

Masters in Cyber Security (Semester System)
EXAMINATION 2019-20

M.Sc. Cyber Security Semester I & Semester II Session 2018-19
M.Sc. Cyber Security Semester III & Semester IV Session 2019-20

SCHEME OF EXAMINATION

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

ELIGIBILITY FOR ADMISSION

Graduates possessing 50% marks in any faculty of any statutory university who have studied Computer Science/ Computer Application or equivalent as a main or vocational subject for three years shall be eligible for admission to the M.Sc. Cyber Security Course (Relaxation to SC/ST etc. as per Prevailing Rules)

PASS CRITERIA

For passing in the examination, a candidate is required to obtain at least 25% in each paper (Internal + External) and 36% marks in the total aggregate in theory and 36% marks in practical separately (in each semester examination).

CLASSIFICATION OF SUCCESSFUL CANDIDATE

Division	Total Marks
First Division	60% and above
Second Division	Above 48% and below 60%
Pass	Above 36% and below 48%
Fail	Below 36%

. BACKLOG

As per University norms

WORKLOAD

- At least 3 hours for lectures and one hour for tutorial should be allotted per week for each theory paper.
- A slot of 2 hours per week should be allotted for each practical paper.

INSTRUCTIONS TO PAPER SETTER

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consists of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus).

The word limit of part A, B and C are 50, 200 and 500 respectively

INSTRUCTIONS FOR STUDENTS

- The student has to complete two months career oriented summer training from any firm/organization. If the student does not get chance to go for training, he/she can chose a research topic and can complete dissertation under the supervision of any of the faculty in his college.
- The student who has opt training, has to provide a signed certificate from the firm/ organization authority stating that the student has spent two months as a trainee in his organization/firm. The student who have opt dissertation, has to submit his/her dissertation report with a certificate from his supervisor.
- In both the cases student has to present his work in front of all the faculty members and fellow students at the starting of the next session.

*** An Academic/ Industrial Tour shall be organized by the college in every session. A Tour Report shall be prepared and submitted by the students after a study tour to industries/academic institutions of repute.**

INSTRUCTIONS FOT PRACTICAL EXAMINATION

Marks Distribution for Practical Exam -

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

1. Each practical exam is to be conducted by two examiners one External and one Internal. External examiner should be senior lecturer from jurisdiction of other universities. Marks distribution for external practical of 40 marks is as under
 - a) Practical Examination exercise of 3 questions 30 marks
 - b) Viva-Voce 5 marks
 - c) Laboratory Exercise File 5 marks
2. Marks distribution for External Project / case study report of 40 marks is as under
 - a. External Evaluation-
 - i. Research Project/ Case Study 25 marks
 - ii. Presentation 10 marks
 - iii. External Viva Voce 5 marks
 - b. Internal Evaluation- Dissertation 10 Marks

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Semester I

Paper Code	Paper Name	Exam Hours	Maximum Marks		Total Marks	Minimum passing Marks
			Internal Marks	External Marks		
Theory Papers						
MCSEC 101	Mathematical Foundation for Cyber Security	3	10	40	50	13 (25%)
MCSEC 102	Cyber Laws and Security Policies	3	10	40	50	13 (25%)
MCSEC 103	Intellectual Property Rights	3	10	40	50	13 (25%)
MCSEC 104	Java	3	10	40	50	13 (25%)
Total of Theory Papers					200	72 (36% aggregate)
Practical Papers						
MCSEC 105	Java Lab	3	10	40	50	13 (25%)
MCSEC 106	Cyber Lab	3	10	40	50	13 (25%)
Total of Practical Papers					100	36 (36% aggregate)
Grand Total					300	108 (36% aggregate)

Semester II

Paper Code	Paper Name	Exam Hours	Maximum Marks		Total Marks	Minimum passing Marks
			Internal	External		
Theory Papers						
MCSEC 201	Software Vulnerability Analysis	3	10	40	50	13 (25%)
MCSEC 202	Security Threats	3	10	40	50	13 (25%)
MCSEC 203	Web Security	3	10	40	50	13 (25%)
MCSEC 204	Python	3	10	40	50	13 (25%)
Total of Theory Papers					200	72 (36% aggregate)
Practical Papers						
MCSEC 205	Python Lab	3	10	40	50	13 (25%)
MCSEC 206	Cyber Lab	3	10	40	50	13 (25%)
Total of Practical Papers					100	36 (36% aggregate)
Grand Total					300	108 (36% aggregate)

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Semester III

Paper Code	Paper Name	Exam Hours	Maximum Marks		Total Marks	Minimum passing Marks
			Internal	External		
Theory Papers						
MCSEC 301	Intrusion Detection and Prevention Systems	3	10	40	50	13 (25%)
MCSEC 302	Information Storage Management	3	10	40	50	13 (25%)
MCSEC 303	Information Systems Audit	3	10	40	50	13 (25%)
MCSEC 304	SQL	3	10	40	50	13 (25%)
Total of Theory Papers					200	72 (36% aggregate)
Practical Papers						
MCSEC 305	Sql Lab	3	10	40	50	13 (25%)
MCSEC 306	Cyber Lab	3	10	40	50	13 (25%)
Total of Practical Papers					100	36 (36% aggregate)
Grand Total					300	108 (36% aggregate)

Semester IV

Paper Code	Paper Name	Exam Hours	Maximum Marks		Total Marks	Minimum Passing Marks
			Internal	External		
Theory Papers						
MCSEC 401	Network and Wireless Security	3	10	40	50	13 (25%)
MCSEC 402	Cyber Crime Investigations and Digital Forensics	3	10	40	50	13 (25%)
MCSEC 403	Digital Watermarking and Steganography	3	10	40	50	13 (25%)
MCSEC 404	Project	3	10	40	50	13 (25%)
Total of Theory Papers					200	72 (36% aggregate)
Practical Papers						
MCSEC 405	Cryptography Lab	3	10	40	50	13 (25%)
MCSEC 406	Cyber Lab	3	10	40	50	13 (25%)
Total of Practical Papers					100	36 (36% aggregate)
Grand Total					300	108 (36% aggregate)

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Semester I

Paper Code: MCSEC -101

Paper Name : Mathematical Foundations for Cyber Security

Scheme of Examination

Maximum Marks: 50

Duration: 3 Hours

Minimum Passing Marks: 13

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus). The word limit of part A, B and C are 50, 200 and 500 respectively.

Unit I

Number Theory: introduction, divisibility, greatest common divisor, prime numbers, fundamental theorem of arithmetic, Messene primes, Fermat numbers, euclidean algorithm, Fermat's theorem, Euler totient function, Euler's theorem. **Congruences:** definition, basic properties, residue classes, Chinese remainder theorem.

Unit II

Algebraic Structures: groups, cyclic groups, cosets, modulo groups, primitive roots, discrete logarithms. **Rings:** sub rings, ideals and quotient rings, integral domains. **Fields:** finite fields, $GF(p^n)$, $GF(2^n)$. **Classification:** structure of finite fields. **Lattice:** lattice as Algebraic system, sub lattices, some special lattices.

Unit III

Probability Theory: introduction, concepts, conditional probability, Baye's theorem, random variables – discrete and continuous, central limit theorem, stochastic process, Markov chain. **Coding Theory:** basics, codes, minimum distance, equivalence of codes, linear codes, generator matrices and parity-check matrices, syndrome decoding, Hamming codes, Hadamard code, Goppa codes.

Suggested Readings

1. Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, 'An introduction to the theory of numbers', John Wiley and Sons 2004.
2. Douglas Stinson, 'Cryptography – Theory and Practice', CRC Press, 2006.
3. Sheldon M Ross, "Introduction to Probability Models", Academic Press, 2003.
4. C.L. Liu, 'Elements of Discrete mathematics', McGraw Hill, 2008.
5. Fraleigh J. B., 'A first course in abstract algebra', Narosa, 1990.
6. Joseph A. Gallian, "'Contemporary Abstract Algebra', Narosa, 1998.

Masters in Cyber Security (Semester System)
EXAMINATION 2019-20

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Paper Code: MCSEC -102

Paper Name : Cyber Laws and Security Policies

Scheme of Examination

Maximum Marks: 50

Duration: 3 Hours

Minimum Passing Marks: 13

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus). The word limit of part A, B and C are 50, 200 and 500 respectively.

Unit I

Introduction to Computer Security: definitions, threats to security, government requirements, information protection and access controls, computer security efforts, standards, computer security mandates and legislation, privacy considerations, international security activity. **Secure System Planning and administration:** introduction to the orange book, security policy requirements, accountability, assurance and documentation requirements, network security, red book and government network evaluations.

Unit II

Information security policies and procedures: corporate policies- tier1, tier2 and tier3 policies, process management, planning and preparation, developing policies, asset classification, policy-developing standards. **Information security:** fundamentals, employee responsibilities, information classification, information handling, tools of information security, information processing, secure program administration.

Unit III

Organizational and Human Security: adoption of information security management standards, human factors in security, role of information security professionals.

Suggested Readings

1. Debby Russell and Sr. G.T Gangemi, "Computer Security Basics (Paperback)", 2nd Edition, O' Reilly Media, 2006.
2. Thomas R. Peltier, "Information Security policies and procedures: A Practitioner's Reference", 2nd Edition Prentice Hall, 2004.
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
5. Jonathan Rosenoer, "Cyber law: the Law of the Internet", Springer-verlag, 1997
6. James Graham, " Cyber Security Essentials" Averbach Publication T & F Group.

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Paper Code: MCSEC -103

Paper Name : Intellectual Property Rights

Scheme of Examination

Maximum Marks: 50

Duration: 3 Hours

Minimum Passing Marks: 13

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consists of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus). The word limit of part A, B and C are 50, 200 and 500 respectively.

Unit I

Intellectual Property Law: Introduction, evolutionary past, IPR tool kit, para-legal tasks in intellectual property law, ethical obligations in para legal tasks **Cyber law:** introduction, innovations and inventions trade related intellectual property right

Unit II

Copyrights: principles, rights afforded by copyright law, copy right ownership, transfer and duration, right to prepare derivative works, rights of distribution, rights of perform the work publicity copyright formalities and registrations, limitations, copyright disputes and international copyright law, semiconductor chip protection act

Unit III

Patents: law of patents, patent searches, patent ownership and transfer, patent infringement, international patent law. **Trade secret:** introduction, maintaining trade secret, physical security, employee limitation, employee confidentiality agreement, trade secret law, unfair competition, trade secret litigation, breach of contract, applying state law.

Suggested Readings

1. Debirag E.Bouchoux: "Intellectual Property". Cengage learning, New Delhi
2. M.Ashok Kumar and Mohd.Iqbal Ali: "Intellectual Property Right" Serials Pub.
3. Cyber Law. Texts & Cases, South-Western's Special Topics Collections
4. Prabhuddha Ganguli: ' Intellectual Property Rights" Tata Mc-Graw –Hill, New Delhi
5. J Martin and C Turner "Intellectual Property" CRC Press
6. Richard Stimm " Intellectual Property" Cengage Learning

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Paper Code: MCSEC -104

Paper Name : Java

Scheme of Examination

Maximum Marks: 50

Duration: 3 Hours

Minimum Passing Marks: 13

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consists of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus). The word limit of part A, B and C are 50, 200 and 500 respectively.

Unit I

Introduction to java: evolution, features, comparison with C and C++; Java program structure; tokens, keywords, constants, variables, data types, type casting, statements, Operators and Expression; Conditional Statements and Loop Statements. **Class:** syntax, instance variable, class variables, methods, constructors, overloading of constructors and methods.

Unit II

Inheritance: types of inheritance, use of super, method overriding, final class, abstract class, wrapper classes.

Arrays, Strings and Vectors, Packages and Interfaces, visibility controls

Unit III

Errors and Exceptions: Types of errors, Exception classes, Exception handling in java, use of try, catch, finally, throw and throws. Taking user input, Command line arguments.

Multithreaded Programming: Creating Threads, Life cycle of thread, Thread priority, Thread synchronization, Inter-thread communication, Implementing the Runnable Interface; **Applet:** Applet Life Cycle, Applet Tag, Adding Applet to HTML File; Passing Parameters to Applets, Getting Input From User.

Suggested Readings

1. The Complete reference Java Ninth Edition By Herbert Schildt (Tata McGraw Hill)
2. Beginning Programming with Java For Dummies by Burd, For Dummies; 3 edition
3. Java: A Beginner's Guide, Sixth Edition: A Beginner's Guide by Herbert Schildt, McGraw-Hill Osborne Media Programming in JAVA By E. Balagurusamy (TMH)
4. JAVA 2 programming Black Book By Steven Holzner et al. (Dreamtech Press)
5. Programming in JAVA By E. Balagurusamy (TMH)

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Semester II

Paper Code: MCSEC 201

Paper Name : Software Vulnerability Analysis

Scheme of Examination

Maximum Marks: 50

Duration: 3 Hours

Minimum Passing Marks: 13

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus). The word limit of part A, B and C are 50, 200 and 500 respectively.

Unit I

Introduction to security & authentication: software security, security failures, bugtraq, CERT Advisories, technical trends affecting software security, penetrate and patch, security goals, prevention, traceability and auditing, monitoring, privacy and confidentiality, Multilevel security, Anonymity, Authentication, Integrity, software security pitfalls, Software project goals. **Application Security & Malicious Code:** software risk management for security, role of security personnel, risk assessment, development goes astray, code review (tools), architectural risk analysis, penetration testing, risk-based security testing, abuse cases and security requirements, security operations

Unit II

Access control & physical protection: Linux access control model, Linux Permissions, modifying file attributes, modifying ownership, the umask, programmatic interface, access control in Windows NT, compartmentalization, fine-grained privileges. **Buffer overflow & rootkits:** buffer overflows as security problems, defending against buffer overflow, internal buffer overflows, tools for handling buffer overflows, smashing heaps and stacks, heap overflows, stack overflows, decoding the stack.

Unit III

Network Security & Intrusion: OSI model, sockets, socket functions, socket addresses, network byte order, internet address conversion, simple server and web clients, Tinyweb server. Peeling back the lower layers, network sniffing, raw socket sniffer, libpcap sniffer, decoding the layers, active sniffing, Denial of Service, SYN Flooding, ping of death, teardrop, ping flooding, amplification attacks, Distributed DoS Flooding, TCP/IP hijacking, RST hijacking, continued hijacking, port scanning, stealth SYN Scan, FIN, X-mas, and Null scans, spoofing Decoys, idle scanning, proactive defence (shroud), reach out and hack someone.

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Suggested Readings

1. John Viega & Gary McGraw: *Building Secure Software: How to Avoid Security Problems the Right Way* (Addison-Wesley Professional Computing Series)
2. Gary McGraw: *Software Security: Building Security In* (Addison-Wesley Professional Computing Series)
3. Michael Howard, David LeBlanc, John Viega: *19 Deadly Sins of Software Security: Programming Flaws and How to Fix Them (Security One-off)* (Addison-Wesley Professional Computing Series)
4. Jon Erickson: *Hacking: The Art of Exploitation*, 2nd Edition (No Starch Press, San Francisco)
5. Richard Sinn “ Software Security , Theory Programming and Practice” Cengage Learning

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Paper Code: MCSEC 202

Paper Name : Security Threats

Scheme of Examination

Maximum Marks: 50

Duration: 3 Hours

Minimum Passing Marks: 13

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus). The word limit of part A, B and C are 50, 200 and 500 respectively.

Unit I

Security threats: introduction, sources, motives, target assets and vulnerabilities, consequences of threats, e-mail threats, web threats, intruders and hackers, insider threats.

Network Threats: active/ passive, interference, interception, impersonation, worms, virus, spams, adware, spyware, Trojans. Covert channels, backdoors, bots, IP spoofing, ARP spoofing, session hijacking, sabotage-internal threats, environmental threats, threats to server security.

Unit II

Security threat management: risk assessment, forensic analysis, security threat correlation, threat awareness, vulnerability sources and assessment, vulnerability assessment tools, threat identification, **Threat analysis:** threat modelling, model for Information Security planning.

Unit III

Security Elements: authorization and authentication, types, policies and techniques, security certification, security monitoring and auditing, security requirements specifications, security policies and procedures, firewalls, IDS, log files, honey pots. **Access control:** trusted computing and multilevel security, security models, trusted systems, software security issues, physical and infrastructure security, security awareness, training, e-mail, and Internet use policies.

Suggested Readings

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

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Paper Code: MCSEC 203

Paper Name : Web Security

Scheme of Examination

Maximum Marks: 50

Duration: 3 Hours

Minimum Passing Marks: 13

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus). The word limit of part A, B and C are 50, 200 and 500 respectively.

Unit I

Introduction: web security, web languages, web attacks, N-tier web applications, web servers: Apache, IIS, database servers, computer security, cryptography basics, public key cryptography, RSA, shopping, payment gateways

Unit II

Web hacking: basics HTTP & HTTPS URL, web under the cover, overview of java security, reading the HTML source, applet security servlets, symmetric and asymmetric encryptions, network security basics, firewalls & IDS.

Unit III

Digital certificates and digital signatures: digital certificates, hashing, message digest. digital signatures basics, securing databases, secure JDBC, securing large applications, cyber graffiti

Suggested Readings

1. McClure, Stuart, Saumil Shah, and Shreeraj Shah. Web Hacking: attacks and defence. Addison Wesley. 2003.
2. Garms, Jess and Daniel Somerfield. Professional Java Security. Wrox. 2001.

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Paper Code: MCSEC 204

Paper Name : Python

Scheme of Examination

Maximum Marks: 50

Duration: 3 Hours

Minimum Passing Marks: 13

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consists of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus). The word limit of part A, B and C are 50, 200 and 500 respectively.

Unit I

Overview of Programming : Structure of a Python Program, Python Interpreter, Using Python as calculator, Python shell, Indentation. Identifiers and keywords, data types, Operators. Creating Python Programs : Input and Output Statements, if-else statements, Loops(while, for) and Control Statements (continue, break), nested loops.

Unit II

Functions and scoping. Iteration and Recursion, Stack diagrams for recursive functions, Multiple assignment, Implementing 2-D matrices. Strings and Lists: String as a compound data type, Length, Traversal, String slices, String comparison, find function, Looping and counting, List values, Accessing elements, List length, List membership, Lists and for loops, List operations, List deletion. Cloning lists, Nested lists . Exception handling.

Unit III

Basic File Operations in Python, Object Oriented Programming: Introduction to Classes, Objects and Methods, Standard Libraries. Tuples, sequences and dictionaries. Overview of sets, stacks and queues. Overview of packages: networkx, matplotlib.pyplot, numpy. Usage of Python in encryption and decryption. Applications of Python in real world.

Suggested Readings

1. T. Budd, Exploring Python, TMH, 1st Ed, 2011
2. Introduction to Computation and Programming Using Python. By John V. Guttag, MIT Press.
3. Learning Python , Mark Lutz, David Ascher, O'Reilly

Web Resources

1. http://files.swaroopch.com/python/byte_of_python.pdf
2. <https://www.cs.uky.edu/~keen/115/Haltermanpythonbook.pdf>
3. <http://greenteapress.com/thinkpython/thinkpython.pdf>
4. Python tutorials: <https://docs.python.org/3/tutorial/index.html>

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Semester III

Paper Code: MCSEC 301

Paper Name : Intrusion Detection and Prevention Systems

Scheme of Examination

Maximum Marks: 50

Duration: 3 Hours

Minimum Passing Marks: 13

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus). The word limit of part A, B and C are 50, 200 and 500 respectively.

Unit I

Intrusion detection: basics, IDS and IPS analysis schemes, attacks, detection approaches, misuse detection, anomaly detection, specification based detection, hybrid detection. **Architecture and implementation:** centralized, distributed, cooperative intrusion detection, tiered architecture

Unit II

Justifying intrusion detection: intrusion detection in security, threat briefing, quantifying Risk, return on investment (ROI). **Application and tools:** tool selection and acquisition process, bro intrusion detection, prelude intrusion detection, cisco security IDS, snorts intrusion detection, NFR security

Unit III

Legal issues and organization standards: law enforcement, criminal prosecutions, standard of due care, evidentiary issues, organizations and standardizations.

Suggested Readings

1. Ali A. Ghorbani, Wei Lu, "Network Intrusion Detection and Prevention: Concepts and Techniques", Springer, 2010
2. Carl Enrolf, Eugene Schultz, Jim Mellander, "Intrusion detection and Prevention", McGraw Hill, 2004
3. Paul E. Proctor, "The Practical Intrusion Detection Handbook", Prentice Hall, 2001.
4. Ankit Fadia and Mnu Zacharia, "Intrusion Alert", Vikas Publishing house Pvt., Ltd, 2007
5. Earl Carter, Jonathan Hogue, "Intrusion Prevention Fundamentals", Pearson Education, 2006.

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Paper Code: MCSEC 302

Paper Name : Information Storage Management

Scheme of Examination

Maximum Marks: 50

Duration: 3 Hours

Minimum Passing Marks: 13

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus). The word limit of part A, B and C are 50, 200 and 500 respectively.

Unit I

Storage Technology: data proliferation and the varying value of data with time and usage, sources of data and states of data creation, data center requirements and evolution, basic storage management skills and activities, storage infrastructure components, evolution of storage, information lifecycle management, data categorization, storage and regulations. **Storage system architecture:** intelligent disk subsystems, component architecture, performance and logical partitioning, RAID & parity algorithms, protection, and back end management.

Unit II

Network storage: JBOD, DAS, SAN, NAS, & CAS evolution, elements, connectivity, standards & management. **Introduction to information availability:** business continuity and disaster recovery basics, local business continuity techniques, remote business continuity techniques, disaster recovery principles & techniques

Unit III

Managing & monitoring: management philosophies (holistic vs. system & component), industry management standards (SNMP, SMI-S, CIM), Standard framework applications, key management metrics (thresholds, availability, capacity, security, performance), metric analysis methodologies & trend analysis, reactive and pro-active management best practices, provisioning & configuration change planning, problem reporting, prioritization, and handling techniques, management tools overview. **Securing storage and storage virtualization:** storage security, critical security attributes, elements of a shared storage model virtualization technologies, block-level and file level virtualization technologies and processes.

Suggested Readings

1. Marc Farley Osborne, "Building Storage Networks", Tata Mac Graw Hill, 2001
2. Robert Spalding and Robert Spalding, "Storage Networks: The Complete Reference", Tata McGraw Hill, 2003
3. Meeta Gupta, "Storage Area Network Fundamentals", Pearson Education Ltd., 2002
4. Gerald J Kowalski and Mark T Maybury, "Information Storage Retrieval Systems theory & Implementation", BS Publications, 2000
5. Thejendra BS, "Disaster Recovery & Business continuity", Shroff Publishers & Distributors, 2006

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Paper Code: MCSEC 303

Paper Name : Information Systems Audit

Scheme of Examination

Maximum Marks: 50

Duration: 3 Hours

Minimum Passing Marks: 13

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus). The word limit of part A, B and C are 50, 200 and 500 respectively.

Unit I

Information system auditing: basics, conducting information system audit, **Management control framework-I:** introduction, evaluating the planning, leading, controlling function, systems development management controls, approaches to auditing systems development, systems development process, major phases, programming management controls, data resource management controls.

Unit II

Management control framework-II: security management controls, operations management controls, quality assurance management controls. **Application control framework-I:** boundary controls, input controls, communication controls. **Application control framework-II:** processing controls, database controls, output controls.

Unit III

Evidence collection: audit software, code review, test data, and code comparison, concurrent auditing techniques, interviews, questionnaires, and control flowcharts, performance management tools, **Evidence evaluation:** evaluating asset safeguarding and data integrity, evaluating system effectiveness, evaluating system efficiency.

Suggested Readings

1. Ron Weber, Information Systems Control and Audit, Pearson Education, 2002.
2. M.Revathy Sriram, Systems Audit, TMH, New Delhi, 2001.
3. Jalote : Software Project Mangement in Practice, Pearson Education
4. Royce : Software Project Management, Pearson Education.

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Paper Code: MCSEC 304

Paper Name : SQL

Scheme of Examination

Maximum Marks: 50

Duration: 3 Hours

Minimum Passing Marks: 13

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consists of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus). The word limit of part A, B and C are 50, 200 and 500 respectively.

Unit I

SQL: Data Types, statements: select, insert, update,delete, create, alter, drop; views, SQL algebraic operations, nested queries; Stored procedures: Advantages, Variables, creating and calling procedures, if and case statements, loops, Cursors, Functions, Triggers.

Unit II

Normalization: Definition, Functional dependencies and inference rules, 1NF, 2NF, 3NF and BCNF; Transactions processing: Definition , desirable properties of transactions, serial and non-serial schedules ,concept of serialazability , conflict-serializable schedules.

Unit III

Concurrency Control: Two-phase locking techniques, dealing with Deadlock and starvation, deadlock prevention protocols, basic timestamp ordering algorithm; Overview of database recovery techniques;concept of datawarehousing.

Suggested Readings

1. Fundamentals of Database Systems,Ramez A. Elmasri, Shamkant Navathe,5th Ed(Pearson)
2. Database System Concepts By Korth, Silberschatz, Sudarshan (Mcgraw Hill)
3. An Introduction to Database Systems By Bipin C. Desai (Galgotia Publication.)
4. SQL, PL/SQL Programming By Ivan Bayross (BPB)
5. Commercial Application Development Using Oracle Developer 2000 By Ivan Bayross (BPB)

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Semester IV

Paper Code: MCSEC401

Paper Name : Network & Wireless Security

Scheme of Examination

Maximum Marks: 50

Duration: 3 Hours

Minimum Passing Marks: 13

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus). The word limit of part A, B and C are 50, 200 and 500 respectively.

Unit I

Network: concepts, threats, network security controls, importance of security, threat models, common mitigation methods. **Authentication:** overview, authentication of people, security handshake pitfalls, strong password protocols, Kerberos, public key infrastructure. **IP security:** overview, architecture, authentication header, encapsulating security payload, key management. **Web security:** considerations, secure socket layer and transport layer security, secure electronic transaction.

Unit II

Electronic Mail Security: store and forward, security services for e-mail, establishing keys, privacy authentication of the source, message integrity, non-repudiation, proof of submission and delivery, pretty good privacy, secure/multipurpose internet mail extension. **Wireless technologies:** introduction, wireless data networks, personal area networks, transmission media, WLAN standards, securing WLANS, WEP (Wired Equivalence Protocol). **Wireless Threats:** kinds of security breaches, eavesdropping, communication jamming, RF interference, convert wireless channels, DOS attack, spoofing, theft of services, traffic analysis, cryptographic threats, wireless security standards.

Unit III

Security in data networks: wireless device security issues, CDPD security (Cellular Digital Packet Data), GPRS security (General Packet Radio Service), GSM (Global System for Mobile Communication) security, IP security. **Wireless transport layer security:** secure socket layer, wireless transport layer security, WAP security architecture, WAP gateway. **Bluetooth Security:** basics, piconets, bluetooth security architecture, scatternets, security at the baseband layer and link layer, frequency hopping, security manager, authentication, encryption, threats to bluetooth security.

Suggested Readings

1. Charles P. Fleeger, "Security in Computing", Prentice Hall, New Delhi, 2009
2. Behrouz A. Forouzan, "Cryptography & Network Security", Tata McGraw Hill, India, New Delhi, 2009.
3. William Stallings, "Cryptography and Network Security, Prentice Hall, New Delhi, 2006.
4. Bruce Schneier, "Applied Cryptography", John Wiley & Sons, New York, 2004.
5. Nichols and Lekka, "Wireless Security-Models, Threats and Solutions", Tata McGraw – Hill, New Delhi, 2006.
6. Merritt Maxim and David Pollino, "Wireless Security", Osborne/McGraw Hill, New Delhi, 2005.

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Paper Code: MCSEC 402

Paper Name : Cyber Crime Investigations and Digital Forensics

Scheme of Examination

Maximum Marks: 50

Duration: 3 Hours

Minimum Passing Marks: 13

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus). The word limit of part A, B and C are 50, 200 and 500 respectively.

Unit I

Cyber Crime: nature, scope, types, categories, property social engineering, cyber crime issues: unauthorized access to computers, computer intrusions, white collar crimes, viruses and malicious code, internet hacking and cracking, virus attacks, pornography, software piracy, intellectual property, mail bombs, exploitation, stalking and obscenity in internet, digital laws and legislation, law enforcement roles and responses.

Unit II

Investigation: introduction investigation Tools, eDiscovery, digital evidence collection, evidence preservation, e-mail investigation, e-mail tracking, IP tracking, e-mail recovery. encryption and decryption methods, search and seizure of computers, recovering deleted evidences, password cracking.

Unit III

Digital Forensics : Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, Network Forensics. **Laws and Acts:** Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC , Electronic Communication Privacy ACT, Legal Policies.

Suggested Readings

1. Nelson Phillips and Enfinger Stuart, "Computer Forensics and Investigations", Cengage Learning, New Delhi, 2009
2. Kevin Mandia, Chris Prosis, Matt Pepe, "Incident Response and Computer Forensics", TataMcGraw -Hill, New Delhi, 2006
3. Robert M Slade," Software Forensics", Tata McGraw - Hill, New Delhi, 2005
4. Bernadette H Schell, Clemens Martin, "Cybercrime", ABC – CLIO Inc, California, 2004
5. "Understanding Forensics in IT ", NIIT Ltd, 2005.

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Paper Code: MCSEC403

Paper Name : Digital Watermarking and Steganography

Scheme of Examination

Maximum Marks: 50

Duration: 3 Hours

Minimum Passing Marks: 13

The question paper contains 3 sections. **Section-A** consists of 10 questions (at least 3 questions from each unit of syllabus). **Section-B** will consist of 9 questions (3 questions from each unit of syllabus). **Section-C** will consist of 6 questions (2 questions from each unit of syllabus). The word limit of part A, B and C are 50, 200 and 500 respectively.

Unit I

Watermarking: history, importance, applications, properties, evaluation. **Watermarking models & message coding:** notation, communications, communication based models, geometric models, mapping messages into message vectors, error correction coding, detecting multi-symbol watermarks.

Unit II

Watermarking Errors: informed embedding, informed coding, structured dirty-paper codes, message errors, false positive errors, false negative errors, ROC curves, effect of whitening on error rates. **Perceptual Models:** evaluating perceptual impact, general form of a perceptual model, example, Robust watermarking approaches, redundant embedding, spread spectrum coding, embedding in perceptually significant coefficients

Unit III

Watermark Security & Authentication: security requirements, watermark security and cryptography, attacks, exact authentication, selective authentication, localization, restoration. **Steganography:** steganography communication, notation and terminology, information, theoretic and practical steganographic methods, minimizing the embedding impact, Steganalysis

Suggested Readings

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, "Digital Watermarking and Steganography", Morgan Kaufmann Publishers, New York, 2008.
2. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, "Digital Watermarking", Morgan Kaufmann Publishers, New York, 2003.
3. Michael Arnold, Martin Schmucker, Stephen D. Wolthusen, "Techniques and Applications of Digital Watermarking and Content Protection", Artech House, London, 2003.
4. Juergen Seits, "Digital Watermarking for Digital Media", IDEA Group Publisher, New York, 2005.
5. Peter Wayner, "Disappearing Cryptography – Information Hiding: Steganography & Watermarking", Morgan Kaufmann Publishers, New York, 2002.

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

Paper Code: MCSEC 404

Paper Name : Research Project/ Case Study

Scheme of Examination

Maximum Marks: 50

Duration: 3 Hours

Minimum Passing Marks: 13

Research Project / Case Study Work:

1. Research Project/ case study Work may be done individually or in groups in case of bigger projects. However if project is done in group each student must be given a responsibility for a distinct module and care should be taken to monitor the individual student.
2. Research Project/case study Work can be carried out in the college or outside with prior permission of college.
3. The Student must submit a synopsis of the research project/case study report to the college for approval. The Project Guide can accept the project or suggest modification for resubmission. Only on acceptance of draft project report the student should make the final copies.
4. **The Research Project/ Case Study Report should be hand written**

Submission Copy:

The Student should submit spiral bound copy of the project/case study report.

Format of the Report:

(a) Paper:

The Report shall be typed on White Paper of A4 size.

(b) Final Submission:

The Report to be submitted must be original.

(c) Typing:

Font:- Times New Roman

Heading:- 16 pt., Bold

Subheading:- 14 pt, Bold

Content:- 12 pt.

Line Spacing:- 1.5 line.

Typing Side :-One Side

Font Color:- Black.

(d) Margins:

The typing must be done in the following margin:

Left : 0.75"

Right: 0.75"

Top: 1"

Bottom: 1"

Left Gutter: 0.5"

(e) Binding:

The report shall be Spiral Bound.

(f) Title Cover:

The Title cover should contain the following details:

Top: Project/case study Title in block capitals of 16pt.

Centre: Name of project developer's and Guide name.

Bottom: Name of the university, Year of submission all in block capitals of 14pt letters on separate lines with proper spacing and centering.

Masters in Cyber Security (Semester System)

EXAMINATION 2019-20

(g) Blank sheets:

At the beginning and end of the report, two white blank papers should be provided, one for the Purpose of Binding and other to be left blank.

(h) Content:

- I).** Acknowledgement
- II).** Institute/College/Organization certificate where the project is being developed.
- III).** Table of contents
- IV).** A brief overview of project
- V).** Profiles of problem assigned
- VI).** Study of Existing System
- VII).** System Requirement
- VIII).** Project plan
 - Team Structure
 - Development Schedule
 - Programming language and Development Tools
- IX).** Requirement Specification
- X).** Design
 - Detailed DFD's and Structure Diagram
 - Data structure, Database and File Specification

- XI).** Project Legacy
 - Current Status of project
 - Remaining Areas of concern
 - Technical and Managerial Lessons Learnt
 - Future Recommendations
- XII).** Nomenclature and Abbreviations.
- XIII).** Bibliography
- XIV).** Source Code.