modern Cryptography Theory and Practice", Pearson Education, 2004
7. Atul Kahate, "Cryptography and Network Security", Tata McGraw Hill, 2003.
8. William Stallings, "Cryptography and Network Security", 3rd Edition, Pearson education, 2003


CHAIRMAN

BOARD OF STUDIES (ENGINEERING)


Registrar
People's University
Bhopal (M.P.)


DEAN

FACULTY OF ENGINEERING