CYBER SECURITY

II Semester: CSE

Course Code	Category	Hours / Week			Credits	Maximum Marks		
BCSB11	Core	L	T	P	C	CIA	SEE	Total
		3	0	0	3	30	70	100
Contact Classes: 45	Total Tutorials: Nil	Total Practical Classes: Nil				Total Classes: 45		

I.COURSE OVERVIEW:

The course offers a comprehensive understanding of web security concepts, equipping students with the knowledge and skills to combat cybercrimes effectively. Students will learn to identify and analyze key components of cyber security network architecture, enabling them to design robust and secure systems.

II.OBJECTIVES:

The students will try to learn:

I. The core information assurance principles.
II. The key components of cyber security network architecture.
III. How to Apply cyber security architecture principles.
IV. The risk management processes and practices.

III.COURSE OUTCOMES:

After successful completion of the course, students should be able to:

CO 1	**Summarize** web security concepts to overcome cybercrimes.	Understand
CO 2	**Make use of** cryptography techniques for protecting systems from unauthorized access and information security.	Remember
CO 3	**Demonstrate** web hacking and cybercrime investigation tools for detecting and recovering in the web domain.	Apply
CO 4	**Identify** digital forensics procedures and policies to manage organizational security risks.	Understand
CO 5	**Recognize** database security concepts and cyber laws for data protection in digital space.	Create

IV. SYLLABUS:

UNIT-I	INTRODUCTION	Classes: 09

A web security forensic lesson, web languages, introduction to different web attacks, overview of n-tier web applications; Web servers: Apache, IIS, database servers, introduction and overview of cybercrime, nature and scope of cybercrime, types of cybercrime: social engineering, categories of cybercrime, property cybercrime.

UNIT-II	REVIEW OF COMPUTER SECURITY AND CYBER CRIME ISSUES	Classes: 09

Public key cryptography, RSA, online shopping, payment gateways, 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-III	WEB HACKING BASICS AND INVESTIGATION	Classes: 09

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

Investigation: Introduction to cybercrime investigation, investigation tools, e-discovery, digital evidence collection, evidence preservation, e-mail investigation, e-mail tracking, IP tracking, e-mail recovery, hands on case studies; Encryption and Decryption methods, search and seizure of computers, recovering deleted evidences, password cracking.

UNIT-IV	DIGITAL CERTIFICATES AND DIGITAL FORENSICS	Classes: 09

Digital certificates, hashing, message digest, and digital signatures; 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.

UNIT-V	SECURING DATABASES, LAWS AND ACTS	Classes: 09

Basics, secure JDBC, securing large applications, cyber graffiti; 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.

Text Books:

1. Mc Clure, Stuart, Saumil Shah, Shreeraj Shah, “Web Hacking: Attacks and Defense”, Addison-Wesley Professional, Illustrated Edition, 2003.
2. Garms, Jess, Daniel Somerfield, “Professional Java Security”, Wrox Press, Illustrated Edition, 2001.

Reference Books:

1. Nelson Phillips, EnfingerSteuart, “Computer Forensics and Investigations”, Cengage Learning, New Delhi, 2009.
2. Kevin Mandia, Chris Prosise, Matt Pepe, “Incident Response and Computer Forensics “, Tata McGraw Hill, 2009
3. Robert M Slade, “Software Forensics”, Tata McGraw Hill, New Delhi, 1st Edition, 2005.

Web References:

1. http://www.mail.nih.gov/user/faq/tlsssl.htm
2. http://www.openssl.org/
3. http://www.ntsecurity.net/

E-Text Books:

1. https://www.mitre.org/sites/.../pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf
2. https://www.coursera.org/specializations/cyber-security
3. https://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf