Bachelor of Computer Application Semester – 5

Pre-requisites for the course	12th Standard in relevant Stream
Course Code	501- CYBER SECURITY 26520- BCASEC301-3C
Course Type	SEC
Credit	02
Contact Hours	02 Hours in a week
Course focussing on	Knowledge Enhancement
Relevance of course to	Global Level
Relation to	Professional Skill

Course Objectives: The course has been designed keeping in view the disciplinary or inter-disciplinary nature of the programme. It is Skill Enhancement Course (SEC) for the B.C.A. programme and also open to students of the university under choice-based credit system (CBCS). The course has been designed-

- To enable students to get basics of cyber security
- To understand basic of threats and vulnerabilities
- Understand the importance of security.

By the end of this course, students should be able to-
(i) Get an overview Cyber security

(ii) Get knowledge of cryptography

(iii) Knowledge about cyber fraud

On completion of the course students will be able to:
LO 1 –Basic concept of cyber security
LO 2 – understand the concept of Threats and vulnerabilities LO 3 – Understand about cryptography.

Teaching Methods:
Teaching will take place through lectures and interactions. For students, regular attendance and participation in the class is essential. Group and individual activities from student participants would supplement classroom engagement. ICT tools would be used extensively during teaching. Students are expected to participate actively in discussions based on their critical understanding of the assigned readings. 80% attendance is necessary to attend the end semester exam.
1 credit = 15 hours theory and 30 hours practical/practical related training
Detailed Syllabus:2 credit course

B.C.A.	Paper No: 501 – Cyber Security		
			Credits: 02
External Evaluation:25			
Internal Evaluation:25		**Duration 01:15 Hrs**	
	Course Contents	**Teaching Hours**	**Weightage of Marks**
Unit-1	**Introduction to Information Security and cryptography** • Definition of Information Security, Evolution of Information Security. • Basics Principles of Information Security (CIA triad), Terminologies in information security • Overview of Cryptography & Steganography • Understanding the AES and DSA (overview) • Private key and Public key Cryptography	15	25
Unit-2	**Threats and vulnerabilities**		
	• Introduction of Threats and vulnerabilities • Types of Hackers, Hacktivism • Common Threats to the data • Vulnerability and Penetration testing and its tools • Unauthorized access and hacking • Trojan, virus and worm attacks • Denial of services, Email spoofing, spamming, bombing, and email frauds	15	25

Mode of Evaluation:
For 2 credit course

Internal Evaluation: 25- Marks

External Evaluation : 25-Marks

List of Reference Books/e-resources/e-content

S.No	Text Books:	Author	Edition	Publication
1.	Cryptography and Network Security	Williamstallings	Fourth Edition	McGrawHill India, 2017
2.	Information security: Principles and Practice	MarkStamp	Second Edition	JohnWiley&Sons, Inc., 2011
Reference Book				
1.	Cryptography and Network Security by Ferouzan, Behrouz A.			
2.	Data and Computer Communication, Pearson Education By StallingsWilliam			
3.	Cryptography and Network Security By .Bose			
Online Resources				
1.	https://onlinecourses.swayam2.ac.in/nou19_cs08			
2.	https://www.coursera.org/learn/introduction-cybersecurity-cyber-attacks			
3.	https://www.codecademy.com/learn/introduction-to-cybersecurity			