Department of Information Technology (In-house)

B.Sc. in Information Technology (Cyber Security)

(Effective from academic session 2019-20)

Semester-V

Name of the Course: B.Sc. in Information Technology (Cyber Security) **Subject: Digital Forensics & Digital Forensics Lab**	
Course Code: BITCS501 & BITCS591	**Semester: V**
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.	To provide computer forensics systems
2.	To provide an understanding Computer forensics fundamentals
3.	To analyze various computer forensics technologies

Objective:	
Sl. No.	
1.	To identify methods for data recovery.
2.	To apply the methods for preservation of digital evidence.

Pre-Requisite:	
Sl. No.	
1.	Database System

Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Computer Forensics Fundamentals** What is Computer Forensics?, Use of Computer Forensics in Law Enforcement, Computer Forensics Assistance to Human Resources/Employment Proceedings, Computer Forensics Services, Benefits of Professional Forensics Methodology, Steps taken by Computer Forensics Specialists Types of Computer Forensics Technology: Types of Military Computer Forensic Technology, Types of Law Enforcement — Computer Forensic Technology — Types of Business Computer Forensic Technology Computer Forensics Evidence and Capture: Data Recovery Defined — Data Back-up and Recovery — The Role of Back-up in Data Recovery — The Data-Recovery Solution.	**12**	**23**
02	**Evidence Collection and Data Seizure** Why Collect Evidence? Collection Options — Obstacles — Types of Evidence — The Rules of Evidence — Volatile Evidence — General Procedure — Collection and Archiving — Methods of Collection — Artifacts — Collection Steps — Controlling Contamination: The Chain of Custody Duplication and Preservation of Digital Evidence: Preserving the Digital Crime Scene — Computer Evidence Processing Steps — Legal Aspects of Collecting and Preserving Computer Forensic Evidence Computer Image Verification and Authentication: Special Needs of Evidential Authentication — Practical Consideration —Practical Implementation.	**12**	**23**

03	**Computer Forensics analysis and validation** Determining what data to collect and analyze, validating forensic data, addressing data-hiding techniques, and performing remote acquisitions Network Forensics: Network forensics overview, performing live acquisitions, developing standard procedures for network forensics, using network tools, examining the honeynet project. Processing Crime and Incident Scenes: Identifying digital evidence, collecting evidence in private-sector incident scenes, processing law enforcement crime scenes, preparing for a search, securing a computer incident or crime scene, seizing digital evidence at the scene, storing digital evidence, obtaining a digital hash, reviewing a case	**12**	**24**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester Examination	**4**	**30**
	Total:	**40**	**100**

Practical:

Skills to be developed:

Intellectual skills:

1. Understand the definition of computer forensics fundamentals
2. Describe the types of computer forensics technology.
3. Analyze various computer forensics systems.
4. Illustrate the methods for data recovery, evidence collection and data seizure.
5. Summarize duplication and preservation of digital evidence.

List of Practical:

Based on theory lectures.

Assignments:

Based on theory lectures.

List of Books

Text Books:

Name of Author	Title of the Book	Edition/ISSN/ISBN	Name of the Publisher
John R. Vacca	Computer Forensics, Computer Crime Investigation	2nd Edition	Firewall Media, New Delhi
Nelson, Phillips Enfinger, Steuart	Computer Forensics and Investigations		CENGAGE Learning
Reference Books:			
Keith J. Jones, Richard Bejtiich, Curtis W. Rose, Addison Wesley	Real Digital Forensics		Pearson Education
Tony Sammes and Brian Jenkinson	Forensic Compiling, A Tractitioneris Guide		Springer International edition
Christopher L.T. Brown	Computer Evidence Collection & Presentation		Firewall Media
Jesus Mena	Homeland Security, Techniques &		Firewall Media

	Technologies		
Robert M. Slade	Software Forensics Collecting Evidence from the Scene of a Digital Crime		TMH 2005

List of equipment/apparatus for laboratory experiments:

Sl. No.	
1.	Computer with Internet Connection

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**

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: Visual Cryptography**	
Course Code: BITCS502A	**Semester: V**
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 understand the fundamentals of Cryptography
2.	To acquire knowledge on standard algorithms used to provide confidentiality, integrity and authenticity.
3.	To understand the various key distribution and management schemes

Objective:	
Sl. No.	
1.	To design security applications in the field of Information technology
2.	To understand how to deploy encryption techniques to secure data in transit across data networks
3.	Analyze the vulnerabilities in any computing system and hence be able to design a security solution.

Pre-Requisite:	
Sl. No.	
1.	Cryptography

Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Introduction** Terminologies used in Cryptography; Substitution Techniques – The Caesar Cipher, One-Time Pads, The Vernam Cipher, Book Cipher; Transposition Techniques – Encipherment/Decipherment Complexity, Digrams, Trigrams, and Other Patterns.	**7**	**14**
02	**Watermarking** History of watermarking – Importance of digital watermarking – Applications – Properties – Evaluating watermarking systems. WATERMARKING MODELS & MESSAGE CODING: Notation – Communications – Communication based models – Geometric models – Mapping messages into message vectors – Error correction coding – Detecting multi-symbol watermarks.	**7**	**14**
03	**Encryption for Images**	**7**	**14**
04	**Encryption for Video**	**7**	**14**
05	**Type of Attacks** Need for Security; Security Attack – Threats, Vulnerabilities, and Controls, Types of Threats (Attacks); Security Services – Confidentiality, Integrity, Availability; Information Security; Methods	**8**	**14**

	of Protection.		
	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**
R.A. Mollin	An Introduction to Cryptography		Chapman & Hall, 2001
Silverman and Tate	Rational Points on Elliptic Curves		Springer 2005
Reference Books:			
Hankerson, Menezes, Vanstone	Guide to elliptic curve cryptography		Springer, 2004
Jones and Jones	Elementary Number Theory		Springer, 1998
Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker	Digital Watermarking and Steganography		Margan Kaufmann Publishers, New York, 2008

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: Threats in Mobile Application**	
Course Code: BITCS502 B	**Semester: V**
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.	Get to know the most important security risks (OWASP Mobile Top 10) of mobile apps with the aid of intentionally vulnerable mobile apps for iPhone and Android.
2.	Give overview of security architecture of a Mobile.

Objective:	
Sl. No.	
1.	The security architecture of Android and iOS, you will be guided through various application vulnerabilities and the corresponding countermeasures
2.	To apply what you have learned to your company's mobile application projects and will gain the competence for secure development and evaluation (self-assessment) of mobile apps

Pre-Requisite:	
Sl. No.	
1.	Good understanding of mobile devices advantageous
2.	Ability to read and understand source code

Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Software and System Security** Control hijacking attacks – buffer overflow, integer overflow, bypassing browser memory protection, Sandboxing and Isolation, Tools and techniques for writing robust application software, Security vulnerability detection tools, and techniques – program analysis (static, concolic and dynamic analysis), Privilege, access control, and Operating System Security, Exploitation techniques, and Fuzzing	**7**	**14**
02	**Network Security & Web Security** Security Issues in TCP/IP – TCP, DNS, Routing (Topics such as basic problems of security in TCP/IP,, IPsec, BGP Security, DNS Cache poisoning etc), Network Defense tools – Firewalls, Intrusion Detection, Filtering, DNSSec, NSec3, Distributed Firewalls, Intrusion Detection tools, Threat Models, Denial of Service Attacks, DOS-proof network architecture, Security architecture of World Wide Web, Security Architecture of Web Servers, and Web Clients, Web Application Security – Cross Site Scripting Attacks, Cross Site Request	**8**	**14**

	Forgery, SQL Injection Attacks, Content Security Policies (CSP) in web, Session Management and User Authentication, Session Integrity, Https, SSL/TLS, Threat Modeling, Attack Surfaces, and other comprehensive approaches to network design for security		
03	**Security in Mobile Platforms** Android vs. ioS security model, threat models, information tracking, rootkits, Threats in mobile applications, analyzer for mobile apps to discover security vulnerabilities, Viruses, spywares, and keyloggers and malware detection	**7**	**14**
04	**Introduction to Hardware Security, Supply Chain Security** Threats of Hardware Trojans and Supply Chain Security, Side Channel Analysis based Threats, and attacks	**7**	**14**
05	**Issues in Critical Infrastructure and SCADA Security** Security issues in SCADA, IP Convergence Cyber Physical System Security threats, Threat models in SCADA and various protection approaches, Machine learning and SCADA Security	**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
Scott J. Roberts, Rebekah Brown	Intelligence- Driven Incident Response: Outwitting the Adversary		O'Reilly Media, 2017
Henry Dalzie	How to Define and Build an Effective Cyber Threat Intelligence Capability		Elsevier Science & Technology, 2014
Reference Books:			
John Robertson, Ahmad Diab, Ericsson Marin, Eric Nunes, VivinPaliath, Jana Shakarian, Paulo Shakarian,	DarkWeb Cyber Threat Intelligence Mining		Cambridge University Press, 2017
Bob Gourley	The Cyber Threat		Createspace Independent Pub, 2014
Wei-Meng Lee	Beginning AndroidTM 4 Application Development		John Wiley & Sons,2017

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

Group	Unit	Objective Questions (MCQ only with the	Subjective Questions

		correct answer)					
		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:

Name of the Course: B.Sc. in Information Technology (Cyber Security) **Subject: Information and Coding Theory**	
Course Code: BITCS502 C	**Semester: V**
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.	Introduced to the basic notions of information and channel capacity.
2.	To introduce information theory, the fundamentals of error control coding techniques and their applications, and basic cryptography.
3.	To provide a complementary U/G physical layer communication
4.	To convolutional and block codes, decoding techniques, and automatic repeat request (ARQ) schemes.

Objective:	
Sl. No.	
1.	Understand how error control coding techniques are applied in communication systems.
2.	Able to understand the basic concepts of cryptography.
3.	To enhance knowledge of probabilities, entropy, measures of information.

Pre-Requisite:	
Sl. No.	
1.	Probability and Statistics

Contents		**3 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**INFORMATION ENTROPY FUNDAMENTALS** Uncertainty, Information and Entropy – Source coding Theorem – Huffman coding –Shannon Fano coding – Discrete Memory less channels – channel capacity – channel coding Theorem – Channel capacity Theorem.	**12**	**23**
02	**DATA AND VOICE CODING** Differential Pulse code Modulation – Adaptive Differential Pulse Code Modulation – Adaptive subband coding – Delta Modulation – Adaptive Delta Modulation – Coding of speech signal at low bit rates (Vocoders, LPC). Denial of Service Attacks, DOS-proof network architecture, Security architecture of World Wide Web, Security Architecture of Web Servers, and Web Clients, Web Application Security – Cross Site Scripting Attacks, Cross Site Request Forgery, SQL Injection Attacks, Content Security Policies (CSP) in web, Session Management and User Authentication, Session Integrity, Https, SSL/TLS, Threat Modeling, Attack Surfaces, and other comprehensive approaches to	**12**	**24**

	network design for security		
03	**ERROR CONTROL CODING** Linear Block codes – Syndrome Decoding – Minimum distance consideration – cyclic codes – Generator Polynomial – Parity check polynomial – Encoder for cyclic codes – calculation of syndrome – Convolutional codes.	**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
Simon Haykin	Communication Systems	4th Edition	John Wiley and Sons, 2001
Fred Halsall	Multimedia Communications, Applications Networks Protocols and Standards		Pearson Education, Asia 2002
Reference Books:			
Mark Nelson	Data Compression Book		Publication 1992
Watkinson J	Compression in Video and Audio		Focal Press, London, 1995

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**

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: Cyber Law & Cyber Crime Investigation**	
Course Code: BITCS503	**Semester: V**
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 provide knowledge related to auditing of computer systems, managing and mitigating risk situations in the organization and techniques for investigating financial frauds.
2.	To create awareness on cybercrime & IT law.
3.	Provide the assistance to handle cybercrime.
4.	To protect the girls against the cybercrime.

Objective:	
Sl. No.	
1.	This course will look at the emerging legal, policy and regulatory issues pertaining to cyberspace and cybercrimes
2.	To cover all the topics from fundamental knowledge of Information Technology and Computer Architecture so that the participant can use to understand various aspects of working of a computer.
3.	To enable the participants appreciate, evaluate and interpret the case laws with reference to the IT Act and other Laws associated with the cyberspace.
4.	To identify the emerging Cyberlaws, Cybercrime & Cyber security trends and jurisprudence impacting cyberspace in today's scenario.

Contents		**4 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Introduction to Cyberspace, Cybercrime and Cyber Law** The World Wide Web, Web Centric Business, e-Business Architecture, Models of e-Business, e-Commerce, Threats to virtual world. IT Act 2000 - Objectives, Applicability, Non-applicability, Definitions, Amendments and Limitations. Cyber Crimes- Cyber Squatting, Cyber Espionage, Cyber Warfare, Cyber Terrorism, Cyber Defamation. Social Media-Online Safety for women and children, Misuse of Private information.	**9**	**17**
02	**Regulatory Framework of Information and Technology Act 2000** Information Technology Act 2000, Digital Signature, E-Signature, Electronic Records, Electronic Evidence and Electronic Governance. Controller, Certifying Authority and Cyber Appellate Tribunal. (Rules announced under the Act), Network and Network Security, Access and Unauthorized Access, Data Security, E Contracts and E Forms.	**9**	**17**
03	**Offences and Penalties**	**9**	**18**

	Information Technology (Amendment) Act 2008 – Objective, Applicability and Jurisdiction; Various cyber-crimes under Sections 43 (a) to (j), 43A, 65, 66, 66A to 66F, 67, 67A, 67B, 70, 70A, 70B, 80 etc. along with respective penalties, punishment and fines, Penal Provisions for Phishing, Spam, Virus, Worms, Malware, Hacking, Trespass and Stalking; Human rights in cyberspace, International Co-operation in investigating cybercrimes.		
04	**Indian Evidence Act** Classification – civil, criminal cases. Essential elements of criminal law. Constitution and hierarchy of criminal courts. Criminal Procedure Code. Cognizable and non-cognizable offences. Bailable and non-bailable offences. Sentences which the court of Chief Judicial Magistrate may pass. Indian Evidence Act – Evidence and rules of relevancy in brief. Expert witness. Cross examination and re-examination of witnesses. Sections 32, 45, 46, 47, 57, 58, 60, 73, 135, 136, 137, 138, 141. Section 293 in the code of criminal procedure. Secondary EvidenceSection 65-B.	**9**	**18**
	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
Karnika Seth	Computers, Internet and New Technology Laws		Lexis NexisButtersworthWadhwa, 2012
Jonathan Rosenoer	Cyber Law: The Law of Internet		Springer- Verlag, New York, 1997
Reference Books:			
Sreenivasulu N.S	Law Relating to Intellectual Property		Patridge Publishing, 2013
PavanDuggal	Cyber Law – The Indian Perspective		Saakshar Law Publications
Harish Chander	Cyber Laws and IT Protection		PHI Learning Pvt. Ltd, 2012

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	**1,2,3,4**	**10**	**10**				
B	**1,2,3,4,**			**5**	**3**	**5**	**60**

C	**1,2,3,4**			**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: Web Application Security**	
Course Code: BITCS504	**Semester: V**
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.	Be familiar with the capabilities of various Browser Proxies
2.	Be familiar with the capabilities of various Penetration Testing tools
3.	Be prepared to detect Access Control Vulnerabilities
4.	Be prepared to detect SQL Injection Vulnerabilities

Objective:	
Sl. No.	
1.	Understand the concepts and terminology behind defensive, secure, coding
2.	Appreciate the magnitude of the problems associated with web application security and the potential risks associated with those problems
3.	Understand the use of Threat Modeling as a tool in identifying software vulnerabilities based on realistic threats against meaningful assets
4.	Understand the consequences for not properly handling untrusted data such as denial of service, cross-site scripting, and injections

Pre-Requisite:	
Sl. No.	
1.	Basic knowledge of Web Application
2.	Understanding Internet Architectures

Contents		**4 Hrs./week**	
Chapter	**Name of the Topic**	**Hours**	**Marks**
01	**Application Security** HTTPS, HSTS, SMIME, PGP, SET, E-mail and IM security, DNSSec, eSMTPS, DKIM, MARC, DNSSec, SMTP STS	**9**	**17**
02	**Secure Configuration of Applications** Security Issues in TCP/IP – Web Server, Database Server, Email Server	**9**	**18**
03	**Security protocols at application level** PGP, HTTPS, SSH, etc. Proxy or application level gateways as security devices	**9**	**17**
04	**Vulnerabilities and Countermeasures** Popular OWASP Vulnerabilities and Countermeasures	**9**	**18**
	Sub Total:	**36**	**70**
	Internal Assessment Examination & Preparation of Semester	**4**	**30**

	Examination		
	Total:	**40**	**100**

List of Books
Text Books:

Name of Author	**Title of the Book**	**Edition/ISSN/ISBN**	**Name of the Publisher**
NitesbDbanjani, Billy Rios & Brett Hardin	Hacking: The Next generation		O'reilly, 2009
Joel Scambray, Vincent Liu & Caleb Sima	Hacking Exposed Web Applications		McGraw-Hill Education, 2010

Reference Books:

Mike Shema	Seven Deadliest Web Application Attacks		Elsevier, 2010

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	**1,2,3,4**	**10**	**10**				
B	**1,3,4**			**5**	**3**	**5**	**60**
C	**1,2,3,4**			**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: Industrial Training and Internship**	
Course Code:BITCS581	**Semester: V**
Duration:	**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: NA**
	Practical Sessional external examination: 100
Contents	
Students be encouraged to go to Industrial Training/Internship for at least 2-3 months during semester break.	

Name of the Course: B.Sc. in Information Technology (Cyber Security) **Subject: Major Project I**	
Course Code:BITCS582	**Semester: V**
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.	