INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)
Dundigal, Hyderabad - 500 043

COMPUTER SCIENCE AND ENGINEERING

COURSE DESCRIPTION FORM

Course Title	**Cyber Security**			
Course Code	BCS006			
Course Structure	Lectures	Tutorials	Practicals	Credits
	3	-	-	3
Course Coordinator	Rajasekhar Nennuri Assistant Professor			
Team of Instructors	-			

I. COURSE OVERVIEW

The course covers various web languages, web servers and types and categories of cyber crime. The course also specifies the computer security and issues in cyber crime. It also discuss about security related to applets and servlets, network security basics. Cyber crime investigation tools, encryption and decryption methods are explained.It also deals with digital forensics and act and laws of cyber crime.

II. PREREQUISITE(S)

Level	Credits	Periods/ Week	Prerequisites
PG	3	3	Fundamentals of Information Security, Basics of Java programming

III. MARKS DISTRIBUTION

Subject	SEE Examination	CIA Examination	Total Marks
Cyber Security	70 Marks	30 Marks	100 Marks

Semester End Examination 70 Marks All the Units (1, 2, 3, 4 and 5)	70 Marks (3 Hours)	5 questions to be answered. Each question carries 14 Marks

<table>
<tr><td rowspan="6">Average of two CIA Examinations</td><td colspan="4">Continuous Internal Assessment (CIA) - 1</td></tr>
<tr><td rowspan="3">30 Marks
(2 Hours)</td><td rowspan="3">Units
I, II and
III (half)</td><td rowspan="2">Continuous Internal Examination (CIE)
(2 hours)
[4 questions to be answered out of 5 questions from Part- A & B]</td><td>Part - A
5 questions to be answered out of 5 questions, each carries 1 mark.</td></tr>
<tr><td>Part - B
4 questions each carry 5 marks.</td></tr>
<tr><td>Technical Seminar and Term Paper</td><td>5 marks</td></tr>
<tr><td colspan="4">Continuous Internal Assessment (CIA) - 2</td></tr>
<tr><td rowspan="3">30 Marks
(2 Hours)</td><td rowspan="3">Units
III (half)
IV and V</td><td rowspan="2">Continuous Internal Examination (CIE)
(2 hours)
[4 questions to be answered out of 5 questions from Part- A & B]</td><td>Part – A
5 questions to be answered out of 5 questions, each</td></tr>
<tr><td>Part - B
4 questions each carry 5 marks.</td></tr>
<tr><td>Technical Seminar and Term Paper</td><td>5 marks</td></tr>
</table>

IV. EVALUATION SCHEME

S. No	Component	Duration	Marks
1	CIE - I Examination	2 hour	25
2	Technical Seminar and Term Paper	10 minutes seminar and 1000 words document	05
TOTAL			30
3	CIE - II Examination	2 hour	25
4	Technical Seminar and Term Paper	10 minutes seminar and 1000 words document	05
TOTAL			30
CIA Examination marks to be considered as average of above two CIA's			
5	EXTERNAL Examination	3 hours	70
GRAND TOTAL			100

V. COURSE OBJECTIVES

The course should enable the students to

I. Explain the core information assurance principles.
II. Identify the key components of cyber security network architecture.
III. Apply cyber security architecture principles
IV. Describe risk management processes and practices.

I. COURSE OUTCOMES

At the end of the course the students are able to:

1. **Identify** different types of web attacks.
2. **Understand** various categories of cyber crime.
3. **Design** different security algorithms.
4. **Identify** various cyber crime issues**.**
5. **Understand** the concept of security in applets and servlets .
6. **Develop** cyber crime investigation tools.
7. **Understand** about digital forensics.
8. **Evaluate** the type of forensics.
9. **Identify** the laws and acts related to cyber crime.

II. HOW PROGRAM OUTCOMES ARE ASSESSED

Program Outcomes		Level	Proficiency assessed by
PO1	**Engineering knowledge**: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.	H	Seminar
PO2	**Problem analysis**: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	H	Seminar
PO3	**Design/development of solutions**: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.	S	Projects
PO4	**Conduct investigations of complex problems**: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	H	Projects
PO5	**Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.	S	Projects
PO6	**The engineer and society**: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.	N	--
PO7	**Environment and sustainability**: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	N	--
PO8	**Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.	N	--
PO9	**Individual and team work**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	N	--
PO10	**Communication**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.	N	--

Program Outcomes		Level	Proficiency assessed by
PO11	**Project management and finance**: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.	N	--
PO12	**Life-long learning**: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.	S	Projects

III. HOW PROGRAM SPECIFIC OUTCOMES ARE ASSESSED

Program Specific Outcomes		Level	Proficiency assessed by
PSO1	**Professional Skills:** The ability to research, understand and implement computer programs in the areas related to algorithms, system software, multimedia, web design, big data analytics, and networking for efficient analysis and design of computer-based systems of varying complexity.	H	Lectures, Seminars
PSO2	**Problem-solving Skills:** The ability to apply standard practices and strategies in software project development using open-ended programming environments to deliver a quality product for business success.	S	Projects
PSO3	**Successful Career and Entrepreneurship:** The ability to employ modern computer languages, environments, and platforms in creating innovative career paths, to be an entrepreneur, and a zest for higher studies.	N	--

N - None **S - Supportive** **H - Highly related**

IV. SYLLABUS

UNIT – I

INTRODUCTION

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

UNIT-II

REVIEW OF COMPUTER SECURITY AND CYBER CRIME ISSUES

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

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 cyber crime 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

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

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 private act ,legal policies.

Text Books:

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

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 Mc Graw Hill, 3. Robert M Slade, "Software Forensics", Tata Mc Graw Hill, New Delhi, 1st Edition, 2005.

V. COURSE PLAN

At the end of the course, the students are able to achieve the following course learning outcomes.

Lecture No.	Course learning outcomes	Topics to be covered	Reference
1 – 3	**Identify** different types of web attacks	A web security forensic lesson, web languages, introduction to different web attacks	T1
4 – 6	**Understand** various categories of cyber crime. .	introduction and overview of cyber crime , types of cyber crime: social engineering, categories of cyber crime.	T1
7 – 9	**Design** different security algorithms	Public key cryptography, RSA algorithm	T1
10 – 13	**Identify** various cyber crime issues	computer intrusions, white collar crimes, viruses and malicious code, internet hacking and cracking, virus attacks, pornography,	T1
14 – 16			
17 – 20	**Understand** the concept of security in applets and servlets .	Web hacking basics HTTP and HTTPS URL, web under the cover overview of java security reading the HTML source, applet security, servlets security.	T2
21 – 22			

23 – 25	**Develop** cyber crime investigation tools.	Introduction to cyber crime investigation, investigation tools, e-discovery, digital evidence collection, evidence preservation, e-mail investigation, e-mail tracking, IP tracking, e-mail recovery.	
25 – 28			
29 – 31	**Understand** about digital forensics	Digital forensics: Introduction to digital forensics , forensic software and hardware analysis and advanced tools, forensic technology	
32 – 35			
35 – 38	**Evaluate** the type of forensics.		
39 -- 42	**Identify** the laws and acts related to cyber crime	Laws and acts: Laws and ethics, digital evidence controls, evidence handling procedures, basics of Indian Evidence Act IPC and CrPC, electronic communication	
43 – 45			

XI MAPPING COURSE OBJECTIVES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES

Course Objectives	Program Outcomes												Program Specific Outcomes		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
I	H	H										S	H	H	
II		H	S		S								S	H	
III	S	H	S										H		
IV	H	S											H	S	
V	H	S											H	S	

S - Supportive **H - Highly related**

XII MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES ANDPROGRAM SPECIFIC OUTCOMES

Course Objectives	Program Outcomes												Program Specific Outcomes		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
1	H			S									H	S	
2	S	H	S									S	H		
3	S	H			S								S		
4	H			S								S	S	S	
5	S	H	S		S							S	H		
6	H	S		S									S		
7	H				S							S	H	S	
8	H			S									H	S	
9	S	H	S									S	H		

S - Supportive **H - Highly related**

Prepared by: Rajasekhar Nennuri, Assistant Professor

HOD, CSE