COURSE CONTENT

CYBER SECURITY								
II Semester: CSE								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
BCSE15	**Elective**	3	0	0	3	40	60	100
Contact Classes: 45	**Total Tutorials: Nil**	**Total Practical Classes: Nil**				**Total Classes: 45**		
Prerequisite: Computer Networks								

I. COURSE OVERVIEW:

This course focuses on effectively applying analytical and critical thinking to plan and execute security measures to shield an organization's computer systems, networks, and network devices from infiltration and cyber-attacks. Cyber Security course covers topics such as an overview of cybercrimes, computer security, cryptography algorithms, internet hacking and cracking, web hacking, cybercrime investigation, digital forensics and certificates, securing databases, laws, and acts. Provide career opportunities as Cyber Security Analyst, Cyber Security Practitioner, Cyber Defense Analyst, and Information Security Engineer in leading IT and Governmental Organizations.

II. COURSE OBJECTIVES:

The students will try to learn:

I. Preventing, monitoring, and responding to data breaches and cyber-attacks.
II. The core information of assurance principles.
III. The key components of cyber security network architecture.
IV. The cyber security architecture principles

III. COURSE OUTCOMES:

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

CO1	Outline web security concepts to overcome cyber crimes
CO2	Make use of cryptography techniques for protecting systems from unauthorized access and information protection
CO 3	Demonstrate cybercrime investigation tools for detecting and recovering the loss in the web domain.
CO 4	Summarize digital security procedures and policies to manage organizational security risks.
CO 5	Outline cyber laws and Acts to offer legal electric communication

IV. COURSE CONTENT:

MODULE-I: INTRODUCTION (9)

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.

MODULE-II: REVIEW OF COMPUTER SECURITY AND CYBERCRIME ISSUES (9)

Public key cryptography, RSA, online shopping, payment gateways, unauthorized access to computers, computer intrusions, white collar crimes, viruses, malicious code, internet hacking and cracking, virus attacks, pornography, software piracy, intellectual property, mail bombs, exploitation, stalking and obscenity in the internet, digital laws and legislation, law enforcement roles and responses.

MODULE-III: WEB HACKING BASICS AND INVESTIGATION (9)

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 evidence, password cracking.

MODULE-IV: DIGITAL CERTIFICATES AND DIGITAL FORENSICS (9)

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.

MODULE-V: SECURING DATABASES, LAWS AND ACTS (9)

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.

.

V TEXTBOOKS:

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”, Word Press, Illustrated Edition, 2001.

VI. REFERENCE BOOKS:

1. Nelson Phillips, Enfinger Steuart, “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.

VII. WEB REFERENCES:

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

3. http://www.ntsecurity.net/

VIII.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

IX. MATERIALS ONLINE

1. Course template
2. Tutorial question bank
3. Tech talk topics
4. Open,Ended experiments
5. Definitions and terminology
6. Assignments
7. Model question paper, I
8. Model question paper, II
9. Lecture notes
10. Power Point presentation
11. E-Learning Readiness Videos (ELRV)