SRI CHANDRASEKHARENDRA SARASWATHI VISWA MAHAVIDYALAYA

(Deemed to be University U/S 3 of UGC Act 1956) (Accredited with "A" Grade by NAAC)
Enathur, Kanchipuram – 631561

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CURRICULUM AND SYLLABUS FOR FULL TIME

B.E. (Hons.) Computer Science and Engineering with Specialization in Cyber Security

(Applicable for students admitted from 2025-2026 onwards)

REGULATION AY 2025-2026

B.E. (Hons.) Computer Science and Engineering with Specialization in Cyber Security

These regulations are applicable to the students admitted from the AY 2025-26 Onwards.

CHOICE BASED CREDIT SYSTEM FOR B.E. (Hons) CSE with CS FULL-TIME PROGRAMME CREDITS

Theory courses: Courses with 4/3 credits will be assigned 3 Lectures and 2/1 Tutorial hours per week.

Practical courses: Courses with 2 credits will be assigned 4 hours of lab/practical work per week

From semester III to VII, the honors. Credits distribution as follows

Sl.No	Semester	Credits
1.	III	3
2.	IV	5
3.	V	3
4.	VI	3
5.	VII	5
Total		**19**

For the award of the Hons./Minor degree, a student has to earn a minimum of 19 credits.

DURATION OF THE PROGRAMME

A student is normally expected to complete B.E. (HONS.) CSE with CS programme in four years and in any case, not more than seven years from the time of admission.

REGISTRATION FOR COURSES

A newly admitted student will automatically be registered for all the courses prescribed for the first year, without any option.

All other students shall submit a completed registration form indicating the list of courses intended to be credited during the next semester. This registration will be done a week before the last working day of the current semester. Late registration, with the approval of the Dean on the recommendation of the Head of the Department, along with a late fee will be done, up to the last working day.

Registration for the project work shall be done only for the final semester.

ASSESSMENT

The break-up of assessment and examination marks for theory subjects is as follows.

First Assessment Test	:	15 Marks
Second Assessment Test	:	15 Marks
Assignment & Attendance (seminars, group discussion)	:	10 Marks
Total (Internal Marks)	:	40 Marks
End semester Examination (External Marks)	:	60 Marks

Total (Internal + External)	:	100 Marks

The break-up of the assessment and examination marks for practical is as follows.

Observations	:	15 Marks
Model Test	:	15 Marks
Record book & Attendance	:	10 Marks
Total (Internal Marks)	:	40 Marks
End semester Examination (External Marks)	:	60 Marks
Total (Internal + External)	:	100 Marks

The project work will be assessed for 40 marks by a committee consisting of the Guide and the Head of the Department. The Head of the Department shall be the Chairman. 60 marks are allotted for the project viva voce examination at the end of the semester.

WITHDRAWAL FROM A COURSE

A student can withdraw from the course at any time before a date fixed by the Head of the Department prior to the second assessment, with the approval of the Dean on the recommendation of the Head of the Department.

TEMPORARY BREAK OF STUDY

A student can take a one-time temporary break of study covering the current year/semester and/or the next semester with the approval of the Dean on the recommendation of the Head of the Department, not later than seven days after the completion of the mid-semester test. However, the student must complete the entire program within the maximum period of seven years.

SUBSTITUTE ASSESMENT

A student, who has missed, for genuine reasons accepted by the Head of the Department, one or more of the assessments of a course other than the end semester examination, may take a substitute assessment for any one of the missed assessments. The substitute assessment must be completed before the commencement of the end-semester examination.

A student who wishes to have a substitute assessment for a missed assessment must apply to the concerned faculty member within a week from the date of the missed assessment.

ATTENDANCE REQUIREMENTS

To be eligible to appear for the examination in a particular course, a student must put in a minimum of 80% of attendance in the course. However, if the attendance is 70% or above but less than 80% in any course, the authorities can permit the student to appear for the examination in the course on payment of the prescribed condonation fee.

A student who withdraws from or does not meet the minimum attendance requirement in the course must re-register for and repeat the course.

PASSING AND DECLARATION OF EXAMINATION RESULTS

All assessments of all the courses on the absolute mark basis will be considered and passed by the results passing board in accordance with the rules of the University. Thereafter, the Controller of Examinations shall convert the marks for each course to the corresponding letter grade as follows, compute the grade point average & cumulative grade point average and prepare the grade cards.

90 to 100 marks	-	Grade 'S'
80 to 89 marks	-	Grade 'A'
70 to 79 marks	-	Grade 'B'
60 to 69 marks	-	Grade 'C'
55 to 59 marks	-	Grade 'D'
50 to 54 marks	-	Grade 'E'
less than 50 marks	-	Grade 'F'
Insufficient attendance	-	Grade 'I'
Withdrawn from the course	-	Grade 'W'

A student who obtains less than 50 marks out of 100 in the subject or less than 24 out of 60 in

External exam or is absent for the examination will be awarded Grade 'F'.

A student who earns a grade of S, A, B, C, D or E for a course is declared to have successfully completed that course and earned the credits for that course. Such a course cannot be repeated by the student.

A student who obtains letter grade F in a course has to reappear for the examination in that course.

The following grade points are associated with each letter grade for calculating the grade point average.

S – 10; A-9; B-8; C-7; D-6; E-5; F-0

A student can apply for revaluation of one or more of his /her examination answer papers within a week from the date of issue of Grade sheet to the student on payment of the prescribed fee per paper. The application must be made to the Controller of Examinations with the recommendation of the Head of the Department.

After results are declared, Grade cards will be issued to the students. The Grade card will contain the list of courses registered during the year/semester, the grades scored and the grade point average (GPA) for the year/semester.

GPA is the sum of the products of the number of credits of a course with the grade point scored in that course, taken over all the courses for the Year/Semester , divided by the sum of the number of credits for all courses taken in that year/semester. CGPA is similarly calculated considering all the courses taken from the time of admission.

After successful completion of the program, the Degree will be awarded with the following classification based on CGPA:

For First Class with Distinction, the student must pass all the courses in the first attempt and obtain a CGPA of 8.25 or above.

For First Class, the student must pass within four years from the time of admission and obtain a CGPA of 6.5 or above.

For Second Class, the student must pass within seven years from the time of admission.

B.E. (Hons.) Computer Science and Engineering with Specialization in Cyber Security

Honors Course						
Sl.No	**Semester**	**Course Title**	**L**	**T**	**P**	**C**
1.	III	Cyber Space Operations	3	0	0	3
2.	IV	Cryptography and Network Security with Lab	3	0	0	5
3.	V	Database and Application Security	3	0	0	3
4.	VI	Cloud Security	3	0	0	3
5.	VII	Quantum Security	3	0	0	3
6.	VII	Forensics and Investigation Lab	0	0	4	2
Total						**19**

III – SEMESTER

Course Code		L	T	P	C
Course Title	**CYBER SPACE OPERATIONS**	3	0	0	3

PRE-REQUISITES

Basic computer knowledge

OBJECTIVES

- To Learn the Basics of Cyber space operations
- To understand about cyber crimes
- To understand about cyber threats in cyber space.
- To understand about the social media and the crime related to social media
- To understand about cyber forensics

COURSE OUTCOMES

At the end of course, the students will be able to

1. Understand the concept of Cyber space operations.
2. Understand the cybercrimes its impact
3. Learn about cyber threats.
4. Understand crime in social media
5. Understand about cyber forensics

POs and COs MAPPING TABLES

	PO 01	PO 02	PO 03	PO 04	PO 05	PO 06	PO 07	PO 08	PO 09	PO 10	PO 11	PO 12	PSO 01	PSO 02	PSO 03
CO 01	3	2	-	1	-							2			
CO 02	3	3	1	2	-							1			
CO 03	3	2	2	1	-	2						2			
CO 04	3	2	1	1	1	1						2			
CO 05	3	3	2	2	1	2						2			

LEGEND: 1-LOW, 2 – MEDIUM, 3-HIGH

UNIT – I	**CYBER SPACE OPERATIONS**	9

Introduction to Cyber Operations: Defining Cyberspace, Architecture of cyberspace, Cyberspace Operation- Network Operations (NetOps), Defensive Cyberspace Operations (DCO), Offensive Cyberspace Operations (OCO). Cyber warfare, Regulation of cyberspace, OSI Model, Network Topologies.

UNIT – II	**CYBER CRIME**	9

Cybercrime - Classifications of Cybercrimes, Common cybercrimes - cybercrime targeting computers and mobiles, cybercrime against women and children, financial frauds, social engineering attacks, Cybercriminals, Cyber offenses – Cyber Terrorism. Cyber security

challenges, Cyber security measures by Indian Government		
UNIT – III	**VULNERABILITY IN CYBERSPACE**	9
Types of Hackers- Hackers and Crackers - Cyber-Attacks and Vulnerabilities- Malware threats- Sniffing - Gaining Access - Hiding Files - Covering Tracks- Worms – Trojans Viruses- Backdoors. Vulnerabilities- Overview, Vulnerabilities in Software, System administration, Threat actors, attacks, Cyber Security access control, Authentication, Security policy, Threat Management.		
UNIT – IV	**SOCIAL NETWORKS**	9
Introduction to Social networks. Types of Social media, Social media platforms, Social media monitoring, Hashtag, Viral content, Social media marketing, Social media privacy, Challenges, Security issues related to social media, Flagging and reporting of inappropriate content, Laws regarding posting of inappropriate content.		
UNIT – V	**CYBER FORENSICS**	9
Cyber forensics : Need for cyber forensics, cyber forensics process, types of cyber forensics, cyber forensic Tools and Techniques , Types of cyber forensic investigation, challenges in cyber forensic, case studies.		

TEXT BOOKS

1.	Cyber Operations: A Case Study Approach - Jerry M. Couretas 1st Edition (2024)
2.	Cyber Security - Praveen Kumar Tripathi, Niraj Kumar Tiwari 1st Edition (2024) Publisher: S.K. Kataria & Sons
3.	Cyber security and digital forensics 2025 springer

REFERENCES

1.	Information Security, Privacy and Digital Forensics Editors: Naveen Kumar Chaudhary, S.S. Iyengar, Chirag Modi Publisher: Springer 2026
2.	Cyber Forensic Analytics BY Gayathri gupta 2025
3.	A Handbook on Basics of Cyber Hygiene for Higher Education Institutions, © University Grants Commission Nov 2024

LEARNING OUTCOMES

By the end of this course, learners will be able to:

1.	Understand the Basics of Network , Cyber space and its operations
2.	Analyze Cybercrime and its effects.
3.	Explain various threats, cyber security mechanism.
4.	Apply social media in effectively
5.	Understand cyber forensics

PREPARED BY

Dr. D. Thamaraiselvi, B Karthikeyan Asst.Professor CSE Dept.,

IV – SEMESTER

Course Code	<<Course Code>>	L	T	P	C
Course Title	CRYPTOGRAPHY AND NETWORK SECURITY	3	0	4	5

PRE-REQUISITES

- Fundamentals of **Data Structures**
- Basic knowledge of **Cyber Space Operations**
- Familiarity with **C / Java / Python programming**

OBJECTIVES

•	To understand the fundamental concepts of information security and types of cyber-attacks.
•	To study classical and modern cryptographic techniques for secure communication.
•	To learn symmetric and asymmetric encryption algorithms and their applications.
•	To understand authentication mechanisms, digital signatures, and key management techniques.
•	To analyze network security threats and apply appropriate protection mechanisms.
•	To explore data compression techniques and their role in efficient data transmission.

COURSE OUTCOMES

At the end of course, the students will be able to

1.	Understand cryptographic fundamentals and security principles
2.	Apply encryption algorithms for secure communication
3.	Analyze network attacks and implement defense mechanisms
4.	Use authentication and key management techniques
5.	Apply data compression methods and evaluate performance

POs and COs MAPPING TABLES

	PO 01	PO 02	PO 03	PO 04	PO 05	PO 06	PO 07	PO 08	PO 09	PO 10	PO 11	PO 12	PSO 01	PSO 02	PSO 03
CO 01	3	2	-	-	-	1	-	1	-	-	-	1			
CO 02	3	3	2	-	2	-	-	-	-	-	-	-			
CO 03	3	3	2	2	2	1	-	1	-	1	-	-			
CO 04	2	2	2	1	1	-	-	-	-	-	-	-			
CO 05	2	2	2	2	2	1	1	1	1	1	1	2			

LEGEND:1-LOW, 2 – MEDIUM, 3-HIGH

UNIT – I	**Security Concepts & Classical Encryption**	**9**

Need for Security and Security Approaches - Principles of Security (CIA Triad) - Types of Attacks (Active & Passive) - Basics of Cryptography (Plaintext, cipher text) - Encryption and Decryption Process - Classical Encryption Techniques (Substitution & Transposition) - Cryptanalysis (Types of Attacks, Key Range & Key Size)

UNIT – II	**Cryptographic Algorithms**	**9**

Symmetric Key Cryptography – Concepts and Types - Block Cipher Algorithms: DES and IDEA - Modes of Operation in Encryption - Cryptanalysis Techniques (Differential & Linear) - Asymmetric Key Cryptography – RSA Algorithm -Knapsack Algorithm and Key Exchange Concepts - Digital Signatures and Hybrid Cryptography		
UNIT – III	**Network Security & Authentication**	**9**
Network Attacks: DoS and IP Spoofing - Conventional Encryption and Message Confidentiality - Key Distribution and Management Techniques - Message Authentication Methods - Hash Functions: MD5 and SHA-1 - Public Key Cryptography Principles - Firewalls and Basic Network Security Mechanisms, Multi-Factor Authentication (MFA), Intrusion Detection Systems (IDS/IPS)		
UNIT – IV	**Fundamentals of Data Compression**	**9**
Need for Data Compression - Communication Model and Compression Process - Compression Ratio and Performance Measures - Requirements and Characteristics of Compression - Classification of Compression Techniques - Lossless Compression Methods - Lossy Compression Methods		
UNIT – V	**Advanced Compression Techniques & Trends**	**9**
Entropy Encoding (Run Length, Repetitive & Zero Encoding) - Statistical Encoding (Huffman Coding) - Arithmetic Coding Technique - Lempel-Ziv (LZ) Coding - Source Encoding – Vector Quantization - Recent Trends in Encryption Techniques - Recent Trends in Data Compression, AI-based Compression Techniques		
LIST OF EXPERIMENTS		
UNIT – I	**Security Basics & Classical Encryption**	
1.	Implementation of Caesar Cipher (Substitution Technique)	
2.	Implementation of Playfair Cipher	
3.	Implementation of Rail Fence Cipher (Transposition Technique)	
UNIT – II	**Cryptography Algorithms**	
4	Implementation of RSA Algorithm (Encryption & Decryption)	
5.	Demonstration of Diffie-Hellman Key Exchange	
6.	Implementation of Digital Signature (Creation & Verification)	
UNIT – III	**Network Security & Authentication**	
7.	Implementation of Huffman Coding	
8.	Implementation of Lempel-Ziv (LZ) Compression	
9.	Mini Project: Secure Data Transmission using Compression + Encryption	
UNIT – IV	**Data Compression Basics**	
10.	Implementation of Run Length Encoding (RLE)	
11.	Program to calculate Compression Ratio	
12.	Demonstration of Lossless vs Lossy Compression Techniques	
UNIT – V	**Advanced Compression Techniques**	
13.	Implementation of Huffman Coding	
14.	Implementation of Lempel-Ziv (LZ) Compression	

15.	Mini Project: Secure Data Transmission using Compression + Encryption
Lab Tools and Environments (optional)	
Programming Environment: Python / C / C++ / Java	
Core Libraries: Python: hashlib, cryptography Java: java.security, javax.crypto	
Database Tools: (optional)	
Cloud & Collaboration Platforms: (optional) Google Colab / GitHub	
Frameworks (basic exposure): (optional)	
Data Formats & APIs: (optional)	
TEXT BOOKS	
1.	Cryptography and Network Security: Principles and Practice Author: William Stallings Edition: 8th Edition (2024) Publisher: Pearson
2.	Cryptography and Network Security Author: Atul Kahate Edition: 4th Edition (2025) Publisher: McGraw Hill
REFERENCES	
1.	Cryptography and Network Security Author: Behrouz A. Forouzan Edition: 3rd Edition Publisher: McGraw-Hill Education (2015)
2.	**Cryptography: Algorithms, Protocols, and Standards for Computer Security, Zoubir Z. Mammeri , 2024 published by John Wiley & Sons(2024)**
3.	Information Theory and Coding Authors: Muralidhar Kulkarni, K. S. Shivaprakasha Edition: 1st Edition Publisher: John Wiley & Sons (2019)
LEARNING OUTCOMES	
1.	**Explain** the fundamental concepts of security, types of attacks, and security principles.
2.	**Apply** classical and modern encryption techniques to secure data and communication.
3.	**Analyze** symmetric and asymmetric cryptographic algorithms such as DES and RSA.
4.	**Demonstrate** the use of authentication techniques, hash functions, and digital signatures.
5.	**Evaluate** network security threats such as DoS and IP spoofing and propose suitable countermeasures.
6.	**Apply** data compression techniques such as Huffman coding, Lempel-Ziv, and Run-Length encoding.
7.	Understand recent trends in cryptography and data compression for real-world applications.
PREPARED BY	
Mr.E.Sankar, Mr.V.Balu, Mr.B.Karthikeyan Asst. Prof., CSE Dept.,	