SES's L.S. RAHEJA COLLEGE OF ARTS AND COMMERCE (AUTONOMOUS)

BOARD OF STUDIES: Information Technology and Data Science
PROGRAMME: Bachelor of Commerce (Financial Markets)
SEMESTER: III
NOMENCLATURE OF THE COURSE: CYBER SECURITY
NEP Vertical: OE
Credit: 02

(As Per Choice Based Credit System (under NEP 2020) with effect from the academic year 2025-26)

Programme:	Bachelor of Commerce (Financial Markets)
Nomenclature of the Course	Cyber Security
Total Marks	50
Semester:	III
Academic year	2025-26

LEARNING OBJECTIVES:

1. Comprehend the fundamental concepts of cyber security and recognize the associated challenges and risks.
2. Understand the use of various tools, processes, and methods for effectively securing systems and networks.
3. Understand the principles of cryptography and its application.
4. Analyze and evaluate cyber terrorism case studies, understanding the motives, techniques involved.

COURSE OUTCOMES:

1. To understand the fundamentals of the cyber security domain and related issues.
2. To impart knowledge of various tools, processes and methods to ensure security of systems.
3. To discuss cryptography and its applications.
4. To examine various cyber terrorism cases.

Unit	Course Content	Andragogy	No of Lectures
I	**1.1 Introduction to Computer Security**: Introduction, How Seriously Should You Take Threats to Network Security? Identifying Types of Threats, Assessing the Likelihood of an Attack on Your Network, Basic Security Terminology, Concepts and Approaches, How Do Legal Issues Impact Network Security? Online Security Resources **1.2 Cyber Stalking, Fraud, and Abuse:** How Internet Fraud Works, Identity Theft, Cyber Stalking, Protecting against Investment Fraud **1.3 Malware:** Viruses, Trojan Horses, The Buffer-Overflow Attack, The Sasser Virus/Buffer Overflow, Spyware, Other Forms of Malware, Detecting and Eliminating Viruses and Spyware	• Task or problem centred • Give students problems: Provide problems for students to solve independently or in groups. • Encourage self-directed learning: Allow students to choose their learning methods and materials. • Use real-life examples: Incorporate real-life examples into lessons.	15
II	**2.1 Encryption:** Cryptography Basics, History of Encryption, Modern Methods, Legitimate Versus Fraudulent Encryption Methods, Encryptions Used in Internet, Virtual Private Networks	• Task or problem centred • Give students problems: Provide	15

	2.2 Computer Security Software: Virus Scanners, Firewalls, Antispyware, Intrusion-Detection Software and Honeypots **2.3 Cyber Terrorism and Information Warfare:** Actual Cases of Cyber Terrorism, China Eagle Union, Economic Attacks, Military Operations Attacks, General Attacks, Supervisory Control and Data Acquisitions, Information Warfare, Future Trends, Defense against Cyber Terrorism	problems for students to solve independently or in groups.	

SUGGESTED READINGS

1. Chuck Easttom, Computer Security Fundamentals, Pearson, 2011
2. Mayank Bhushan, Rajkumar Singh Rathore, Aatif Jamshed, Fundamentals of Cyber Security, 2017
3. Sunit Belapure, Nina Godbole "Cyber Security",Willey.
4. Mayank Bhushan, "Fundamentals of Cyber Security", BPS Publications.

QUESTION PAPER PATTERN

(A) FOR CONTINUOUS EVALUATION

Particulars	Marks
Presentation/Viva Voce/Quiz	10
Assignment/Project	10
Total	**20**

(B) QUESTION PAPER PATTERN FOR SEMESTER END EXAMINATION

Question No.	**Description**	**Total Marks**
Q. 1	**Attempt the following Unit I**	**15**
A	Remembering	
B	Analysing	
C	Applying	
	OR	
P	Remembering	
Q	Analysing	
R	Applying	
Q. 2	**Attempt the following Unit II**	**15**
A	Understand	
B	Applying	
C	Evaluating	
	OR	
P	Understand	
Q	Applying	
R	Evaluating	