Department of Information Technology (In-house)

B.Sc. in Information Technology (Cyber Security)

(Effective from academic session 2019-20)

Semester-VI

Name of the Course: B.Sc. in Information Technology (Cyber Security) **Subject: Security Assessment and Risk Analysis**	
Course Code: BITCS601A	**Semester: VI**
Duration: 36 Hrs.	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial: 0	**Attendance : 5**
Practical: 0	**Continuous Assessment: 25**
Credit: 3	**Practical Sessional internal continuous evaluation: NA**
	Practical Sessional external examination: NA

Aim:	
Sl. No.	
1.	It will provide a background in the many aspects of security management associated with today's modern communications and networks
2.	It includes the fundamentals of Risk Analysis, Risk Management, Security Policy, Security Operations, Legal issues, Business issues and Secure Systems Development.

Objective:	
Sl. No.	
1.	Understand the role of Security Management in information technology
2.	Quantify the properties of Information Security systems
3.	Develop project plans for secure complex systems with knowledge of SANS 20 critical controls
4.	Demonstrate understanding of the role of firewalls, guards, proxy servers and intrusion detection in networks on a Linux OS with traffic analysis
5.	Evaluate the residual risk of a protected network

Pre-Requisite:	
Sl. No.	
1.	Application of cryptography

Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Risk Assessment** Understand the principles and terminology of risk; Probability, Likelihood, Threat, Vulnerability, Impact , Threat actor, Risk owner, Understand and describe the five key steps in risk management: Identify assets Identify threats and vulnerabilities, Assess the impact of threats and vulnerabilities on an organisation Identify ways to manage those threats and vulnerabilities, Monitor and report on risk management action, Discuss qualitative and quantitative approaches to risk assessment; Quantitative approaches (such as loss expectancy approaches (SLE/ARO)), Quantitative scalar approaches (such as High/Medium/Low), Illustrate how the results of an assessment can be presented; Financial impact, Dashboards, Heat maps, RAG.	**12**	**23**
02	**Risk Assessment: Threat and Vulnerabilities** Define and state the differences between: Threat, Vulnerability, Exploit, Attack, Describe and explain the following: Categories of threats The concept of a threat lifecycle The use of threat	**12**	**23**

	intelligence in an organisation. The uses of attribution, Discuss vulnerabilities, especially those relating to people and staff. Apprentices will understand how they can be exploited to attack an organisation; Phishing, Social engineering, Blended attacks, Describe common methods for finding vulnerabilities; Penetration testing Phishing simulators Social engineering attacks		
03	**Risk Assessment: Standards** Explain that risk assessment can be carried out using several methodologies or frameworks, but that it is better to select one methodology or framework for consistent and comparable results, List the common risk assessment methodologies or frameworks; ISO/IEC 27005, NIST, Risk Management, Framework, OCTAVE, FAIR, Compare common risk methodologies/frameworks; highlighting similarities and differences. Demonstrate how to select and then apply a risk methodology/framework in an organisation.	**12**	**24**
	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
Mark Ryan M. Talabis and Jason L. Martin	Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis		Syngress, 2012
Reference Books:			
Douglas J. Landoll	The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments		CRC Press, 2011

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	**1,2,3**	**10**	**10**				
B	**1,2,3**			**5**	**3**	**5**	**60**
C	**1,2,3**			**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: Malware Detection**	
Course Code: BITCS601B	**Semester: VI**
Duration: 36 Hrs.	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial: 0	**Attendance : 5**
Practical: 0	**Continuous Assessment: 25**
Credit: 3	**Practical Sessional internal continuous evaluation: NA**
	Practical Sessional external examination: NA

Aim:	
Sl. No.	
1.	Possess the skills necessary to carry out independent analysis of modern malware samples using both static and dynamic analysis techniques.
2.	Have an intimate understanding of executable formats, Windows internals and API, and analysis techniques.
3.	Extract investigative leads from host and network¬based indicators associated with a malicious program
4.	Apply techniques and concepts to unpack, extract, decrypt, or bypass new anti¬analysis techniques in future malware samples

Objective:	
Sl. No.	
1.	To understand of operating system and malware.
2.	Able to analize static and dynamic analysis of malware.

Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**INTRODUCTION** Introduction to malware, OS security concepts, malware threats, evolution of malware, malware types viruses, worms, rootkits, Trojans, bots, spyware, adware, logic bombs, malware analysis, static malware analysis, dynamic malware analysis	**7**	**14**
02	**STATIC ANALYSIS** X86 Architecture- Main Memory, Instructions, Opcodes and Endianness, Operands, Registers, Simple Instructions, The Stack, Conditionals, Branching, Rep Instructions, C Main Method and Offsets. Antivirus Scanning, Fingerprint for Malware, Portable Executable File Format, The PE File Headers and Sections, The Structure of a Virtual Machine, Reverse Engineering- x86 Architecture, recognizing c code constructs in assembly, c++ analysis, Analyzing Windows programs, Anti-static analysis techniques obfuscation, packing, metamorphism, polymorphism.	**7**	**14**
03	**DYNAMIC ANALYSIS** Live malware analysis, dead malware analysis, analyzing traces of malware- system-calls, api-calls, registries, network activities. Anti-dynamic analysis techniquesanti-vm, runtime-evasion techniques, , Malware Sandbox, Monitoring with Process Monitor, Packet Sniffing with Wireshark, Kernel vs. User-	**7**	**14**

	Mode Debugging, OllyDbg, Breakpoints, Tracing, Exception Handling, Patching		
04	**Malware Functionality** Downloader, Backdoors, Credential Stealers, Persistence Mechanisms, Privilege Escalation, Covert malware launching-Launchers, Process Injection, Process Replacement, Hook Injection, Detours, APC injection.	**7**	**14**
05	**Malware Detection Techniques & Android Malware** Signature-based techniques: malware signatures, packed malware signature, metamorphic and polymorphic malware signature Non-signature based techniques: similarity-based techniques, machine-learning methods, invariant inferences Malware Characterization, Case Studies – Plankton, DroidKungFu, AnserverBot, Smartphone (Apps) Security	**8**	**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
Michael Davis, Sean Bodmer, Aaron Lemasters	Hacking exposed™ malware & rootkits: malware & rootkits security secrets & Solutions	ISBN: 978-0-07-159119-5	McGraw-Hill
Filiol	Computer viruses: from theory to applications		Eric Springer Science & Business Media, 2006

Reference Books:

Xuxian Jiang and Yajin Zhou	Android Malware	ISBN 978-1-4614-7393-0	Springer
Michael Sikorski and Andrew Honig	Practical malware analysis The Hands-On Guide to Dissecting Malicious Software	ISBN-10: 159327-290-1	

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: ML for Security**	
Course Code: BITCS601C	**Semester: VI**
Duration: 36 Hrs.	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial: 0	**Attendance : 5**
Practical: 0	**Continuous Assessment: 25**
Credit: 3	**Practical Sessional internal continuous evaluation: NA**
	Practical Sessional external examination: NA

Aim:	
Sl. No.	
1.	To discuss the relationship between AI/ML and security/privacy;
2.	To identity how AI/ML can be used to launch cyber-attacks;
3.	To identify use cases for incorporating AI/ML for security and trust;
4.	To identify use cases for defining security and trust of AI/ML;

Objective:	
Sl. No.	
1.	Identify security requirements and capabilities of AI/ML enabled applications and services;
2.	Identify security requirements and capabilities for security applications and services incorporating AI/ML
3.	Able to identify ways forward for SG17 to undertake in its future study, including potential new work items.

Pre-Requisite:	
Sl. No.	
1.	**AI and ML**

Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Introduction** Overview of information security, current security landscape, the case for security data mining Supervised Learning (Regression/Classification); Basic methods: Distance-based methods, Nearest-Neighbours, Decision Trees, Naive Bayes; Linear models: Linear Regression, Logistic Regression, Generalized Linear Models; Support Vector Machines, Nonlinearity and Kernel Methods; Beyond Binary Classification: Multi-class/Structured Outputs, Ranking	**12**	**23**
02	**Clustering and Learning** Unsupervised Learning Clustering: K-means/Kernel K-means; Dimensionality Reduction: PCA and kernel PCA; Matrix Factorization and Matrix Completion; Generative Models (mixture models and latent factor models);Evaluating Machine Learning algorithms and Model Selection, Introduction to Statistical Learning Theory, Ensemble Methods (Boosting, Bagging, Random Forests) Sparse Modeling and Estimation, Modeling Sequence/Time-Series Data, Deep Learning and Feature Representation Learning	**12**	**24**

03	**Advance Learning and Security** Scalable Machine Learning (Online and Distributed Learning) A selection from some other advanced topics, Semi-supervised Learning, Active Learning, Reinforcement Learning, Inference in Graphical Models, Introduction to Bayesian Learning and Inference; Anomaly Detection, Evasion Attacks, Membership Inference,MalwareAnalysis,Model Stealing & Watermarking, Poisoning, Network Traffic Analysis, Generative Adversarial Networks, Differential Privacy,Variational Auto-Encoders	**12**	**23**
	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**
K.P. Soman, R.Loganathan, V.Ajay	Machine Learning with SVM and other Kernel methods		PHI Learning Private Limited,2009.
ShaiShalev-Shwartz, Shai Ben-David	Understanding Machine Learning: From Theory to Algorithms	1 edition	Cambridge University Press;
Reference Books:			
Kevin Murphy	Machine Learning: A Probabilistic Perspective		MIT Press, 2012
Trevor Hastie, Robert Tibshirani, Jerome Friedman	The Elements of Statistical Learning		Springer 2009
Christopher Bishop	Pattern Recognition and Machine Learning		Springer, 2007

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	**1,2,3**	**10**	**10**				
B	**1,2,3**			**5**	**3**	**5**	**60**
C	**1,2,3**			**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:

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)

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: Image Processing and Security**	
Course Code: BITCS601D	**Semester: VI**
Duration: 36 Hrs.	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 3 hrs./week	**End Semester Exam: 70**
Tutorial: 0	**Attendance : 5**
Practical: 0	**Continuous Assessment: 25**
Credit: 3	**Practical Sessional internal continuous evaluation: NA**
	Practical Sessional external examination: NA

Aim:	
Sl. No.	
1.	To learn basic concepts of image processing, fundamentals and mathematical models in digital image and video processing.
2.	To study different types of image transforms for image processing and security.
3.	To develop time and frequency domain techniques for image enhancement.
4.	To understand Image segmentation, restoration, and morphological signal Processing with applications security.

Objective:	
Sl. No.	
1.	To develop any image processing application.
2.	To understand the rapid advances in Machine vision.
3.	To learn different techniques employed for the enhancement of images.
4.	Able to learn different causes for image degradation and overview of image restoration techniques.

Pre-Requisite:	
Sl. No.	
1.	Basic Mathematics

Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Image Representation &Modeling** The Human Eye-Brain System As A Model, Image Formation, Image Models, Basic Image Processing: Sampling and Quantization, Brightness and Colour, Histogram, Filters and Convolution, Frequency Domain Processing, Edge Detection, Boundaries and Line Extraction, Segmentation and Feature Extraction, 2-D Shape Representation and Matching.3-D Representation and Matching, Visual Perception – The Human Eye, How It Works and Fails, Image Hardware and Software – Cameras, Displays, Frame Grabbers, Image Processing Architectures, Image Formation – 2d Image Acquisition and Sampling Theory.	**18**	**35**
02	**Image Transforms** Fourier Transform, Application and Use, Wavelet Trans, Hadamard Cosine Transform, Image Enhancement – Point and Region Operators, Unsharp Masking, Image Compression – Jpeg, Mpeg. Image Restoration – Direct, Inverse, Pseudo-Inverse, Blurring (Spatial Motion), Implementations – Software and Hardware, Image Interpretation – Edge Detection, Feature Extraction, Template	**18**	**35**

	Matching, Hough Transform.		
	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**
Feng Liu, Wei Qi Yan	Visual Cryptography for Image Processing and Security: Theory, Methods, and Applications	2nd edition	Springer

Reference Books:

Bernd Jähne	Digital Image Processing and Image Formation	7th edition	Springer

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	**1,2**	**10**	**10**				
B	**1,2**			**5**	**3**	**5**	**60**
C	**1,2**			**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**

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)

Name of the Course: B.Sc. in Information Technology (Cyber Security) **Subject: Biometric Security**	
Course Code: BITCS602	**Semester: VI**
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.	Demonstrate knowledge of the basic physical and biological science and engineering principles underlying biometric systems
2.	Understand and analyze biometric systems at the component level and be able to analyze and design basic biometric system applications
3.	Be able to work effectively in teams and express their work and ideas orally and in writing.
4.	Identify the sociological and acceptance issues associated with the design and implementation of biometric systems
5.	Understand various Biometric security issues

Objective:	
Sl. No.	
1.	To provide students with understanding of biometrics, biometric equipment and standards applied to security.

Pre-Requisite:	
Sl. No.	
1.	Fundamental knowledge in Biometrics

Contents		**4 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Overview of Biometrics** Definitions, biometric modalities, basic applications, access control, security	**7**	**14**
02	**Biometric System Architecture** Scanning/digitizing, enhancement, feature extraction, classification, matching, searching and verification.	**7**	**14**
03	**Probability, statistics and estimation Random variables** Discrete and continuous distribution - pattern classification and recognition - Signals in time and frequency domain – multivariate statistical analysis.	**8**	**14**
04	**Algorithms** Face recognition Voice Recognition Fingerprint Recognition Iris Recognition Other biometric modalities: Retina, signature, hand geometry, gait, keystroke Quantitative analysis on the biometrics, Performance evaluation in Biometrics – false acceptance rate; false rejection rate.	**7**	**14**
05	**Multimodal Biometric systems** Biometric system integration, multimodal biometric systems: theory and applications, performance evaluation of multimodal biometric	**7**	**14**

	systems. Biometric System Security: Biometric attacks/tampering; solutions; biometric encryption		
	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**
Benjamin Muller	Security, Risk and the Biometric State: Governing Borders and Bodies	1st Edition	Routledge, 2010
Anil K jain, Patrick Flynn, Arun A.	Handbook of Biometrics		Springer, 2008
Reference Books:			
Julian D. M. Ashbourn	Biometrics: Advanced Identify Verification: The Complete Guide		Springer-verlag, 2000
: J. Wayman, A. Jain, D. Maltoni and D. Maio	Biometric Systems: Technology, Design and Performance Evaluation		Springer, 2005

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**

Name of the Course: B.Sc. in Information Technology (Cyber Security) **Subject: Blockchain and Crypto currency**	
Course Code: BITCS603	**Semester: VI**
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.	Explain cryptographic building blocks and reason about their security
2.	Define Bitcoin's consensus mechanism
3.	Learn how the individual components of the Bitcoin protocol make the whole system works: transactions, script, blocks, and the peer-to-peer network
4.	Define how mining can be re-designed in alternative cryptocurrencies

Objective:	
Sl. No.	
1.	To learn Blockchain systems: Nuts and Bolts
2.	Able to analyse Decentralized systems
3.	To understand Tokenization and ICOs
4.	To describe Cryptography of Blockchain

Pre-Requisite:	
Sl. No.	
1.	Database System
2.	Cryptography
3.	Basic Financial Knowledge

Contents		**4 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**INTRODUCTION** Need for Distributed Record Keeping, Modeling faults and adversaries, Byzantine Generals problem, Consensus algorithms and their scalability problems, Why Nakamoto Came up with Blockchain based cryptocurrency? Technologies Borrowed in Blockchain – hash pointers, consensus, byzantine fault-tolerant distributed computing, digital cash etc.	**6**	**10**
02	**Basic Distributed Computing** Atomic Broadcast, Consensus, Byzantine Models of fault tolerance	**6**	**10**
03	**Basic Crypto primitives** Hash functions, Puzzle friendly Hash, Collison resistant hash, digital signatures, public key crypto, verifiable random functions, Zero-knowledge systems	**6**	**15**
04	**Blockchain 1.0** Bitcoinblockchain, the challenges, and solutions, proof of work, Proof	**6**	**10**

	of stake, alternatives to Bitcoin consensus, Bitcoin scripting language and their use		
05	**Blockchain 2.0** Ethereum and Smart Contracts, The Turing Completeness of Smart Contract Languages and verification challenges, Using smart contracts to enforce legal contracts, comparing Bitcoin scripting vs. Ethereum Smart Contracts	**3**	**5**
05	**Blockchain 3.0** Hyperledger fabric, the plug and play platform and mechanisms in permissioned blockchain	**3**	**10**
06	**Privacy, Security issues in Blockchain** Pseudo-anonymity vs. anonymity, Zcash and Zk-SNARKS for anonymity preservation, attacks on Blockchains – such as Sybil attacks, selfish mining, 51% attacks - -advent of algorand, and Sharding based consensus algorithms to prevent these	**6**	**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
Don Tapscott , Alex Tapscott	Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World Paperback		
Reference Books:			
William Mougayar	The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology		Wiley

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 6**	**10**	**10**				

B **C**	**1 to 6** **1 to 6**			**5** **5**	**3** **3**	**5** **15**	**60**

- 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: Grand Viva**	
Course Code:BITCS681	**Semester: VI**
Duration: 36 Hrs.	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 0	**End Semester Exam: 100**
Tutorial: 0	**Attendance: 0**
Practical: 2 hrs./week	**Continuous Assessment: 0**
Credit: 1	**Practical Sessional internal continuous evaluation: 0**
	Practical Sessional external examination: 0
Contents	
Students will give a viva from all the subject that they have covered in the course.	

Name of the Course: B.Sc. in Information Technology (Cyber Security) **Subject: Major Project II**	
Course Code: BITCS682	**Semester: VI**
Duration: 36 Hrs.	**Maximum Marks: 100**
Teaching Scheme	**Examination Scheme**
Theory: 0	**End Semester Exam: 100**
Tutorial: 0	**Attendance: 0**
Practical: 8 hrs./week	**Continuous Assessment: 0**
Credit: 4	**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.	