

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING - DATA SCIENCE

COURSE MODULE OF THE SUBJECT TAUGHT FOR THE SESSION 2026-27

(ODD SEM)

Course Syllabus with CO's

Faculty Name: Mrs. Sushmitha N				Academic Year: 2025 - 2026			
Department: CSE (Data Science)							
Cours e Code	CourseTitle	Core/Elective	Prerequisite	Contac t Hours			Total Hrs/ Sessions
				L	T	P	
BCS703	Cryptography & Network Security	Core	Knowledge of Data Communication and Number theory	4	0	0	50

Course Learning Objectives: This course will enable students to:

Learning Objectives:

- Understand the basics of Cryptography concepts, Security and its principle
- To analyse different Cryptographic Algorithms
- To illustrate public and private key cryptography
- To understand the key distribution scenario and certification

To understand approaches and techniques to build protection mechanisms in order to secure computer networks

Module 1	Contact Hours
A model for Network Security, Classical encryption techniques: Symmetric cipher model, Substitution ciphers-Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Hill Cipher, Polyalphabetic Ciphers, One time pad, Steganography. Block Ciphers and Data Encryption Standards: Traditional Block Cipher structures, data Encryption Standard (DES), A DES Example, The strength of DES, Block cipher design principles.	10
Module 2	Contact Hours
Pseudorandom number Generators: Linear Congruential Generators, Blum Blum Shub Generator. Public key cryptography and RSA: Principles of public key cryptosystems-Public key cryptosystems, Applications for public key cryptosystems, Requirements for public key cryptography, Public key Cryptanalysis, The RSA algorithm: Description of the Algorithm, Computational aspects, The Security of RSA. Diffie-Hellman key exchange: The Algorithm, Key exchange Protocols, Man-in-the-middle Attack, Elliptic Curve Cryptography: Analog of Diffie-Hellman key Exchange, Elliptic Curve Encryption/Decryption, Security of Elliptic Curve Cryptography.	10
Module - 3	Contact Hours
Applications of Cryptographic Hash functions, Two simple Hash functions, Key management and distribution: Symmetric key distribution using symmetric encryption, Symmetric key distribution using asymmetric encryption, Distribution of public keys, X.509 Certificates, Public Key Infrastructures	10

Module - 4	
Predictive Analytics I - Data mining process, methods, and Algorithms: Data Mining Concepts and Applications, Data Mining Applications, Data Mining Process, Data Mining Methods. Prescriptive Analytics - Optimization and Simulation: Model-Based Decision-Making, Structure of Mathematical Models for Decision Support, Certainty, Uncertainty, and Risk, Decision Modeling with Spreadsheets.	10
Module - 5	
Domain keys Identified Mail. IP Security: IP Security overview, IP Security Policy, Encapsulating Security Payload, Combining security associations, Internet key exchange	10
TextBooks: William Stallings, “Cryptography and Network Security”, Pearson Publication, Seventh Edition.	
Reference Books: 1. Keith M Martin, “Everyday Cryptography”, Oxford University Press 2. V.K Pachghare, “Cryptography and Network Security”, PHI, 2nd Edition	
Course outcomes: The students should be able to: CO1: Explain the basic concepts of Cryptography and Security aspects CO2: Apply different Cryptographic Algorithms for different applications CO3: Analyze different methods for authentication and access control. CO4: Describe key management, key distribution and Certificates. CO5: Explain about Electronic mail and IP Security.	
Continuous Internal Evaluation: For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.	

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING - DATA SCIENCE

The Correlation of Course Outcomes (CO's) and Program Outcomes (PO's)

Subject Code	BCS703											
List of Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	Total
CO-1	2											2
CO-2		2										2
CO-3		2										2
CO-4	2											2
CO-5			2									2
Total	4	4	2									10

Note: 3 = Strong Contribution 2 = Average Contribution 1 = Weak Contribution - = No Contribution

The Correlation of Course Outcomes (CO's) and Program Specific Outcomes (PSO's)

Subject Code: BCS703			
List of Course Outcome's	PSO1	PSO2	Total
CO-1	-	-	
CO-2	-	2	2
CO-3	-	2	2
CO-4	-	-	
CO-5	-	-	
Total	-	4	4

Note: 3 = Strong Contribution 2 = Average Contribution 1 = Weak Contribution - = No Contribution