Course Code: 20CS1005 **R20**

SIDDARTHA INSTITUTE OF ENGINEERING & TECHNOLOGY::
PUTTUR(AUTONOMOUS)
Siddharth Nagar, Narayanavanam Road – 517583

QUESTION BANK (DESCRIPTIVE)

Subject with Code: Cyber Crime Investigation & Digital Forensics (**20CS1005**)
Year &Sem : III B.Tech & II-Sem

Course &Branch: B.Tech - CIC
Regulation: R20

UNIT –I
INTRODUCTION

1	**a**	What is Cybercrime? Explain different classifications of Cybercrime.	[L2][CO1]	**[6M]**
	b	Illustrate the challenges and prevention of Cybercrime.	[L2][CO1]	**[6M]**
2		Explain the types of Cybercrimes in detail.	[L2][CO1]	**[12M]**
3	**a**	What do you mean by Mens Rea and Actus Reus?	[L1][CO1]	**[6M]**
	b	Summarize nature and scope of Cybercrime.	[L2][CO1]	**[6M]**
4	**a**	Classify the different social engineering attack techniques.	[L2][CO1]	**[6M]**
	b	Compare Individual and Government/Organization Cybercrime.	[L4][CO1]	**[6M]**
5	**a**	Explain the types of Individual Cybercrime.	[L6][CO1]	**[6M]**
	b	Define Tailgating, Quid Pro Quo, Vishing, Water Holing, Pretexting.	[L2][CO1]	**[6M]**
6		Demonstrate the three fragmentation of Cybercrime with a neat Flow chart.	[L3][CO1]	**[6M]**
7	**a**	Determine SQL Injections, DDOS attacks, Ransomware, Brute Force attacks.	[L5][CO1]	**[6M]**
	b	Distinguish Authentication and Authorization.	[L4][CO1]	**[6M]**
8	**a**	Define Social Engineering with examples.	[L2][CO1]	**[6M]**
	b	Differentiate Property and Individual Cybercrime.	[L3][CO1]	**[6M]**
9		Explain the categories of Cybercrime in detail.	[L6][CO1]	**[12M]**
10		Demonstrate Property Cybercrime in detail.	[L3][CO1]	**[12M]**

Course Code: 20CS1005 **R20**

UNIT –II
CYBER CRIME ISSUES

1		Explain the process of Computer Intrusion in detail.	[L5][CO4]	**[12M]**
2		Discuss in detail about Malicious code and its attack ways.	[L6][CO4]	**[12M]**
3	**a**	Explain the different strategies to prevent unauthorized access.	[L2][CO4]	**[6M]**
	b	Recall the White Collar crime. Explain its types.	[L5][CO4]	**[6M]**
4	**a**	Explain Trojans, Viruses, Worms and Backdoor attacks.	[L2][CO4]	**[6M]**
	b	Give brief description about types of Exploitation..	[L2][CO4]	**[6M]**
5		Explain in details about internet Hacking and Cracking.	[L5][CO4]	**[12M]**
6		Illustrate in brief about virus attacks.	[L2][CO4]	**[12M]**
7		Explain in detail about Software Piracy and its types.	[L2][CO4]	**[12M]**
8		Evaluate in detail about Mail Bombs.	[L5][CO4]	**[12M]**
9		Distinguish Exploitation and Stalking.	[L4][CO4]	**[12M]**
10		Estimate the different roles and responsibilities of Law enforcement against Cybercrime.	[L6][CO4]	**[12M]**

UNIT –III
INVESTIGATION

1		Illustrate in brief about the working of E-discovery.	[L2][CO3]	**[12M]**
2		Explain in detail about digital evidence collection.	[L5][CO3]	**[12M]**
3		Elaborate different Investigation Tools.	[L6][CO3]	**[12M]**
4	a	Explain the different Cybercrime Investigation technique.	[L2][CO3]	**[6M]**
	b	Write about Data Carving and its limitations.	[L2][CO3]	**[6M]**
5		Explain the recovery process of deleted evidences.	[L5][CO3]	**[12M]**
6		Demonstrate Password Cracking in detail.	[L3][CO3]	**[12M]**
7		Compare E-mail tracking and IP tracking.	[L4][CO3]	**[12M]**
8		Summarize briefly about E-mail tracking.	[L2][CO3]	**[12M]**
9		Give brief description about E-mail Investigation.	[L2][CO3]	**[12M]**
10		Discuss the various steps in preserving digital evidence.	[L6][CO3]	**[12M]**

UNIT –IV
DIGITAL FORENSICS

1		Explain the process of Digital Forensics..	[L5][CO4]	**[12M]**
2		Discuss in detail about Digital Forensics.	[L6][CO4]	**[12M]**
3	**a**	Explain Forensic Hardware and its different tools	[L2][CO4]	**[6M]**
	b	Recall the Forensic Software. Explain in detail about different Software tools.	[L5][CO4]	**[6M]**
4	**a**	Explain the different Digital Forensics Techniques.	[L2][CO4]	**[6M]**
	b	Give brief description about Digital Forensics practices.	[L2][CO4]	**[6M]**
5		Explain Forensic Ballistics in details.	[L5][CO4]	**[12M]**
6		Illustrate in brief about Windows system Forensics.	[L2][CO4]	**[12M]**
7		Explain in detail about Linux system Forensics.	[L2][CO4]	**[12M]**
8		Evaluate Finger print Recognition in detail.	[L5][CO4]	**[12M]**
9		Distinguish Face and IRIS Recognition.	[L4][CO4]	**[12M]**
10		Estimate the different Video and Audio Enhancement techniques.	[L6][CO4]	**[12M]**

Course Code: 20CS1005 **R20**

UNIT –V
ROLE OF CERT IN CYBER SECURITY

1	Explain CERT in detail.	[L2][CO5]	**[12M]**
2	Distinguish between Reactive and Proactive security.	[L4][CO5]	**[12M]**
3	Explain security quality management services.	[L2][CO5]	**[12M]**
4	Evaluate and explain the IT security policies for Government organizations.	[L5][CO5]	**[12M]**
5	Differentiate IDS and Firewall.	[L4][CO5]	**[12M]**
6	State and explain CRET-In security guidelines.	[L2][CO5]	**[12M]**
7	Estimate the strategy to give security guidelines to Web servers.	[L6][CO5]	**[12M]**
8	Illustrate the security guidelines for Network.	[L2][CO5]	**[12M]**
9	Explain in detail about the Intrusion Detection System.	[L2][CO5]	**[12M]**
10	Discuss in detail about the security guidelines for Stand Alone system.	[L6][CO5]	**[12M]**

Prepared by:
Dr.J.Maria Arockia Dass, Associate Professor, Dept. of CSE, SIETK