M.Sc. (Computer Science)
Semester-2
MSCS-2-03T: Introduction to Cyber Security

Total Marks: 100
External Marks: 70
Internal Marks: 30
Credits: 4
Pass Percentage: 40%

INSTRUCTIONS FOR THE PAPER SETTER/EXAMINER

1. The syllabus prescribed should be strictly adhered to.
2. The question paper will consist of three sections: A, B, and C. Sections A and B will have four questions from the respective sections of the syllabus and will carry 10 marks each. The candidates will attempt two questions from each section.
3. Section C will have fifteen short answer questions covering the entire syllabus. Each question will carry 3 marks. Candidates will attempt any ten questions from this section.
4. The examiner shall give a clear instruction to the candidates to attempt questions only at one place and only once. Second or subsequent attempts, unless the earlier ones have been crossed out, shall not be evaluated.
5. The duration of each paper will be three hours.

INSTRUCTIONS FOR THE CANDIDATES

Candidates are required to attempt any two questions each from the sections A and B of the question paper and any ten short q questions from Section C. They have to attempt questions only at one place and only once. Second or subsequent attempts, unless the earlier ones have been crossed out, shall not be evaluated.

SECTION-A

Unit I: Cyber Attacks: Introduction, Types. Assets: Identification, Accountability. Vulnerability and Threats, Risk Management, Qualitative Risk Assessment, Information Security Framework: Introduction, Policies, Standards, Baselines, Guidelines and Procedures.

Unit II: Security: Basics, User Access Controls, Authentication, Access Control: Framework, Techniques and Technologies, Training and Awareness and Its types, Technical Security Controls: Preventive, Detective, Corrective. Protection form malicious attacks.

Unit III: Networks and Communication: Data Communication, Characteristics and components, Data flow. Computer Network, Categories, Protocol, External Services, Cloud Computing: Introduction, Models, Benefits, Challenges, Private, Public Clouds.

Unit IV: Software Engineering Life Cycle: Stages, Models: Waterfall, Iterative, Spiral, V Model, Big Bang, Agile, RAD, Prototype.

SECTION-B

Unit V: Authentication: Authentication Vs Authorization, Methods and Protocols: Kerberos, SSL, Protocol, Password Authentication, Challenge-Handshake Authentication (CHAP), MSCHAP, Extensible Authentication, Remote Authentication.

Unit VI: Service Set Identification (SSID), Encryption Methods: Wire Equivalent Privacy, WPA, WPA2, MAC Filtering, Wireless Routers, Creating Wireless Network, WLAN.

Unit VII: Investigation Techniques and Cyber Forensics: Types of Investigation, Evidence and Analysis, Steps for Forensics Investigation, Forensics Tools, Investigation, Common Types of Email Abuse, Tracking Location of Email Sender, Scam or Hoax Emails and Websites, Fake Social Media Profile.

Unit VIII: Cryptography: Objectives, Type, OS Encryption, Public key Cryptography.

Reference Books:

- Mayank Bhushan, Rajkumar Singh Rathore, Aatif Jamshed, “Fundamentals of Cyber Security”, BPB Publications.
- Nina Godbole, Sunit Belapure, “Cyber Security”, Wiley.
- Sanil Nadkarni, Fundamentals of Information Security”, pbp.
- Mike Chapple, James Michael Stewart, Darril Gibson, “CISSP Certified Information Systems Security Professional Official Study Guide” 9th Edition, SYBEX, A Wiley Brand.
- William Chuck Eastton, “Computer Security Fundamentals”, 4th Edition, Pearson.