Basavarajeswari Group of Institutions

BALLARI INSTITUTE OF TECHNOLOGY & MANAGEMENT

(Autonomous Institute under Visvesvaraya Technological University, Belagavi)

USN											Course Code	2	1	C	S	6	5	4

Sixth Semester B.E. Degree Examination – September 2024

INTRODUCTION TO CYBER SECURITY

Duration: 3 hrs **Max. Marks: 100**

Note: 1. Answer any* FIVE *full questions choosing ONE full Question from each Module.
2. Missing data, if any, may be suitably assumed

Q. No		*Question*	*Marks*	*(RBTL:CO:PO)*
		Module-1		
1.	**a.**	Define the following terms: - i) Cybercrime ii) Cybernetics iii) Cybersquatting iv) Cyber terrorism v) Cyberwarfare.	**5**	1:1:1.2.2
	b.	Who are Cybercriminals? List and explain the categorization of cybercriminals.	**7**	2:1:1.2.2
	c.	Describe various types of Cybercrimes against an organisation.	**8**	2:1:1.2.3
		OR		
2.	**a.**	Write a short note on: i) The Legal perspectives on Cybercrime. ii) An Indian perspectives on Cybercrime.	**8**	2:1:1.4.2
	b.	Discuss the global perspectives on Cybercrimes.	**6**	2:1:1.4.2
	c.	Outline the impact of the **5P** Netizen mantra on enhancing Cyber security?	**6**	2:1:1.3.2
		Module-2		
3.	**a.**	Explain the phases involved in the planning of a Cybercrime?	**8**	2:2:1.3.1
	b.	Differentiate the Passive and Active attacks involved in a cyberattack.	**6**	2:2:1.3.2
	c.	Define social engineering. Explain types of social engineering	**6**	2:2:1.3.1
		OR		
4.	**a.**	Explain the different methods of cyberstalking.	**8**	2:2:1.3.2
	b.	Outline the safety and security measures while using the compute in a cybercafé.	**6**	2:2:1.3.1
	c.	Discuss how botnets can be used as a fuel to Cybercrimes.	**6**	2:2:1.3.1
		Module-3		
5.	**a.**	Describe the different approaches involved in password cracking.	**8**	2:3:1.2.1
	b.	Compare between a proxy server and an anonymizer.	**6**	2:3:1.2.1
	c.	Outline the concept of Trojan horses and Backdoors.	**6**	2:3:1.2.2
		OR		

6.	**a.**	Distinguish between a Virus and a Worm.	**8**	2:3:1.4.2
	b.	Define a DoS attack. List and explain different levels of DoS attacks.	**6**	2:3:1.3.2
	c.	Summarize the role of Steganography and Steganalysis in cybersecurity.	**6**	2:3:1.2.2

Module-4

7.	**a.**	Explain four types of phishing methods to reveal personal information on Internet.	**8**	2:4:1.2.1
	b.	Discuss the different phishing techniques.	**6**	2:4:1.2.2
	c.	Describe the various types of phishing scams.	**6**	2:4:1.2.2

OR

8.	**a.**	Describe the countermeasures to prevent being victim of phishing attack.	**8**	2:4:1.3.2
	b.	Outline the different types of Identity theft.	**6**	2:4:1.3.1
	c.	Discuss the countermeasures prevent being a victim of Identity theft?	**6**	2:4:1.3.2

Module-5

9.	**a.**	Define digital forensics science. Discuss the need for computer forensics in investigation of cybercrime.	**8**	2:5:1.2.2
	b.	Explain difference between forensics policy and security policy.	**6**	2:5:1.3.2
	c.	Outline the typical use cases of digital forensics.	**6**	2:5:1.4.2

OR

10	**a.**	Explain the phases in the computer forensics life cycle.	**8**	2:5:1.4.1
	b.	Outline the precautions to be taken while collecting Electronic Evidence.	**6**	2:5:1.4.2
	c.	Explain the chain custody concepts in Cyber Forensics.	**6**	2:5:1.4.2

** ** **

Note: (RBTL - Revised Bloom's Taxonomy Level: CO - Course Outcome: PI – Programme Outcome)