COURSE PLAN & COURSE DATA SHEET

PROGRAM: B.TECH	DEGREE: 3
COURSE: CRYPTOGRAPHY AND DATA COMPRESSION	SEMESTER: 6TH CREDITS: 3
COURSE CODE: CS-310 REGULATION:	COURSE TYPE: CORE
COURSE AREA/DOMAIN:	CONTACT HOURS: 3+1 (Tutorial) hours/Week.
CORRESPONDING LAB COURSE CODE (IF ANY):	LAB COURSE NAME (IF ANY):

PROGRAM EDUCATIONAL OBJECTIVES:

SYLLABUS:

UNIT	DETAILS	HOURS
I	UNIT I COMPRESSION: Packing; Huffman coding; run length encoding; Lempel-Ziv-Welch; Phil Katz's PKZIP; Delta modulation; JPEG.	7
II	ERROR DETECTION AND CORRECTION: Parity; 1, 2, n-dimensions, Hamming codes; pout-of-q codes	7
III	CRYPTOGRAPHY: Vocabulary; history, steganography – visual, textual; cipher hiding; false errors; public key cryptography - authentication, signatures, deniability	7
IV	MATHEMATICS: Information; confusion; diffusion; modular arithmetic; inverses; Fermat's little theorem, Chinese remainder theorem; factoring; prime numbers; discrete logarithms	7
V	ALGORITHMS: DES; AES (Rijndael); IDEA; one time pad; secret sharing and splitting; RSA; elliptic curves; modes; random numbers	7
	TOTAL HOURS	35

Teacher Centric Approach

TC1: Chalk and Talk, **TC2: PPT,** **TC3: Video Lectures** **TC4: Blended learning**

Learner Centric Approach:

LC1: Assignment. **LC2: Mini project.** **LC3: Quiz/Class test.** **LC 4: Seminar on recent trends.**

LC5: Group Task. **LC6: Others**

DETAILED SESSION PLAN

Lecture session/ Number	Topics to be covered	CO addressed	Teacher Centric Approach	Learner Centric Approach	References	Relevance with POs and PSOs
1.	COMPRESSION		TC1	LC1,LC3	T1/T2/R1/W1	
2.	Packing		TC1	LC1,LC3	T1/T2/R1/W1	
3.	Huffman coding		TC1,TC2	LC1,LC3	T1/T2/R1/W1	
4.	run length encoding;		TC1,TC2	LC1,LC3	T1/T2/R1/W1	
5.	Lempel-Ziv-Welch, JPEG		TC1,TC2	LC1,LC3	T1/T2/R1/W1	
6.	Phil Katz's PKZIP; Delta modulation		TC1,TC2	LC1,LC3	T1/T2/R1/W1	
7.	ERROR DETECTION AND CORRECTION		TC1	LC1,LC3	T1/T2/R1/W1	
8.	Parity; 1, 2, n-dimensions		TC1	LC1,LC3	T1/T2/R1/W1	
9.	Hamming codes; pout-of-q codes		TC1,TC2	LC1,LC3	T1/T2/R1/W1	
10.	CRYPTOGRAPHY		TC1	LC1,LC3	T1/T2/R1/W1	
11.	steganography		TC1	LC1,LC3	T1/T2/R1/W1	
12.	visual, textual; cipher hiding		TC1	LC1,LC3	T1/T2/R1/W1	
13.	false errors		TC1	LC1,LC3	T1/T2/R1/W1	
14.	public key cryptography		TC1	LC1,LC3	T1/T2/R1/W1	
15.	- authentication,		TC1	LC1,LC3	T1/T2/R1/W1	
16.	signatures		TC1	LC1,LC3	T1/T2/R1/W1	
17.	deniability		TC1,TC2	LC1,LC3	T1/T2/R1/W1	
18.	confusion; diffusion		TC1	LC1,LC3	T1/T2/R1/W1	
19.	modular arithmetic		TC1	LC1,LC3	T1/T2/R1/W1	
20.	inverses; Fermat's little theorem		TC1	LC1,LC3	T1/T2/R1/W1	
21.	Chinese remainder theorem		TC1,TC2	LC1,LC3	T1/T2/R1/W1	

22.	factoring; prime numbers		TC1,TC2	LC1,LC3	T1/T2/R1/W1	
23.	discrete logarithms		TC1,TC2	LC1,LC3	T1/T2/R1/W1	
24.	DES		TC1	LC1,LC3	T1/T2/R1/W1	
25.	AES (Rijndael)		TC1,TC2	LC1,LC3	T1/T2/R1/W1	
26.	IDEA		TC1	LC1,LC3	T1/T2/R1/W1	
27.	one time pad; secret sharing and		TC1	LC1,LC3	T1/T2/R1/W1	
28.	RSA;		TC1,TC2	LC1,LC3	T1/T2/R1/W1	
29.	elliptic curves; modes: random		TC1,TC2	LC1,LC3	T1/T2/R1/W1	

TEXT/REFERENCE BOOKS:

T/R	BOOK TITLE/AUTHORS/PUBLICATION
1	IEEE, "Integration of Data Compression and Cryptography: Another Way to Increase the Information Security", IEEE Computer Society
2	Behrouz A. Forouzan "Cryptography and Network Security", TMH
3	Atul Kahate , "Cryptography and Network Security", 3rd Edition, Tata Mcgraw Hill.
4	Mani Subramanian, "Network Management Principles & Practices", Addison Wesley, 1999
5	Kauffman C., Perlman R. and Spenser M., "Network Security", 2nd Edition, Prentice Hall, 2002

# WEB SOURCE REFERENCES (W):

1	https://www.tutorialspoint.com/information_security_cyber_law/network_security.htmL
2	
3	
4	
5	
6	
7	

COURSE PRE-REQUISITES:

C.CODE	COURSE NAME	DESCRIPTION	SEM
CS-310	**CRYPTOGRAPHY AND DATA COMPRESSION**	**3-0-0**	**6TH**

COURSE OBJECTIVES:

1	The main objective behind this course is to learn about the various network attacks and preventing attacks. This course is designed to cover Application security, Network security, Web security etc.
2	Develop a basic understanding of cryptography, how it has evolved, and some key encryption techniques used today.

3	Develop an understanding of security policies (such as authentication, integrity and confidentiality), as well as protocols to implement such policies in the form of message exchanges.
4	Data Communications and Computer Networks, Computer Programming, Data Structures, Prime Number Theory

COURSE OUTCOMES:

S.NO	DESCRIPTION	PO(1..12) MAPPING	PSO(1..3) MAPPING
Cxxx.1	Understand and analyze public-key cryptography, RSA and other public-key cryptosystems	PO1,PO2,PO3	PSO1,PSO2,PSO3
Cxxx.2	Analyze and design hash and MAC algorithms, and digital signatures.	PO1,PO2,PO12	PSO1,PSO2,PSO3
Cxxx.3	Design network application security schemes, such as PGP, S/ MIME, IPSec, SSL, TLS, HTTPS, SSH, etc.	PO1,PO2,PO3,PO12	PSO2,PSO3
Cxxx.4	Understand key management and distribution schemes and design User Authentication Protocol	PO1,PO2,PO3,PO6,PO12	PSO1,PSO2,PSO3
Cxxx.5	Know about Intruders and Intruder Detection mechanisms, Types of Malicious software, Firewall Characteristics, Types of Firewalls, Firewall Location and Configurations	PO1,PO2,PO3,PO6,PO12	PSO1,PSO2,PSO3
COURSE OVERALL PO/PSO MAPPING:			

COURSE OUTCOMES VS POs MAPPING (DETAILED; HIGH:3; MEDIUM:2; LOW:1)**:**

S.NO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
Cxxx.1	2	1	1	-	-	-	-	-	-	-	-	-	1	2	3
Cxxx.2	1	2	-	-	-	-	-	-	-	-	-	2	1	2	1
Cxxx.3	1	1	2	-	-	-	-	-	-	-	-	1	-	1	2
Cxxx.4	2	1	2	-	-	2	-	-	-	-	-	1	1	2	2
Cxxx.5	1	2	1	-	-	1	-	-	-	-	-	2	1	1	2
Cxxx*															

** For Entire Course, PO & PSO Mapping*

POs & PSO REFERENCE:

PO 1	**Engineering Knowledge:** Apply the knowledge of mathematics, science, engineering and Application fundamentals, and an engineering and Application specialization to the solution of complex engineering	PO7	**Environment and sustainability**: Understand the impact of professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need	PSO 1	Professional Skills: An ability to understand the basic concepts in Electronics & Communication Engineering and to apply them to various areas, like Electronics, Communications, Signal

	problems.		for sustainable development.		processing, VLSI, Embedded systems etc., in the design and implementation of complex systems.
PO 2	**Problem Analysis:** Identify, formulate, research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO8	**Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of engineering practice.	PSO 2	Problem-Solving Skills: An ability to solve complex Electronics and communication Engineering problems, using latest hardware and software tools, along with analytical skills to arrive cost effective and appropriate solutions.
PO 3	**Design/development of solutions**: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations	PO9	**Individual and teamwork**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PSO 3	Successful Career and Entrepreneurship: An understanding of social-awareness & environmental-wisdom along with ethical responsibility to have a successful career and to sustain passion and zeal for real-world applications using optimal resources as an Entrepreneur.
PO 4	**Conduct investigations of complex problems**: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO10	**Communication**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.		
PO	**Modern tool usage**: Create,	PO11	**Project management**		

5	select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.		**and finance**: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.		
PO 6	**The engineer and society**: Apply reasoning informed by contextual knowledge to assess societal, health, safety, legal and cultural issues, and the consequent responsibilities relevant to the professional engineering practice.	PO12	**Life-long learning:** Recognize the need for and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.		

COs VS POs MAPPING JUSTIFICATION:

S.NO	PO/PSO MAPPED	LEVEL OF MAPPING	JUSTIFICATION
Cxxx.1			
Cxxx.2			
Cxxx.3			
Cxxx.4			
Cxxx.5			
Cxxx*			

GAPS IN THE SYLLABUS - TO MEET INDUSTRY/PROFESSION REQUIREMENTS, POs & PSOs:

SNO	DESCRIPTION	PROPOSED ACTIONS
1		
2		
3		
4		
5		

PROPOSED ACTIONS: TOPICS BEYOND SYLLABUS/ASSIGNMENT/INDUSTRY VISIT/GUEST LECTURER/NPTEL ETC

# TOPICS BEYOND SYLLABUS/ADVANCED TOPICS/DESIGN:

1	
2	
3	
4	
5	
6	
7	

DELIVERY/INSTRUCTIONAL METHODOLOGIES:

☐ CHALK & TALK	☐ STUD. ASSIGNMENT	☐ WEB RESOURCES	☐ NPTEL/OTHERS
☐ LCD/SMART BOARDS	☐ STUD. SEMINARS	☐ ADD-ON COURSES	☐ WEBNIARS

ASSESSMENT METHODOLOGIES-DIRECT

☐ ASSIGNMENTS	☐ STUD. SEMINARS	☐ TESTS/MODEL EXAMS	☐ UNIV. EXAMINATION
☐ STUD. LAB PRACTICES	☐ STUD. VIVA	☐ MINI/MAJOR PROJECTS	☐ CERTIFICATIONS
☐ ADD-ON COURSES	☐ OTHERS		

ASSESSMENT METHODOLOGIES-INDIRECT

☐ ASSESSMENT OF COURSE OUTCOMES (BY FEEDBACK, ONCE)	☐ STUDENT FEEDBACK ON FACULTY (TWICE)
☐ ASSESSMENT OF MINI/MAJOR PROJECTS BY EXT. EXPERTS	☐ OTHERS

# INNOVATIONS IN TEACHING/LEARNING/EVALUATION PROCESSES:

1. Learning Through Interactivity

2. The Shift from Physical to eTextbooks

3. Focus on Accessible Education

4. Higher Measurability of Learning Effectiveness

5. Leverage a Single, Unified Platform

Prepared by **Approved by**
(Ms. SHIVANI BANSAL) **(HOD)**

# Additionally, the details to be compiled separately by the Departmental Coordinator for the entire Department.