Maharshi Dayanand University, Rohtak

SCHEME OF STUDIES AND EXAMINATIONS

FOR

MASTER OF TECHNOLOGY

IN

CYBER FORENSICS AND INFORMATION SECURITY

W.E.F. SESSION 2013-14

Maharshi Dayanand University, Rohtak

SCHEME OF STUDIES & EXAMINATION

MASTER OF TECHNOLOGY

(CYBER FORENSICS AND INFORMATION SECURITY)

SEMESTER-I

EFFECTIVE FROM 2013-14

Course No.	Course Title	Teaching Schedule			Marks		Total	Duration of Exam (Hrs)
		L	T	P	Sessional	Exam.		
MTCF 101	Mathematical Foundations of Information Security	4	-	-	50	100	150	3
MTCF 102	Networks and Information Security	4	-	-	50	100	150	3
MTCF 103	Operating Systems and Security	4	-	-	50	100	150	3
MTCF 104	Cyber Forensics	4	-	-	50	100	150	3
	Elective-I	4	-	-	50	100	150	3
MTCF 109	Information Security Lab	-	-	3	50	50	100	3
MTCF 110	OS Security Lab	-	-	3	50	50	100	3
TOTAL		20	-	6	350	600	950	

Elective- I

MTCF 105 – Advanced Computer Networks
MTCF 106 - Professional Ethics and Cyber Security
MTCF 107 – Security Threats
MTCF 108 - Information Theory and Coding

Maharshi Dayanand University, Rohtak

SCHEME OF STUDIES & EXAMINATION

MASTER OF TECHNOLOGY

(CYBER FORENSICS AND INFORMATION SECURITY)

SEMESTER-II

EFFECTIVE FROM 2013-14

Course No.	Course Title	Teaching Schedule			Marks		Total	Duration of Exam (Hrs)
		L	T	P	Sessional	Exam.		
MTCF 201	Ethical Hacking and Digital Forensics	4	-	-	50	100	150	3
MTCF 202	Database Security	4	-	-	50	100	150	3
MTCF 203	Steganography and Digital Watermarking	4	-	-	50	100	150	3
MTCF 204	Mobile & Wireless Security	4	-	-	50	100	150	3
	Elective-II	4	-	-	50	100	150	3
MTCF 209	Ethical Hacking Lab	-	-	3	50	50	100	3
MTCF 210	Steganography Lab	-	-	3	50	50	100	3
TOTAL		20	-	6	350	600	950	

Elective- II

MTCF 205- Security Threats & Vulnerabilities

MTCF 206 -Information Security, Management & Standards

MTCF 207- Multimedia Security

MTCF 208- Computer Security, Audit Assurance and Risk Management

Maharshi Dayanand University, Rohtak

SCHEME OF STUDIES & EXAMINATION

MASTER OF TECHNOLOGY

(CYBER FORENSICS AND INFORMATION SECURITY)

SEMESTER-III

EFFECTIVE FROM 2013-14

Course No.	Course Title	Teaching Schedule			Marks		Total	Duration of Exam (Hrs)
		L	T	P	Sessional	Exam.		
MTCF 301	Preserving & Recovering Digital Evidence	4	-	-	50	100	150	3
MTCF 302	Cyber Laws & Security Policy	4	-	-	50	100	150	3
	Elective-III	4	-	-	50	100	150	3
MTCF 307	Dissertation Phase 1	-	-	8	100	-	100	3
MTCF 308	Seminar & Technical Writing	-	-	2	50	-	50	-
TOTAL		12	-	10	300	300	600	

Elective- III

MTCF 303- Biometric Security
MTCF 304- Applied Cryptography
MTCF 305- Distributed Systems Security
MTCF 306- Secure Software Engineering

Maharshi Dayanand University, Rohtak

SCHEME OF STUDIES & EXAMINATION

MASTER OF TECHNOLOGY

(CYBER FORENSICS AND INFORMATION SECURITY)

SEMESTER-IV

EFFECTIVE FROM 2013-14

Course No.	Course Title	Teaching Schedule			Marks		Total
		L	T	P	Sessional	Exam.	
MTCF 401	Dissertation Phase- II	-	-	24	200	400	600
	Total		-	24	200	400	600

FIRST SEMESTER

MTCF -101 Mathematical Foundations of Information Security

L- T- P	Exams Marks	: 100
4- 0- 0	Sessional Marks	: 50
	Total Marks	: 150
	Duration of Exam	: 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section-A

Topics in elementary number theory: O and notations – time estimates for doing arithmetic – divisibility and the Euclidean algorithm – Congruences: Definitions and properties – linear congruences, residue classes, Euler's phi function – Fermat's Little Theorem – Chinese Remainder Theorem – Applications to factoring – finite fields – quadratic residues and reciprocity: Quadratic residues – Legendre symbol – Jacobi symbol.

Section-B

Simple Cryptosystems: Enciphering Matrices – Encryption Schemes – Symmetric and Asymmetric Cryptosystems – Cryptanalysis – Block ciphers –Use of Block Ciphers – Multiple Encryption – Stream Ciphers –Affine cipher – Vigenere, Hill, and Permutation Cipher – Secure Cryptosystem.

Section-C

Public Key Cryptosystems: The idea of public key cryptography – The Diffie–Hellman Key Agreement Protocol - RSA Cryptosystem – Bit security of RSA – ElGamal Encryption - Discrete Logarithm – Knapsack problem – Zero-Knowledge Protocols – From Cryptography to Communication Security - Oblivious Transfer.

Section-D

Primality and Factoring: Pseudo primes – the rho (γ) method – Format factorization and factor bases – the continued fraction method – the quadratic seieve method. Number Theory and Algebraic Geometry: Elliptic curves – basic facts – elliptic curve cryptosystems – elliptic curve primality test – elliptic curve factorization.

REFERENCES

1. Victor Shoup, "A Computational Introduction to Number Theory and Algebra", Cambridge University Press, 2005.

2. A. Manezes, P. Van Oorschot and S. Vanstone, "Hand Book of Applied Cryptography", CRC Press, 1996

3. Serge Vaudenay, “Classical Introduction to Cryptography – Applications for Communication Security”, Springer, 2006.
4. Neal Koblitz, “A Course in Number Theory and Cryptography”, 2nd Edition, Springer, 2002.
5. Johannes A. Buchman, “Introduction to Cryptography”, 2nd Edition, Springer, 2004.
6. S.C. Coutinho, “The Mathematics of Ciphers – Number Theory and RSA Cryptography”, A.K. Peters, Natick, Massachusetts, 1998.

MTCF -102 Networks and Information Security

L- T- P	Exams Marks	: 100
4- 0- 0	Sessional Marks	: 50
	Total Marks	: 150
	Duration of Exam	: 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section-A

Introduction-Characteristics of Networks, Security Concepts,–Kinds of security breaches – Threats and Risks, Points of vulnerability, Attacks – Passive and Active, Security Services, Confidentiality, Authentication, Non-Repudiation, Integrity, Access Control, Availability, – Methods of defense – Control measures – Effectiveness of controls, Model for Internetwork Security, Internet Standards and RFCs Access Control Mechanisms ,Access Matrix, HRU, TAM, ACL and capabilities

Section-B

Access Control Models, Chinese Wall, Clark-Wilson, Bell-LaPadula, Non Interference and Role Base Model. Cryptography, Encryption techniques – Characteristics of good encryption systems – Secret Key and Public Key Cryptosystems, Symmetric Ciphers, Block Ciphers and Stream Ciphers, DES, IDEA and Key Escrow, RSA and ElGamal, Secure Hash and Key management, Non-repudiation, cryptanalysis.

Section-C

Secure sockets – IPSec overview – IP security architecture – IPSec-Internet Key Exchanging(IKE) – IKE phases – encoding – Internet security – Threats to privacy – Packet sniffing – Spoofing - Web security requirements – Real Time communication security – Security standards–Kerberos.X.509 Authentication Service.

Security protocols – Transport layer protocols – SSL – Electronic mail security – PEM and S/MIME security protocol – Pretty Good Privacy – Web Security - Firewalls design principles – Trusted systems – Electronic payment protocols. Intrusion detection – password management – Viruses and related Threats – Virus Counter measures, Virtual Private Networks.

Section-D

Network Security Applications, Authentication Mechanisms: Passwords, Cryptographic authentication protocol, Smart Card, Biometrics, Digital Signatures and seals, Kerberos, X.509 LDAP Directory. Web Security: SSL Encryption, TLS, SET

E-mail Security, Pretty Good Privacy (PGPs) / MIME, IP Security, Access and System Security, Intruders, Intrusion Detection and Prevention, Firewall, Hardware Firewall, Software Firewall,

Application Firewall, Packet Filtering. , Packet Analysis, Proxy Servers, Firewall setting in Proxy, ACL in Proxy.

References:

1 William Stallings, "Network Security Essentials", 3rd Edition, Pearson Education, 2006
2 Edward Amoroso, "Fundamentals of Computer Security Technology", Prentice-Hall, 1999
3 Charles P. Pleeger, “Security in Computing”, Pearson Education, 5th Edition, 2001.
4 William Stallings, “Cryptography and Network Security: Principles and Standards”, Prentice Hall India, 3rd Edition, 2003.

MTCF -103 Operating Systems and Security

L- T- P	Exams Marks	: 100
4- 0- 0	Sessional Marks	: 50
	Total Marks	: 150
	Duration of Exam	: 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section-A

INTRODUCTION: Operating Systems Concepts – System Calls – OS Organization – Factors in OS Design – Basic Implementation Considerations – Time Sharing and Multi Programming – Real Time Systems. Process Management: Process Concepts, Model – Process Synchronization – Process Scheduling, Threads. Dead Lock: Detection & Recovery, Avoidance, Prevention- Two Phase Locking Issues.

Section-B

Memory Management: Basic Memory Management – Swapping – Virtual Memory – Page Replacement Algorithms-Segmentation. File System And I/O Management: Files – Low Level File Implementations – Memory Mapped Files – Directories, Implementation – Principles of I/O Hardware & Software – Device Drivers – Disks Hardware, Formatting & Arm Scheduling Algorithms.

Section-C

Windows Management Mechanisms - The registry, Registry usage, Registry data types, Local structure, Trouble shooting Registry problems, Registry Internals, Services, Applications, Accounts, Service control Manager, Windows Management Instrumentation, Processes, Threads, and Jobs: Process Internals, Flow of create process, Thread Internals, Examining Thread creation, Thread Scheduling, Job Objects.

Section-D

Secure Operating Systems: Access control and file system security. Remote file system security. NFS, SMB, SFS, User authentication, Passwords, Biometrics, Smartcards. Intrusion Detection And Virus Protection: Trusted Computing, TCPA and NGSCB, Digital Rights Management.

References:

1. Andrew S.Tanenbaum, “Modern Operating Systems”, 2nd edition, Addison Wesley, 2001.
2. Gary Nutt, “Operating Systems A Modern Perspective “, 2nd edition, Pearson Education, 2001.
3. Maurice J. Bach, “The Design of the Unix Operating System”, Prentice Hall of India, 1991.

4. Mark E. Russinovich and David A. Solomon, “Microsoft® Windows® Internals”, 4th Edition, Microsoft Press, 2004.
5. William Stallings, “Operating Systems: Internals and Design Principles”, 5th Edition, Prentice Hall, 2005

MTCF -104 Cyber Forensics

L- T- P	Exams Marks	: 100
4- 0- 0	Sessional Marks	: 50
	Total Marks	: 150
	Duration of Exam	: 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section-A

Introduction to Cyber forensics: Information Security Investigations, Corporate Cyber Forensics, Scientific method in forensic analysis, investigating large scale Data breach cases. Analyzing Malicious software.

Types of Computer Forensics Technology, Types of Military Computer Forensic Technology, Types of Law Enforcement: Computer Forensic Technology, Types of Business Computer Forensic Technology, Specialized Forensics Techniques, Hidden Data and How to Find It, Spyware and Adware, Encryption Methods and Vulnerabilities, Protecting Data from Being Compromised Internet Tracing Methods, Security and Wireless Technologies, Avoiding Pitfalls with Firewalls Biometric Security Systems

Section-B

Types of Computer Forensics Systems: Internet Security Systems, Intrusion Detection Systems, Firewall Security Systems, Storage Area Network Security Systems, Network Disaster Recovery Systems, Public Key Infrastructure Systems, Wireless Network Security Systems, Satellite Encryption Security Systems, Instant Messaging (IM) Security Systems, Net Privacy Systems, Identity Management Security Systems, Identity Theft, Biometric Security Systems

Section-C

Ethical Hacking: Essential Terminology, Windows Hacking, Malware, Scanning, Cracking. Digital Evidence in Criminal Investigations: The Analog and Digital World, Training and Education in digital evidence, Evidence Collection and Data Seizure: Why Collect Evidence, Collection Options Obstacles, Types of Evidence, The Rules of Evidence, Volatile Evidence, General Procedure, Collection and Archiving, Methods of Collection, Artifacts, Collection Steps, Controlling Contamination: The Chain of Custody, Reconstructing the Attack, The digital crime scene, Investigating Cybercrime, Duties Support Functions and Competencies.

Section-D

Identification of Data: Timekeeping, Forensic Identification and Analysis of Technical Surveillance Devices, Reconstructing Past Events: How to Become a Digital Detective, Useable File Formats, Unusable File Formats, Converting Files, Investigating Network Intrusions and Cyber Crime, Network Forensics and Investigating logs, Investigating network Traffic, Investigating Web attacks, Router Forensics. Cyber forensics tools and case studies.

References:

1. John R. Vacca, Computer Forensics: Computer Crime Scene Investigation, 2nd Edition, Charles River Media, 2005
2. Christof Paar, Jan Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, 2nd Edition, Springer's, 2010
3. Ali Jahangiri, Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts, Ali Jahangiri, 2009
4. Computer Forensics: Investigating Network Intrusions and Cyber Crime (Ec-Council Press Series: Computer Forensics), 2010

MTCF -109 Information Security Lab

L-	T-	P
0-	0-	3

Exams Marks	: 50
Sessional Marks	: 50
Total Marks	: 100
Duration of Exam	: 3 hrs.

List of Experiments:

1. Working with Sniffers for monitoring network communication (Ethereal)
2. Understanding of cryptographic algorithms and implementation of the same in C or C++
3. Using open SSL for web server - browser communication
4. Using GNU PGP
5. Performance evaluation of various cryptographic algorithms
6. Using IP TABLES on Linux and setting the filtering rules
7. Configuring S/MIME for e-mail communication
8. Understanding the buffer overflow and format string attacks
9. Using NMAP for ports monitoring
10. Implementation of proxy based security protocols in C or C++ with features like confidentiality, integrity and authentication
11. Socket programming
12. Exposure to Client Server concept using tcp/ip, blowfish, Pretty Good Privacy.

MTCF -110 OS Security Lab

L-	T-	P
0-	0-	3

Exams Marks	: 50
Sessional Marks	: 50
Total Marks	: 100
Duration of Exam	: 3 hrs.

List of Experiments:

1. Write programs using the following system calls of UNIX operating system: fork, exec, getpid, exit, wait, close, stat, opendir, readdir
2. Write programs using the I/O system calls of UNIX operating system (open, read, write, etc)
3. Write C programs to simulate UNIX commands like ls, grep, etc.
4. Implement any file allocation technique (Linked, Indexed or Contiguous)
5. Implementation of Memory and Address Protection
6. Implementation of Access Control List
7. Setting of File Permissions and Protections.
8. Management of the users & the domain.
9. Setting up the local security policy.
10. Start and stop services from user window and command prompt.
11. Use of event viewer.
12. Use of the performance monitor.
13. Management of the IIS and FTP server.

ELECTIVE-I

MTCF -105 Advanced Computer Networks

L- T- P	Exams Marks	: 100
4- 0- 0	Sessional Marks	: 50
	Total Marks	: 150
	Duration of Exam	: 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section-A

Foundation of Networking Protocols: 5-layer TCP/IP Model, 7-layer OSI Model, Internet Protocols and Addressing, Equal-Sized Packets Model: ATM -Networking Devices: Multiplexers, Modems and Internet Access Devices, Switching and Routing Devices, Router Structure.

The Link Layer and Local Area Networks: Link Layer: Introduction and Services, Error-Detection and Error-Correction techniques,- Multiple Access Protocols, Link Layer Addressing, Ethernet, Interconnections: Hubs and Switches, PPP: The Point-lo-Point Protocol, Link Visualization - Routing and Internetworking: Network-Layer Routing, Least-Cost-Path algorithms, Non-Least-Cost-Path algorithms, Intradomain Routing Protocols, Interdomain Routing Protocols, Congestion Control at Network Layer

Section-B

Logical Addressing: IPv4 Addresses, IPv6 Addresses - Internet Protocol: Internetworking, IPv4, IPv6, Transition from IPv4 to IPv6 - Multicasting Techniques and Protocols: Basic Definitions and Techniques, Intradomain Multicast Protocols, Interdomain Multicast Protocols, Node-Level Multicast algorithms - Transport and End-to-End Protocols: Transport Layer, Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Mobile Transport Protocols, TCP Congestion Control - Application Layer: Principles of Network Applications, The Web and HTTP, File Transfer: FTP, Electronic Mail in the Internet, Domain Name System (DNS), P2P File Sharing, Socket Programming with TCP and UDP, Building a Simple Web Server

Section-C

Wireless Networks and Mobile IP: Infrastructure of Wireless Networks, Wireless LAN Technologies. IEK1: S02.11 Wireless Standard, Cellular Networks, Mobile IP, Wireless Mesh Networks (WMNs) - Optical Networks and WDM Systems: Overview of Optical Networks, Basic Optical Networking Devices, Large-Scale Optical Switches, Optical Routers, Wavelength Allocation in Networks, Case Study: An All-Optical Switch

Section-D

VPNs, Tunneling and Overlay Networks: Virtual Private Networks (VPNs), Multiprotocol Label Switching (MPLS), Overlay Networks-VoIP and Multimedia Networking: Overview of IP Telephony, VoIP Signaling Protocols, Real-Time Media Transport Protocols, Distributed Multimedia Networking, Stream Control Transmission Protocol - Mobile A-Hoc Networks: Overview of Wireless Ad-Hoc

Networks, Routing in Ad-Hoc Networks, Routing Protocols for Ad-Hoc Networks - Wireless Sensor Networks: Sensor Networks and Protocol Structures, Communication Energy Model, Clustering Protocols, Routing Protocols

References:

1. Computer Networking: A Top-Down Approach Featuring the Internet, James E Kuro.se, Keith W. Ross, Third Edition, Pearson Education, 2007
2. Computer and Communication Networks, Nader F. Mir, Pearson Education. 2007
3. Data Communications and Networking, Behrouz A. Forouzan, Fourth Edition, Tata McGraw Hill, 2007
4. An Engineering Approach to Computer Networking , S.Keshav. Pearson Education., 4th Edition, 1997
5. Computer Networks, Andrew S. Tanenbaum, Fourth Edition, Prentice Hall, 4th Edition, 2002

MTCF-106 Professional Ethics and Cyber Security

L- T- P	Exams Marks : 100
4- 0- 0	Sessional Marks : 50
	Total Marks : 150
	Duration of Exam : 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section- A

Computer ethics and philosophical ethics: Vacuum of policies, conceptual muddles, social context, moral and legal issues, uniqueness of ethical issues, role of analogy, descriptive and normative claims, ethical relativism, utilitarianism, other theories. Professional Ethics: Characteristics, the system of professions, computing as a profession, professional relationships, responsibilities, code of ethics and professional conduct. Privacy: Computers and privacy issue, reframing this issue, legislative background, better privacy protection.

Section- B

Intellectual property issues in cyberspace: Introduction to intellectual property Protections via Copyright, Trade Secrets, Trademarks, Patents, Contracting to protect intellectual property, Protection options –Encryption, copyright on web-content, copyright on software. Ethical Decision Making: Types of ethical choices, Making defensible decisions, Ethical dilemmas, law and ethics, Guidelines for dilemma (Informal and Formal), Four-step analysis process of solving dilemma Case studies: i) A stolen password ii) Recovery of data leads to Discovery of confidential files iii) Do copyright ethics change overseas?

Section-C

Crime incident Handling Basics: Hacking, cyber activism, Tracking hackers, clues to cyber crime, privacy act, search warrants, common terms, organizational roles, procedure for responding to incidents, reporting procedures, legal considerations, Information Technology Act 2000:Scope, jurisdiction, offense and contraventions, powers of police, adjudication.

Section-D

Cyber Forensics: Cyber forensics, cyber crime examples, forensics casework, investigative incident response actions, computer forensics tools, Threats in cyberspaces, Blended attacks Sample Policy Documents: i) Antivirus Guidelines Policy ii) Internal Lab Security Policy iii) Server Security Policy iv) Wireless Communications Policy. Information Security Certifications, CISSP and SSCP, CISA and CISM, SCP, GIAC, certification weaknesses, Role of these certified professionals, Windows Server 2003 Security Fundamentals.

References:

1. Deborah G Johnson, " Computer Ethics", 4th Edition, Pearson Education Publication, 2008

2. Earnest A. Kallman, J.P Grillo, “Ethical Decision making and IT: An Introduction with Cases”, McGraw Hill Publication, 2008
3. John W. Rittinghouse, William M. Hancock, “Cyber security Operations Handbook”, ElsevierPub, 2003
4. Michael E. Whitman, Herbert J. Mattord, “Principles of Information Security”, 2nd Edition,, Cengage Learning Pub., 2012
5. Randy Weaver, Dawn Weaver, “Network Infrastructure Security”, Cengage Learning Pub., 2006

MTCF -107 Security Threats

L- T- P	Exams Marks : 100
4- 0- 0	Sessional Marks : 50
	Total Marks : 150
	Duration of Exam : 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section- A

Introduction: Security threats - Sources of security threats- Motives - Target Assets and vulnerabilities – Consequences of threats- E-mail threats - Web-threats - Intruders and Hackers, Insider threats, Cyber crimes. Network Threats: Active/ Passive – Interference – Interception – Impersonation – Worms –Virus – Spam's – Ad ware - Spy ware – Trojans and covert channels – Backdoors – Bots – IP, Spoofing - ARP spoofing - Session Hijacking - Sabotage-Internal treats- Environmental threats - Threats to Server security.

Section- B

Security Threat Management: Risk Assessment - Forensic Analysis - Security threat correlation – Threat awareness - Vulnerability sources and assessment- Vulnerability assessment tools -Threat identification - Threat Analysis - Threat Modeling - Model for Information Security Planning.

Section-C

Security Elements: Authorization and Authentication - types, policies and techniques - Security certification - Security monitoring and Auditing - Security Requirements Specifications - Security Polices and Procedures, Firewalls, IDS, Log Files, Honey Pots

Section- D

Access control, Trusted Computing and multilevel security - Security models, Trusted Systems, Software security issues, Physical and infrastructure security, Human factors – Security awareness, training , Email and Internet use policies.

References:

1. Swiderski, Frank and Syndex, "Threat Modeling", Microsoft Press, 2004.
2. William Stallings and Lawrie Brown, "Computer Security: Principles and Practice", Prentice Hall, 2008.
3. Joseph M Kizza, "Computer Network Security", Springer Verlag, 2005
4. Thomas Calabres and Tom Calabrese, "Information Security Intelligence: Cryptographic Principles & Application", Thomson Delmar Learning, 2004.

MTCF -108 Information Theory and Coding

L- T- P	Exams Marks : 100
4- 0- 0	Sessional Marks : 50
	Total Marks : 150
	Duration of Exam : 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section- A

Source Coding - Introduction to information theory, uncertainty and information, average mutual information and entropy, source coding theorem, Shannon-fano coding, Huffman coding, Arithmetic coding, Lempel-Ziv algorithm, run-length encoding and rate distortion function.

Channel capacity and coding - channel models, channel capacity, channel coding, information capacity theorem, random selection of codes. Error control coding: linear block codes and their properties, decoding of linear block code, perfect codes, hamming codes, optimal linear codes and MDS codes.

Section- B

Cyclic codes - polynomials, division algorithm for polynomials, a method for generating cyclic codes, matrix description of cyclic codes, burst error correction, fire codes, golay codes, CRC codes, circuit implementation of cyclic codes. BCH codes: minimal polynomials, generator polynomial for BCH codes, decoding of BCH codes, Reed-Solomon codes and nested codes.

Section-C

Convolutional codes - tree codes and trellis codes, polynomial description of convolutional codes, distance notions for convolutional codes, generation function, matrix description of convolutional codes, viterbi decoding of convolutional codes, distance bounds for convolutional codes, turbo codes and turbo decoding.

Section- D

Trellis Coded Modulation - concept of coded modulation, mapping by set partitioning, ungerboeck's TCM design rules, TCM decoder, Performance evaluation for Additive White Gaussian Noise (AWGN) channel, TCM for fading channels.

References:

1. Ranjan Bose, "Information theory, coding and cryptography", Tata McGraw Hill, 2002.
2. Viterbi, "Information theory and coding", McGraw Hill, 1982.
3. John G. Proakis, "Digital Communications", 2nd Edition, McGraw Hill, 1989.

SECOND SEMESTER

MTCF -201 Ethical Hacking and Digital Forensics

L- T- P	Exams Marks : 100
4- 0- 0	Sessional Marks : 50
	Total Marks : 150
	Duration of Exam : 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section-A

Hacking windows – Network hacking – Web hacking – Password hacking. A study on various attacks – Input validation attacks – SQL injection attacks – Buffer overflow attacks - Privacy attacks.

Section-B

TCP / IP – Checksums – IP Spoofing port scanning, DNS Spoofing. Dos attacks – SYN attacks, Smurf attacks, UDP flooding, DDOS – Models. Firewalls – Packet filter firewalls, Packet Inspection firewalls – Application Proxy Firewalls. Batch File Programming.

Section-C

Fundamentals of Computer Fraud – Threat concepts – Framework for predicting inside attacks – Managing the threat – Strategic Planning Process. Architecture strategies for computer fraud prevention – Protection of Web sites – Intrusion detection system – NIDS, HIDS – Penetrating testing process – Web Services – Reducing transaction risks.

Section-D

Key Fraud Indicator selection process customized taxonomies – Key fraud signature selection process –Accounting Forensics – Computer Forensics – Journaling and it requirements – Standardized logging criteria – Journal risk and control matrix – Neural networks – Misuse detection and Novelty detection.

References:

1. Kenneth C.Brancik “Insider Computer Fraud” Auerbach Publications Taylor & Francis Group, 2008.
2. Ankit Fadia “ Ethical Hacking” 2nd Edition Macmillan India Ltd, 2006

MTCF -202 Database Security

L- T- P	Exams Marks : 100
4- 0- 0	Sessional Marks : 50
	Total Marks : 150
	Duration of Exam : 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section-A

Introduction Introduction to Databases Security Problems in Databases Security Controls, Security Models – 1: Introduction Access Matrix Model Take-Grant Mode! Aclcn Model PN Model Hartsor and Hsiao's Model Fernandez's Model Bussolati and Martella's Model for Distributed databases - Security Models – 2:Bell and LaPadula's Model Biba's Model Dion's Model Sea View Model Jajodia and Sandhu'r Model The Lattice Model for the Flow Control conclusion

Section-B

Security Mechanisms: Introduction User Identification/Authentication Memory Protection Resource Protection Control Flow Mechanisms Isolation Security Functionalities in Some Operating Systems Trusted Computer System Evaluation Criteria - Security Software Design: Introduction A Methodological Approach to Security Software Design Secure Operating System Design Secure DBMS Design Security Packages Database Security Design

Section-C

Statistical Database Protection & Intrusion Detection Systems: Introduction Statistics Concepts and Definitions Types of Attacks Inference Controls evaluation Criteria for Control Comparison. Introduction IDES System RETISS System ASES System Discovery

Section-D

Models For The Protection Of New Generation Database Systems -1: Introduction A Model for the Protection of Frame Based Systems A Model for the Protection of Object: Oriented Systems SORION Mode for the Protection of Object-Oriented Databases Models For The Protection Of New Generation Database Systems -2: A Model for the Protection of New Generation Database Systems: the Orion Model Jajodia anc Kenan’s Model A Model for the Protection of Active Databases Conclusions

References:

1. Database Security by Castano, Silvana; Fugini, Maria Grazia; Martella, Giancarlo, Pearson Edition, 1994
2. Database Security and Auditing: Protecting Data Integrity and Accessibility 1st Edition, Hassan Afyouni Thomos Edition, 2006

MTCF -203 Steganography And Digital Watermarking

L- T- P	Exams Marks : 100
4- 0- 0	Sessional Marks : 50
	Total Marks : 150
	Duration of Exam : 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section-A

Introduction to Information hiding – Brief history and applications of information hiding– Principles of Steganography – Frameworks for secret communication – Security of Steganography systems – Information hiding in noisy data – Adaptive versus non adaptive algorithms – Laplace filtering – Using cover models – Active and malicious attackers – Information hiding in written text – Examples of invisible communications.

Section- B

Survey of steganographic techniques – Substitution system and bitplane tools – Transform domain techniques – Spread spectrum and information hiding – Statistical Steganography - Distortion and code generation techniques – Automated generation of English text.

Section- C

Steganalysis – Detecting hidden information – Extracting hidden information - Disabling hidden information – Watermarking techniques – History – Basic Principles – applications – Requirements of algorithmic design issues – Evaluation and benchmarking of watermarking system.

Section- D

Survey of current watermarking techniques – Cryptographic and psycho visual aspects – Choice of a workspace – Formatting the watermark bets - Merging the watermark and the cover – Optimization of the watermark receiver – Extension from still images to video – Robustness of copyright making systems

Fingerprints – Examples – Classification – Research history – Schemes – Digital copyright and watermarking – Conflict of copyright laws on the internet.

References:

1. Stefan Katzenbelsser and Fabien A. P. Petitcolas, “Information hiding techniques for Steganography and Digital Watermarking”, ARTECH House Publishers, January 2004.
2. Jessica Fridrich, “Steganography in Digital Media: Principles, Algorithms, and Applications”, Cambridge university press, 2010.
3. Steganography, Abbas Cheddad, Vdm Verlag and Dr. Muller, “Digital Image” Aktienge sells chaft & Co. Kg, Dec 2009.
4. Ingemar Cox, Matthew Miller,Jeffrey Bloom,Jessica Fridrich and Ton Kalker, “Digital Watermarking And Steganography”, Morgan Kaufmann Publishers, Nov 2007.

MTCF -204 Mobile & Wireless Security

L- T- P	Exams Marks : 100
4- 0- 0	Sessional Marks : 50
	Total Marks : 150
	Duration of Exam : 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section-A

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.

Section-B

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.

Section-C

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.

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.

Section-D

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.

MTCF -209 Ethical Hacking Lab

L- T- P	Exams Marks : 50
0- 0- 3	Sessional Marks : 50
	Total Marks : 100
	Duration of Exam : 3 hrs.

List of Experiments

1. Working with Trojans, Backdoors and sniffer for monitoring network communication
2. Denial of Service and Session Hijacking using Tear Drop, DDOS attack.
3. Penetration Testing and justification of penetration testing through risk analysis
4. Password guessing and Password Cracking.
5. Wireless Network attacks , Bluetooth attacks
6. Firwalls , Intrusion Detection and Honeypots
7. Malware – Keylogger, Trojans, Keylogger countermeasures
8. Understanding Data Packet Sniffers
9. Windows Hacking – NT LAN Manager, Secure 1 password recovery
10. Implementing Web Data Extractor and Web site watcher.

MTCF -210 Steganography And Digital Watermarking

L-	T-	P
0-	0-	3

Exams Marks	: 50
Sessional Marks	: 50
Total Marks	: 100
Duration of Exam	: 3 hrs.

1. To study Steganography methods
2. To study Digital Watermarking System
3. Implementation of Digital certificates.
4. Implementation of encryption and decryption techniques
5. Information hiding in binary files
6. Information hiding in text
7. Information hiding in images
8. Information hiding in audio/video
9. Information hiding using DNA techniques
10. To invoke different steganography methods
11. Implementation of digital watermarking techniques

ELECTIVE-II

MTCF -205 Security Threats & Vulnerabilities

L- T- P	Exams Marks	: 100
4- 0- 0	Sessional Marks	: 50
	Total Marks	: 150
	Duration of Exam	: 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section- A

Threats and Vulnerabilities to Information and Computing Infrastructures: Internal Security Threats, Physical Security Threats, Fixed-Line Telephone System Vulnerabilities, E-Mail Threats and Vulnerabilities, E-Commerce Vulnerabilities, Hacking Techniques in Wired Networks , Hacking Techniques in Wireless Networks, Computer Viruses and Worms, Trojan Horse Programs, Hoax Viruses and Virus Alerts, Hostile Java Applets, Spyware. Wireless Threats and Attacks: Wireless Threats and Attacks,, WEP Security, Bluetooth Security,, Cracking WEP, Denial of Service Attacks, Network Attacks, Fault Attacks, Side-Channel Attacks

Section- B

Prevention: Keeping the Hackers and Crackers at Bay RFID and Security ,Cryptographic Privacy Protection Techniques, Cryptographic Hardware Security Modules, Smart Card Security, Client-Side Security, Server-Side Security ,Protecting Web Sites, Database Security, Medical Records Security, Access Control: Principles and Solutions, Password Authentication ,Computer and Network Authentication, Antivirus Technology, Biometric Basics and Biometric Authentication.

Section- C

Detection and Recovery: Intrusion Detection Systems Basics, Host-Based Intrusion Detection Systems , Network-Based Intrusion Detection Systems, Use of Agent Technology for Intrusion Detection, Contingency Planning Management, Computer Security Incident Response Teams (CSIRTs) , Implementing a Security Awareness Program, Risk Assessment for Risk Management, Security Insurance and Best Practices. Auditing Information Systems Security, Evidence Collection and Analysis Tools, Information Leakage: Detection and Countermeasures.

Section- D

Management and Policy Considerations: Digital Rights Management , Web Hosting , Managing a Network Environment , E-Mail and Internet Use Policies, Forward Security: Adoptive Cryptography Time Evolution , Security Policy Guidelines , The Asset-Security Goals Continuum: A Process for Security , Multilevel Security, Multilevel Security Models ,Security Architectures , Quality of Security Service: Adaptive Security, Security Policy Enforcement , Guidelines for a Comprehensive Security System.

References:

1. Hossein Bidgoli, Information Security, Volume 3, Threats, Vulnerabilities, Prevention, Detection, and Management, Wiley, 2006
2. Lawrence J Fennelly, Loss Prevention and Crime Prevention , Elsevier, 2004
3. Tipton Ruthbe Rg, Information Security Management, Auerbach, 1997

MTCF -206 Information Security, Management & Standards

L- T- P	Exams Marks : 100
4- 0- 0	Sessional Marks : 50
	Total Marks : 150
	Duration of Exam : 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section-A

Security Risk Assessment and Management: Introduction to Security Risk Management. Reactive and proactive approaches to risk management. Risk assessment, quantitative and qualitative approaches and asset classification - Security Assurance Approaches: Introduction to OCTAVE and COBIT approaches.

Section-B

Security Management of IT Systems: Network security management. Firewalls, IDS and IPS configuration management. Web and wireless security management. General server configuration guidelines and maintenance.

Information Security Management Information classification. Access control models, role-based and lattice models. Mandatory and discretionary access controls. Linux and Windows case studies. Technical controls, for authentication and confidentiality. Password management and key management for users. Case study: Kcrberos.

Section-C

Key Management in Organizations: Public-key Infrastructure. PKI Applications, secure email case study(S/ MIME or PGP). Issues in public-key certificate issue and lifecycle management - Management of IT Security Infrastructure; Computer security log management, malwarc handling and vulnerability management programs. Specifying and enforcing security policies.

Section-D

Auditing and Business continuity Planning: Introduction to information security audit and principles of audit. Business continuity planning and disaster recovery. Case study: 9/11 tragedy. Backup and recovery techniques for applications and storage. Computer forensics: techniques and tools. Audit Tools: NESSUS and NMAP. Information Security Standards and Compliance: Overview of ISO 17799 Standard. Legal and Ethical issues.

References:

1. Slay, J. and Koronios, A., IT Security and Risk Management, Wiley, 2006.
2. Incident Response and Computer Forensics. Chris Prosise and Kevin Mandia, McGraw-Hill 2003.
3. Nina Godbole, Information Systems Security-Security Management, Metrics, Frameworks and Best Practices, Wiley, 2009
4. Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management (Paperback) Auerbach,1st edition, 2001

MTCF -207 Multimedia Security

L- T- P	Exams Marks : 100
4- 0- 0	Sessional Marks : 50
	Total Marks : 150
	Duration of Exam : 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section- A

Digital Watermarking Basics: Models of Watermarking, Basic Message Coding, Error Correction Coding. Digital Watermarking and Digital Communications: Mutual Information and Channel Capacity, How to Design a Good Digital Watermark, Spread Spectrum Watermarking, Block DCT-domain Watermarking, Watermarking with Side-Information (Dirty-paper Coding), Improved Spread Spectrum Watermarking, Affine-Resistant Watermarking.

Section- B

Media Specific Digital Watermarking: Image Watermarking, Video Watermarking, Audio Watermarking, Watermarking for CG-models, Watermarking for Binary Images, Watermarking for 3D Contents, Data Hiding through watermarking techniques.

Section- C

Digital Watermarking Protocols: A Buyer-Seller Watermarking Protocol, An Efficient and Anonymous Buyer-Seller, Watermarking Protocol, Extensions of Watermarking Protocols, Protocols for Secure Computation.

Section-D

Cryptography and Multimedia Encryption: Introduction to Cryptography, Multimedia Processing in the Encryption Domain, Privacy preserving Information Processing, Information Theory and Digital Forensics, Forgeries Detection, New ways for making Forgeries.

References:

1. Digital Watermarking and Steganography, 2nd Edition, by Cox, Miller, Bloom, Fridrich, and Kalker, 2008
2. Multimedia Security Handbook, Borko Furht, Darko Kirovski, CRC Press, 2004
3. Multimedia Security Technologies for Digital Rights Management, Wenjun Zeng, Heather Yu, Ching-Yung Lin, Elsevier, 2006

MTCF -208 Computer Security, Audit Assurance and Risk Management

L- T- P	Exams Marks : 100
4- 0- 0	Sessional Marks : 50
	Total Marks : 150
	Duration of Exam : 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section-A

Essentials of computer security - Sources of security threats – Intruders, Viruses, Worms and related threats - Threat identification - Threat analysis - Vulnerability identification and assessment - Components of Computer Security - Physical security – System access control - Goals of Security - Efforts to secure computer networks – Ethical issues in Computer Security- Operational issues, Human issues. Cryptography - Public Key Cryptography – Principles of Public Key Cryptosystems – The RSA Algorithm – Key Management – Authentication – Elements, types and methods – Digital Signature

Section-B

Intrusion Detection System (IDS) – Types and challenges – Intrusion prevention system (IPS) – Firewalls - Design Principles, Scanning, filtering and blocking. Vulnerabilities – Sources of vulnerabilities, Vulnerability identification and Assessment, Cyber crime and Hackers, Viruses and content filtering - Security Assessment, Analysis and Assurance – Computer network security protocol and standards - Security Policies – Integrity policies – confidentiality policies - Security models - Access Control Matrix Model, Take-Grant Protection Model.

Section-C

Security Monitoring and Auditing - Assurance and Trust, Need for Assurance, Role of Requirements in Assurance, Audit Assurance in Software Development Phases, Building Secure and Trusted Systems - Designing an Auditing System, Implementation Considerations, Auditing to Detect Violations of a security Policy, Auditing Mechanisms, Audit Browsing.

Section- D

Risk management and security planning – Risk management Process Overview- Cost-Benefit Analysis, Risk Analysis, Laws and Customs, Human Issues, Organizational issues - Information system Risk analysis – System approach to risk management, Threat assessment, Assets and safeguards, modes of risk analysis – Effective risk analysis, Qualitative Risk analysis, Value analysis

References

1. Matt Bishop, “Computer Security: Art and Science”, Addison-Wesley Professional, 2003.
2. Joseph M.Kizza, “Computer Network security”, Springer, 2005
3. Matt Bishop, “Introduction to Computer Security”, Addison-Wesley Professional, 2005.
4. Thomas R.Peltier, “Information Security Risk Analysis”, CRC Press, 2001.
5. C.A.Roper, “Risk management for Security professional”, Elsevier, 1999.

THIRD SEMESTER
MTCF -301 Preserving & Recovering Digital Evidence

L- T- P	Exams Marks : 100
4- 0- 0	Sessional Marks : 50
	Total Marks : 150
	Duration of Exam : 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section-A

Digital Investigation: Digital evidence and computer crime – history and terminals of computer crime investigation – technology and law - the investigate process – investigate reconstruction – modus operandi, motive and technology –digital evidence in the court room.

Section- B

Computer basics for digital investigators: applying forensic science to computers – forensic examination of windows systems – forensic examination of unix systems - forensic examination of macintosh systems - forensic examination of handheld devices.

Section-C

Networks: Networks basics for digital investigators – applying forensic science to networks – digital evidence onphysical and datalink layers - digital evidence on network and transport layers - digital evidence on the internet.

Section- D

Investigating Computer Crime: Investigating computer intrusions – investigating cyberstalking – digital evidence as alibi. Guidelines: Handling the digital crime scene – digital evidence examination guidelines.

Reference:

1. Eoghan Casey, Digital Evidence and Computer Crime Forensic science, Computers and Internet', Elsevier Academic Press –Second Edition, 2011
2. Daniel J Capra, A Electronic Discovery and Digital Evidence in a Nut Shell-Shira A scheindlin, The Sedona Conerence-Academic Press-Third Edition, 2009
3. Jack Wiles, Anthony Reyes , Jesse Varsalone The Best Damn Cybercrime and Digital Forensics Book Perio,' – Syngress Publishing, 2007
4. Casey, Eoghan. Computer Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Cambridge: Cambridge University Press, 2000
5.Vacca, John R. Computer Forensics Computer Crime Scene Investigation, Massachusetts: Charles River Media, 2002.

MTCF -302 Cyber Laws & Security Policy

L- T- P	Exams Marks : 100
4- 0- 0	Sessional Marks : 50
	Total Marks : 150
	Duration of Exam : 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section- A

Introduction -Cyber Security and its problem-Intervention Strategies: Redundancy, Diversity and Autarchy. Private ordering solutions, Regulation and Jurisdiction for global Cyber security, Copy Right-source of risks, Pirates, Internet Infringement, Fair Use, postings, criminal liability, First Amendments, Data Losing.

Section-B

Copy Right-Source of risks, Pirates, Internet Infringement, air Use, postings, Criminal Liability, First Amendments, Losing Data, Trademarks, Defamation, Privacy-Common Law Privacy, Constitutional law, Federal Statutes, Anonymity, Technology expanding privacy rights.

Section-C

Duty of Care, Criminal Liability, Procedural issues, Electronic Contracts & Digital Signatures, Misappropriation of information, Civil Rights, Tax, Evidence.

Information security policies and procedures: Corporate policies- Tier 1, Tier 2 and Tier3 policies - process management-planning and preparation-developing policies-asset classification policy-developing standards.

Section-D

Information security: fundamentals-Employee responsibilities- information classification-Information handling- Tools of information security- Information processing-secure program administration.

Organizational and Human Security: Adoption of Information Security Management Standards, Human Factors in Security- Role of information security professionals.

Reference:

1. Jonathan Rosenoer, Cyber Law: The law of the Internet, Springer, 1997

2. Mark F Grady, Fransesco Parisi Thomas R. Peltier, The Law and Economics of Cyber Security, Cambridge University Press, 2005

3. Kenneth J. Knapp, “Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions”, IGI Global, 2009.

4. Thomas R Peltier, Justin Peltier and John blackley, ”Information Security Fundamentals”, 2nd Edition, Prentice Hall, 1996

MTCF -307 Dissertation Phase-I

L- T- P
0- 0- 8

Sessional Marks : 100
Total Marks : 100

Every student will carry out dissertation under the supervision of a Supervisor(s). The topic shall be approved by a Committee constituted by the Head of the concerned Deptt. Every student will be required to present two seminar talks, first at the beginning of the Dissertation (Phase-I) to present the scope of the work and to finalize the topic, and second towards the end of the semester, presenting the work carried out by him/her in the semester. The committee constituted will screen both the presentations so as to award the sessional grades out of A+, A, B, C, D and E. A student scoring 'F' grade shall have to improve this grade before continuing his/her Dissertation in the 4^{th} semester failing which he/she shall have to repeat the Dissertation (Phase-I) next time in the regular 3^{rd} semester

MTCF -308 Seminar & Technical Writing

L- T- P
0- 0- 2

Sessionals Marks : 50
Total Marks : 50

Every student will be required to present a seminar talk on a topic approved by the Department except on his/her dissertation & submit the report to the Department. The committee constituted by the Head of the Department Will evaluates the presentation and will award the marks.

A Student who is awarded the 'F' grade will be required to repeat the seminar on the same topic.

ELECTIVE-III

MTCF -303 Biometric Security

L- T- P	Exams Marks : 100
4- 0- 0	Sessional Marks : 50
	Total Marks : 150
	Duration of Exam : 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section- A

Biometrics- Introduction- benefits of biometrics over traditional authentication systems -benefits of biometrics in identification systems-selecting a biometric for a system –Applications - Key biometric terms and processes - biometric matching methods -Accuracy in biometric systems.

Section-B

Physiological Biometric Technologies: Fingerprints - Technical description –characteristics - Competing technologies - strengths – weaknesses – deployment - Facial scan - Technical description - characteristics - weaknesses-deployment - Iris scan - Technical description – characteristics - strengths – weaknesses – deployment - Retina vascular pattern - Technical description – characteristics - strengths – weaknesses –deployment - Hand scan - Technical description-characteristics - strengths – weaknesses deployment – DNA biometrics.

Section- C

Behavioral Biometric Technologies: Handprint Biometrics - DNA Biometrics - signature and handwriting technology - Technical description – classification - keyboard / keystroke dynamics - Voice – data acquisition - feature extraction - characteristics - strengths – weaknesses deployment.

Section- D

Multi biometrics: Multi biometrics and multi factor biometrics - two-factor authentication with passwords - tickets and tokens – executive decision - implementation plan.

Case studies on Physiological, Behavioral and multifactor biometrics in identification systems.

References:

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, “Biometrics -Identity verification in a network”, Wiley Eastern, 2002.
2. John Chirillo and Scott Blaul,” Implementing Biometric Security”, Wiley Eastern Publications, 2005.
3. John Berger,” Biometrics for Network Security”, Prentice Hall, 2004.

MTCF -304 Applied Cryptography

L- T- P	Exams Marks : 100
4- 0- 0	Sessional Marks : 50
	Total Marks : 150
	Duration of Exam : 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section- A

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

Section- B

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.

Section- C

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. 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

Section-D

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" John Wiley & Sons, Inc, 2nd Edition, 1996.
2. Wenbo Mao, "Modern Cryptography Theory and Practice", Pearson Education, 2004
3. Atul Kahate, "Cryptography and Network Security", Tata McGrew Hill, 2003.

MTCF -305 Distributed Systems Security

L- T- P	Exams Marks : 100
4- 0- 0	Sessional Marks : 50
	Total Marks : 150
	Duration of Exam : 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section- A

Introduction – Distributed Systems, Distributed Systems Security. Security in Engineering: Secure Development Lifecycle Processes - A Typical Security Engineering Process - Security Engineering Guidelines and Resources. Common Security Issues and Technologies: Security Issues, Common Security Techniques.

Host-level Threats and Vulnerabilities: Transient code Vulnerabilities - Resident Code Vulnerabilities - Malware: Trojan Horse – Spyware - Worms/Viruses – Eavesdropping - Job Faults. Infrastructure-Level Threats and Vulnerabilities: Network-Level Threats and Vulnerabilities - Grid Computing Threats and Vulnerabilities – Storage Threats and Vulnerabilities – Overview of Infrastructure Threats and Vulnerabilities.

Section- B

Application-Level Threats and Vulnerabilities: Application-Layer Vulnerabilities –Injection Vulnerabilities - Cross-Site Scripting (XSS) - Improper Session Management - Improper Error Handling - Improper Use of Cryptography - Insecure Configuration Issues - Denial of Service - Canonical Representation Flaws - Overflow Issues. Service-Level Threats and Vulnerabilities: SOA and Role of Standards - Service-Level Security Requirements - Service-Level Threats and Vulnerabilities - Service-Level Attacks - Services Threat Profile.

Section-C

Host-Level Solutions: Sandboxing – Virtualization - Resource Management - Proof-Carrying Code - Memory Firewall – Antimalware. Infrastructure-Level Solutions: Network-Level Solutions - Grid-Level Solutions - Storage-Level Solutions. Application-Level Solutions: Application-Level Security Solutions.

Section-D

Service-Level Solutions: Services Security Policy - SOA Security Standards Stack – Standards in Dept - Deployment Architectures for SOA Security - Managing Service-Level Threats - Compliance in Financial Services - SOX Compliance - SOX Security Solutions - Multilevel Policy-Driven Solution Architecture - Case Study: Grid - The Financial Application - Security Requirements Analysis. Future Directions - Cloud Computing Security – Security Appliances - User centric Identity Management - Identity-Based Encryption (IBE) - Virtualization in Host Security.

References:

1. Abhijit Belapurakar, Anirban Chakrabarti and et al., “Distributed Systems Security: Issues. Processes and solutions”, Wiley, Ltd., Publication, 2009.

2. Abhijit Belapurkar, Anirban Chakrabarti, Harigopal Ponnapalli, Niranjan Varadarajan, Srinivas Padmanabhuni and Srikanth Sundarrajan, “Distributed Systems Security: Issues, Processes and Solutions”, Wiley publications, 2009.
3. Rachid Guerraoui and Franck Petit, “Stabilization, Safety, and Security of Distributed Systems”, Springer, 2010

MTCF -306 Secure Software Engineering

L- T- P	Exams Marks : 100
4- 0- 0	Sessional Marks : 50
	Total Marks : 150
	Duration of Exam : 3 hrs.

NOTE: Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. Students have to attempt 5 questions in total selecting one question from each section and Q.1 which is compulsory.

Section-A

Problem, Process, and Product - Problems of software practitioners – approach through software reliability engineering- experience with SRE – SRE process – defining the product – Testing acquired software – reliability concepts- software and hardware reliability. Implementing Operational Profiles -Developing, identifying, crating, reviewing the operation–concurrence rate–occurrence probabilities- applying operation profiles

Section- B

Engineering "Just Right" Reliability - Defining "failure" for the product - Choosing a common measure for all associated systems. - Setting system failure intensity objectives -Determining user needs for reliability and availability, overall reliability and availability objectives, common failure intensity objective, developed software failure intensity objectives. - Engineering software reliability strategies. Preparing for Test - Preparing test cases. - Planning number of new test cases for current release. -Allocating new test cases. - Distributing new test cases among new operations - Detailing test cases. - Preparing test procedures

Section- C

Executing Test - Planning and allocating test time for the current release. - Invoking test identifying identifying failures - Analyzing test output for deviations. – Determining which deviations are failures. Establishing when failures occurred. Guiding Test - Tracking reliability growth - Estimating failure intensity. - Using failure intensity patterns to guide test - Certifying reliability. Deploying SRE - Core material - Persuading your boss, your coworkers, and stakeholders. - Executing the deployment - Using a consultant.

Section-D

Using UML for Security - UM L diagrams for security requirement -security business process-physical security - security critical interaction - security state. Analyzing Model - Notation - formal semantics - security analysis - important security opportunities. Model based security engineering with UML - UML sec profile- Design principles for secure systems - Applying security patterns. Applications - Secure channel - Developing Secure Java program- more case studies. Tool support for UML Sec - Extending UML CASE TOOLS with analysis tools - Automated tools for UML SEC. Formal Foundations - UML machines - Rely guarantee specifications- reasoning about security properties.

References:

1. John Musa D, "Software Reliability Engineering", 2nd Edition, Tata McGraw-Hill, 2005
2. Jan Jürjens, "Secure Systems Development with UML", Springer; 2004

MTCF -401 Dissertation Phase -II

L- T- P	Exams Marks : 400
0- 0- 24	Sessional Marks : 200
	Total Marks : 600
	Duration of Exam : 3 hrs.

The award of sessional grades out of A+, A, B, C, D and E will be done by an internal Committee constituted by the Head of the Deptt. This assessment shall be based on presentation (s), report, etc. before this committee. In case a student scores 'F' –grade in the sessional, failing which he/ she will not be allowed to submit the dissertation. At the end of the semester, every student will be required to submit three bound copies of his/her Master's dissertation of the office of the concerned Department. Out of these, one copy will be kept for department record & one copy shall be for the supervisor.

A copy of the dissertation will be sent to the external examiner by mail by the concerned department, after his/her appointment and intimation from the university. Dissertation will be evaluated by a committee of examiners consisting of the Head of the Department, dissertation supervisor(s) and one external examiner. There shall be no requirement of a separate evaluation report on the Master Dissertation from the external examiner. The external examiner shall be appointed by the University from a panel of examiners submitted by the respective Head of Department, to the Chairman, Board of Studies. In case the external examiner so appointed by the University does not turn up, the Director/ Principal of the concerned college, on the recommendation of the concerned Head of the Department, shall be authorized, on behalf of the University, to appointed an external examiner from some other institution. The student will defend his/her dissertation through presentation before this committee and the committee will award one of the grades out of A+, A, B, C, D and E Student scoring 'F' grade in the exam shall have to resubmit his /her Dissertation after making all correction / improvements and this dissertation shall be evaluated as above.

Note: The Scheme of awarding the Grades to the student in the course will be supplied by the University to the examiner(s).