MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WEST BENGAL

NH-12 (Old NH-34), Simhat, Haringhata, Nadia -741249

Department of Information Technology (In-house)

B.Sc. in Information Technology (Cyber Security)

(Effective from academic session 2019-20)

Semester-IV

Name of the Course: B.Sc. in Information Technology (Cyber Security) **Subject: Secure Software Design & Enterprise Computing & Secure Software Design & Enterprise Computing Lab**	
Course Code: BITCS401 + BITCS491	**Semester: IV**
Duration: 36 Hrs.	**Maximum Marks: 100 + 100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial: 0	**Attendance : 5**
Practical: 4 hrs./week	**Continuous Assessment: 25**
Credit: 3 + 2	**Practical Sessional internal continuous evaluation: 40**
	Practical Sessional external examination: 60

Aim:	
Sl. No.	
1.	The course takes a software development perspective to the challenges of engineering software systems that are secure.
2.	This course addresses design and implementation issues critical to producing secure software systems.
3.	The course deals with the question of how to make the requirements for confidentiality, integrity, and availability integral to the software development process from requirements gathering to design, development, configuration, deployment, and ongoing maintenance
Objective:	
Sl. No.	
1.	Understand various aspects and principles of software security.
2.	Devise security models for implementing at the design level
3.	Identify and analyze the risks associated with s/w engineering and use relevant models to mitigate the risks.
4.	Understand the various security algorithms to implement for secured computing and computer networks.
5.	Explain different security frameworks for different types of systems including electronic systems.
Pre-Requisites	
1.	Software Engineering Fundamentals

Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	Defining computer security, the principles of secure software, trusted computing base, etc, threat modelling, advanced techniques for mapping security requirements into design specifications. Secure software implementation, deployment and ongoing management.	**7**	**14**

02	Software design and an introduction to hierarchical design representations. Difference between high-level and detailed design. Handling security with high-level design. General Design Notions. Security concerns designs at multiple levels of abstraction, Design patterns, quality assurance activities and strategies that support early vulnerability detection, Trust models, security Architecture & design reviews.	**7**	**14**
03	Software Assurance Model: Identify project security risks & selecting risk management strategies, Risk Management Framework, Security Best practices/ Known Security Flaws, Architectural risk analysis, Security Testing & Reliability (Penn testing, Risk- Based Security Testing, Abuse Cases, Operational testing , Introduction to reliability engineering, software reliability, Software Reliability approaches, Software reliability modelling.	**7**	**14**
04	Software Security in Enterprise Business: Identification and authentication, Enterprise Information Security, Symmetric and asymmetric cryptography, including public key cryptography, data encryption standard (DES), advanced encryption standard (AES), algorithms for hashes and message digests. Authentication, authentication schemes, access control models, Kerberos protocol, public key infrastructure (PKI), protocols specially designed for e-commerce and web applications, firewalls and VPNs. Management issues, technologies, and systems related to information security management at enterprises.	**8**	**14**
05	Security development frameworks. Security issues associated with the development and deployment of information systems, including Internet-based e-commerce, e-business, and e-service systems, as well as the technologies required to develop secure information systems for enterprises, policies and regulations essential to the security of enterprise information systems.	**7**	**14**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Practical:

Skills to be developed:

Intellectual skills:

1. To identify the various requirement development activities viz. elicitation, analysis, specification and verification for the given scenarios.
2. To identify the role of the software in today’s world across a few significant domains related to day to day life
3. To identify the suitable software development model for the given scenario

List of Practical: Based on theory lectures.

Assignments:

Adhered to theory curriculum as conducted by the subject teacher.

List of Books

Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
W. Stallings	Cryptography and network security: Principles and practice	Fifth	Upper Saddle River, NJ: Prentice Hall
C. Kaufman, r. Perlman, & M. Speciner	Network security: Private communication in a public world	Second	Upper Saddle River, NJ:PrenticeHalL
C. P. Pfleeger, S. L. Pfleeger	Security in Computing	Fourth	Upper Saddle River, NJ:Prentice Hall
Reference Books:			
Gary McGraw	Software Security: Building Security		Addison-Wesley
M. Merkow, & J. Breithaupt	Information security: Principles and practices.		Upper Saddle River, NJ:Prentice Hall

List of equipment/apparatus for laboratory experiments:

Sl. No.	
1.	Computer

End Semester Examination Scheme. Maximum Marks-70 Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 5**	**10**	**10**				
B	**1 to 5**			**5**	**3**	**5**	**60**
C	**1 to 5**			**5**	**3**	**15**	

- Only multiple choice type questions (MCQ) with one correct answer are to be set in the objective part.
- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	Chapter	Marks of each question	Question to be set	Question to be answered
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**
Examination Scheme for Practical Sessional examination:				
Practical Internal Sessional Continuous Evaluation				
Internal Examination:				
Continuous evaluation				**40**
External Examination: Examiner-				
Signed Lab Assignments			**10**	
On Spot Experiment			**40**	
Viva voce			**10**	**60**

Name of the Course: B.Sc. in Information Technology (Cyber Security) **Subject: Incident Analysis and Threat Hunting & Incident Analysis and Threat Hunting Lab**	
Course Code: BITCS402 + BITCS492	**Semester: IV**
Duration: 36 Hrs.	**Maximum Marks: 100 + 100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial: 0	**Attendance : 5**
Practical: 4 hrs./week	**Continuous Assessment: 25**
Credit: 3 + 2	**Practical Sessional internal continuous evaluation: 40**
	Practical Sessional external examination: 60

Aim:	
Sl. No.	
1.	Detect and hunt unknown live, dormant, and custom malware in memory across multiple Windows systems in an enterprise environment
2.	Hunt through and perform incident response across hundreds of unique systems simultaneously using PowerShell or F-Response Enterprise and the SIFT Workstation
3.	Identify and track malware beaconing outbound to its command and control (C2) channel via memory forensics, registry analysis, and network connection residue

Objective:	
Sl. No.	
1.	Understand how the attacker can acquire legitimate credentials-including domain administrator rights-even in a locked-down environment
2.	Use collected data to perform effective remediation across the entire enterprise
3.	Recover and analyze archives and .rar files used by APT-like attackers to exfiltrate sensitive data from the enterprise network

Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Advanced Incident Response & Threat Hunting** Real Incident Response Tactics; Threat Hunting; Threat Hunting in the Enterprise;Incident Response and Hunting across Endpoints; Malware Defense Evasion and Identification; Malware Persistence Identification; Investigating WMI-Based Attacks	**9**	**17**
02	**Intrusion Analysis** Stealing and Utilization of Legitimate Credentials; Advanced Evidence of Execution Detection; Lateral Movement Adversary Tactics, Techniques, and Procedures (TTPs); Log Analysis for Incident Responders and Hunters	**9**	**18**
03	**Timeline Analysis**Timeline Analysis Overview; Memory Analysis Timeline Creation; Filesystem Timeline Creation and Analysis; Super	**9**	**17**

	Timeline Creation and Analysis		
04	**Memory Forensics in Incident Response & Threat Hunting** Remote and Enterprise Incident Response; Triage and Endpoint Detection and Response (EDR); Memory Acquisition; Memory Forensics Analysis Process for Response and Hunting; Memory Forensics Examinations; Memory Analysis Tools	**9**	**18**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Practical:

Skills to be developed:

Intellectual skills:

1. Detect how and when a breach occurred
2. Identify compromised and affected systems
3. Perform damage assessments and determine what was stolen or changed
4. Contain and remediate incidents
5. Develop key sources of threat intelligence

List of Practical: Based on theory lectures.

Assignments:

Adhered to theory curriculum as conducted by the subject teacher.

List of Books

Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
Peter H. Gregory	Threat Hunting For Dummies®, Carbon Black Special Edition	ISBN: 978-1-119-31701-2 (pbk); ISBN: 978-1-119-31703-6 (ebk)	John Wiley & Sons, Inc.
Reference Books:			
Michael Collins	Threat Hunting	ISBN: 9781492028260	O'Reilly Media, Inc.

List of equipment/apparatus for laboratory experiments:

Sl. No.	
1.	Computer

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)	**Subjective Questions**

		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 5**	**10**	**10**				
B	**1 to 5**			**5**	**3**	**5**	**60**
C	**1 to 5**			**5**	**3**	**15**	

- Only multiple choice type questions (MCQ) with one correct answer are to be set in the objective part.
- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Examination Scheme for Practical Sessional examination:

Practical Internal Sessional Continuous Evaluation

Internal Examination:

Continuous evaluation			**40**

External Examination: Examiner-

Signed Lab Assignments	**10**	
On Spot Experiment	**40**	
Viva voce	**10**	**60**

Name of the Course: B.Sc. in Information Technology (Cyber Security) **Subject: Cyber Security Vulnerabilities & Cyber Security Safeguards**	
Course Code: BITCS403	**Semester: IV**
Duration: 36 Hrs.	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial: 1 hr./week	**Attendance : 5**
Practical: 0	**Continuous Assessment: 25**
Credit: 4	**Practical Sessional internal continuous evaluation: NA**
	Practical Sessional external examination: NA

Aim:	
Sl. No.	
1.	To learn foundations of Cyber Security and Ethical Hacking analysis using programming languages like python.
2.	To learn various types of algorithms and its applications of Cyber Security and Ethical Hacking using forensic detection
3.	To learn python toolkit for required for programming Cyber Security, Ethical Hacking concepts
4.	To understand the concepts of Cyber Security, Ethical Hacking Forensic detection image processing, pattern recognition, and natural language processing.
Objective:	
Sl. No.	
1.	Understand, appreciate, employ, design and implement appropriate security technologies and policies to protect computers and digital information.
2.	Identify & Evaluate Information Security threats and vulnerabilities in Information Systems and apply security measures to real time
3.	Identify common trade-offs and compromises that are made in the design and development process of Information
4.	Demonstrate the use of standards and cyber laws to enhance information security in the development process and infrastructure protection.

Contents		**4 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Introduction to Cyber Security** Overview of Cyber Security, Internet Governance – Challenges and Constraints, Cyber Threats:- Cyber Warfare-Cyber Crime-Cyber terrorism-Cyber Espionage, Need for a Comprehensive Cyber Security Policy, Need for a Nodal Authority, Need for an International convention on Cyberspace.	**7**	**10**
02	**Cyber Security Vulnerabilities and Cyber Security Safeguards** Cyber Security Vulnerabilities-Overview, vulnerabilities in software,	**5**	**10**

	System administration, Complex Network Architectures, Open Access to Organizational Data, Weak Authentication, Unprotected Broadband communications, Poor Cyber Security Awareness. Cyber Security Safeguards- Overview, Access control, Audit, Authentication, Biometrics, Cryptography, Deception, Denial of Service Filters, Ethical Hacking, Firewalls, Intrusion Detection Systems, Response, Scanning, Security policy, Threat Management		
03	**Securing Web Application, Services and Servers** Introduction, Basic security for HTTP Applications and Services, Basic Security for SOAP Services, Identity Management and Web Services, Authorization Patterns, Security Considerations, Challenges.	**5**	**10**
04	**Intrusion Detection and Prevention** Intrusion, Physical Theft, Abuse of Privileges, Unauthorized Access by Outsider, Malware infection, Intrusion detection and Prevention Techniques, Anti-Malware software, Network based Intrusion detection Systems, Network based Intrusion Prevention Systems, Host based Intrusion prevention Systems, Security Information Management, Network Session Analysis, System Integrity Validation.	**6**	**10**
05	**Cryptography and Network Security** Introduction to Cryptography, Symmetric key Cryptography, Asymmetric key Cryptography, Message Authentication, Digital Signatures, Applications of Cryptography. Overview of Firewalls-Types of Firewalls, User Management, VPN Security Security Protocols: - security at the Application Layer- PGP and S/MIME, Security at Transport Layer- SSL and TLS, Security at Network Layer-IPSec.	**5**	**10**
06	**Cyberspace and the Law** Introduction, Cyber Security Regulations, Roles of International Law, the state and Private Sector in Cyberspace, Cyber Security Standards. The INDIAN Cyberspace, National Cyber Security Policy 2013.	**5**	**10**
07	**Cyber Forensics** Introduction to Cyber Forensics, Handling Preliminary Investigations, Controlling an Investigation, Conducting disk-based analysis, Investigating Information-hiding, Scrutinizing E-mail, Validating E-mail header information, Tracing Internet access, Tracing memory in real-time.	**3**	**10**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

List of Books

Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
ErdalOzkaya, MiladAslaner	Hands-On Cybersecurity for Finance: Identify vulnerabilities and secure your financial services from security breaches	1 edition	Packt Publishing
Lester Evans	Cybersecurity: An Essential Guide to Computer and Cyber Security for Beginners, Including Ethical Hacking, Risk Assessment, Social Engineering, Attack and Defense Strategies, and Cyberwarfare	**ISBN-10:** 1791553583 **ISBN-13:** 978-1791553586	Independently published
Reference Books:			
Edward G. Amoroso, Matthew E. Amoroso	From CIA to APT: An Introduction to Cyber Security	**ISBN-10:** 1522074945 **ISBN-13:** 978-1522074946	Independently published
Brian Walker	Cyber Security: Comprehensive Beginners Guide to Learn the Basics and Effective Methods of Cyber Security	ISBN-10: 1075257670 ISBN-13: 978-1075257674	Independently published

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 5**	**10**	**10**				

B	**1 to 5**			**5**	**3**	**5**	**60**
C	**1 to 5**			**5**	**3**	**15**	

- Only multiple choice type questions (MCQ) with one correct answer are to be set in the objective part.
- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Name of the Course: B.Sc. in Information Technology (Cyber Security) **Subject: Network Security**	
Course Code: BITCS404	**Semester: IV**
Duration: 36 Hrs.	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial: 1 hr./week	**Attendance : 5**
Practical: 0	**Continuous Assessment: 25**
Credit: 4	**Practical Sessional internal continuous evaluation: NA**
	Practical Sessional external examination: NA

Aim:	
Sl. No.	
1.	To develop basic skills of secure network architecture and explain the theory behind the security of different cryptographic algorithms.
2.	To describe common network vulnerabilities and attacks, defense mechanisms against network attacks, and cryptographic protection mechanisms.
3.	To study about message authentication and hash functions

Objective:	
Sl. No.	
1.	Classify the symmetric encryption techniques
2.	Illustrate various Public key cryptographic techniques
3.	Evaluate the authentication and hash algorithms.
4.	Summarize the intrusion detection and its solutions to overcome the attacks. Basic concepts of system level security

Contents		**Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Security in Computing Environment** Need for Security, Security Attack, Security Services, Information Security, Methods of Protection.	**4**	**7**
02	**Basics of Cryptography [3L]** Terminologies used in Cryptography, Substitution Techniques, Transposition Techniques.	**4**	**8**
03	**Encryption and Decryption** Characteristics of Good Encryption Technique, Properties of Trustworthy Encryption Systems, Types of Encryption Systems, Confusion and Diffusion, Cryptanalysis.	**4**	**8**
04	**Key Encryption** Data Encryption Standard (DES) Algorithm, Double and Triple DES, Security of the DES, Advanced Encryption Standard (AES) Algorithm, DES and AES Comparison. Characteristics of Public Key System, RSA Technique, Key Exchange, Diffie-Hellman Scheme, Cryptographic	**4**	**8**

	Hash Functions, Digital Signature, Certificates, Certificate Authorities		
05	**Network Security** Network Concepts, Threats in Networks, Network Security Controls.	**4**	**8**
06	**IP Security** Overview of IP Security (IPSec), IP Security Architecture, Modes of Operation, Security Associations (SA), Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Key Exchange.	**4**	**8**
07	**Web Security** Web Security Requirements, Secure Socket Layer (SSL), Transport Layer Security (TLS), Secure Electronic Transaction (SET).	**4**	**7**
08	**Electronic Mail Security** Threats to E-Mail, Requirements and Solutions, Encryption for Secure E-Mail, Secure E-Mail System.	**4**	**8**
09	**Firewalls** Firewalls – Types, Comparison of Firewall Types, Firewall Configurations	**4**	**8**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

List of Books

Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
Larry L. Peterson, Bruce S. Davie	Computer Networks: A Systems Approach	Fifth	Morgan Kaufmann Publishers
James F. Kurose, Keith W. Ross	Computer Networking – A Top-Down Approach Featuring the Internet	Fifth	Pearson Education

Reference Books:

William Stallings	Cryptography and network security: principles and practice		Pearson Education
Roberta Bragg, Mark Rhodes-Ousley	Network Security: The Complete Reference		TMH

End Semester Examination Scheme. Maximum Marks-70. Time allotted-3hrs.

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks

A	**1 to 9**	**10**	**10**				**60**
B	**1 to 9**			**5**	**3**	**5**	
C	**1 to 9**			**5**	**3**	**15**	

- Only multiple choice type questions (MCQ) with one correct answer are to be set in the objective part.
- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Name of the Course: B.Sc. in Information Technology (Cyber Security) **Subject: Intrusion Detection and Prevention**	
Course Code: BITCS405	**Semester: IV**
Duration: 36 Hrs.	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial: 1 hr./week	**Attendance : 5**
Practical: 0	**Continuous Assessment: 25**
Credit: 4	**Practical Sessional internal continuous evaluation: NA**
	Practical Sessional external examination: NA

Aim:

Sl. No.	
1.	Introduce students to need for Intrusion Detection Systems.
2.	Introduce students to different techniques for Intrusion Detection.
3.	Enable students to use various tools for Intrusion Detection Mechanisms.

Objective:

Sl. No.	
1.	Realize the research aspects in the field of intrusion detection systems.
2.	Optimize performance of detection systems by employing various machine learning techniques.
3.	Apply knowledge of machine learning in system and network protection.

Contents		**4 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**INTRODUCTION:** Understanding Intrusion Detection – Intrusion detection and prevention basics – IDS and IPS analysis schemes, Attacks, Detection approaches –Misuse detection – anomaly detection – specification based detection – hybrid detection THEORETICAL FOUNDATIONS OF DETECTION: Taxonomy of anomaly detection system – fuzzy logic – Bayes theorem – Artificial Neural networks – Support vector machine – Evolutionary computation – Association rules – Clustering	**7**	**14**
02	**ARCHITECTURE AND IMPLEMENTATION:** Centralized – Distributed – Cooperative Intrusion Detection – Tiered architecture	**7**	**14**
03	**JUSTIFYING INTRUSION DETECTION:** Intrusion detection in security – Threat Briefing –Quantifying risk – Return on Investment (ROI)	**8**	**14**
04	**APPLICATIONS AND TOOLS:** Tool Selection and Acquisition Process – Bro Intrusion Detection – Prelude Intrusion Detection – Cisco Security IDS – Snorts Intrusion Detection – NFR security	**7**	**14**

05	**LEGAL ISSUES AND ORGANIZATIONS STANDARDS:** Law Enforcement / Criminal Prosecutions – Standard of Due Care – Evidentiary Issues, Organizations and Standardizations.	**7**	**14**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

List of Books

Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
RafeeqRehman	Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID	First	Prentice Hall
Carl Enrolf, Eugene Schultz, Jim Mellander	Intrusion detection and Prevention		McGraw Hill
Earl Carter, Jonathan Hogue	Intrusion Prevention Fundamentals		Pearson Education
Reference Books:			
Ali A. Ghorbani, Wei Lu	Network Intrusion Detection and Prevention: Concepts and Technique**s**		Springer
Paul E. Proctor	The Practical Intrusion Detection Handbook		Prentice Hall
AnkitFadia and MnuZacharia	Intrusiion Alert		Vikas Publishing house Pvt

End Semester Examination Scheme. **Maximum Marks-70.** **Time allotted-3hrs.**

Group	**Unit**	**Objective Questions** (MCQ only with the correct answer)		**Subjective Questions**			
		No of question to be set	Total Marks	No of question to be set	To answer	Marks per question	Total Marks
A	**1 to 5**	**10**	**10**				
B	**1 to 5**			**5**	**3**	**5**	**60**
C	**1 to 5**			**5**	**3**	**15**	

- Only multiple choice type questions (MCQ) with one correct answer are to be set in the objective part.

- Specific instruction to the students to maintain the order in answering objective questions should be given on top of the question paper.

Examination Scheme for end semester examination:

Group	**Chapter**	**Marks of each question**	**Question to be set**	**Question to be answered**
A	**All**	**1**	**10**	**10**
B	**All**	**5**	**5**	**3**
C	**All**	**15**	**5**	**3**

Name of the Course: B.Sc. in Information Technology (Cyber Security) **Subject: Project II**	
Course Code:BITCS481	**Semester: IV**
Duration: 36 Hrs.	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 0	**End Semester Exam: 100**
Tutorial: 0	**Attendance: 0**
Practical: 4 hrs./week	**Continuous Assessment: 0**
Credit: 2	**Practical Sessional internal continuous evaluation: 40**
	Practical Sessional external examination: 60
Contents	
Students will do projects on application areas of latest technologies and current topics of societal relevance.	