SIR C.R.REDDY COLLEGE OF ENGINEERING, ELURU

DEPARTMENT OF INFORMATION TECHNOLOGY

COURSE HANDOUT

SUBJECT: CRYPTOGRAPHY AND NETWORK SECURITY

CLASS: IV/IV B.Tech. I SEMESTER, A.Y.2022-23

INSTRUCTOR: SRI CHALLA YALLAMANDA

Course Handout Index

S. No	Description
1	College Vision & Mission
2	Department Vision & Mission
3	Program Educational Objectives (PEOs)
4	Program Outcomes (POs)
5	Program Specific Outcomes (PSOs)
6	JNTUK Academic Calendar
7	Department Academic Calendar
8	Course Description
9	Course Objectives
10	Course Outcomes
11	Lesson Plan
12	Evaluation Pattern
13	Timetable
14	Unit wise Questions

College Vision & Mission

Vision: To emerge as a premier institution in the field of technical education and research in the state and as a home for holistic development of the students and contribute to the advancement of society and the region.

Mission: To provide high quality technical education through a creative balance of academic and industry oriented learning; to create an inspiring environment of scholarship and research; to instill high levels of academic and professional discipline; and to establish standards that inculcate ethical and moral values that contribute to growth in career and development of society in general.

Department Vision & Mission

Vision: To be a premier department in the region in the field of Information Technology through academic excellence and research that enable graduates to meet the challenges of industry and society.

Mission: To Provide dynamic teaching-learning environment to make the students industry ready and advancement in career; to inculcate professional and leadership quality for better employability and entrepreneurship; to make high quality professional with moral and ethical values suitable for industry and society.

Program Educational Objectives (PEOs)

PEO1: Solve real world problems through effective professional skills in Information Technology industry and academic research.

PEO2: Analyze and develop applications in Information Technology domain and adapt to changing technology trends with continuous learning.

PEO3: Practice the profession in society with ethical and moral values.

Program Outcomes (POs)

PO1: Engineering Knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

PO2: Problem Analysis: Identify, formulate, research literature, and analyze complex engineering problems reaching substantiated conclusions using the first principles of mathematics, natural sciences, and engineering sciences.

PO3: Design/Development of Solutions: Design solutions for complex engineering problems and system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, society, and environmental considerations.

PO4: 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.

PO5: Modern Tool Usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

PO6: The Engineer and Society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO7: Environment and Sustainability: Understand the impact of the professional engineering solutions in society and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

PO8: Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

PO9: Individual and Team Work: Function effectively as an individual, and as a member or leader in diverse teams, and in multi-disciplinary settings.

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.

PO11: Project Management 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 multi-disciplinary environments.

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.

Program Specific Outcomes (PSOs)

PSO1: Design Skill: Design and develop softwares in the area of relevance under realistic constraints.

PSO2: New Technology: Adapt new and fast emerging technologies in the field of Information Technology.

JNTUK Academic Calendar

Website: www.jntuk.edu.in
Email: dap@jntuk.edu.in

Phone: 0884-2300991

Directorate of Academic Planning

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA-533003, Andhra Pradesh, INDIA
(Established by AP Government Act No. 30 of 2008)

Lr. No. DAP/AC/IV Year /B. Tech/B. Pharmacy/2022 *Date 25.06.2022*

Dr. KVSG Murali Krishna,
M.E, Ph.D.,
Director, Academic Planning
JNTUK, Kakinada

To
All the Principals of Affiliated Colleges,
JNTUK, Kakinada.

Academic Calendar for IV Year - B. Tech/B. Pharmacy for the AY 2022-23

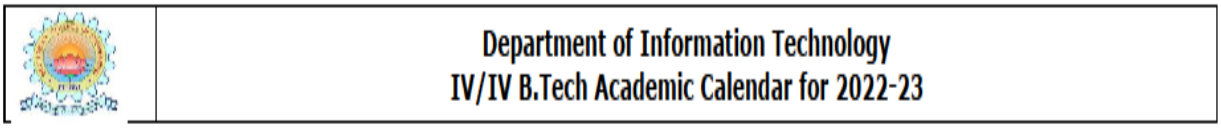
I SEMESTER			
Description	**From**	**To**	**Weeks**
Commencement of Class Work	**04.07.2022**		
I Unit of Instruction	04.07.2022	27.08.2022	8W
I Mid Examinations	29.08.2022	03.09.2022	1W
II Unit of Instructions	05.09.2022	29.10.2022	8W
II Mid Examinations	31.10.2022	05.11.2022	1W
Preparation & Practicals	07.11.2022	12.11.2022	1W
End Examinations	14.11.2022	26.11.2022	2W
Commencement of II Semester Class Work	**05.12.2022**		
II SEMESTER			
I Unit of Instructions	**05.12.2022**	28.01.2023	8W
I Mid Examinations	30.01.2023	04.01.2023	1W
II Unit of Instructions	06.01.2023	01.04.2023	8W
II Mid Examinations	03.04.2023	08.04.2023	1W
Preparation & Practicals	10.04.2023	15.04.2023	1W
End Examinations	17.04.2023	29.04.2023	2W

Director, 25/6/22
Academics & Planning,
JNTUK

Director
Academic Planning
JNTUK Kakinada

Copy to the Secretary to the Hon'ble Vice Chancellor, JNTUK
Copy to Rector, Registrar, JNTUK
Copy to Director Academic Audit, JNTUK
Copy to Director of Evaluation, JNTUK

Department Academic Calendar



Department of Information Technology
IV/IV B.Tech Academic Calendar for 2022-23

2022-23	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M
Jul 22						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
Aug 22		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
Sep 22					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30			
Oct 22							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Nov 22			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30					
Dec 22					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		
Jan 23	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31						
Feb 23				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28						
Mar 23				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
Apr 23							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
May 23		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
Jun 23					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30			

List of Holidays	Oct 9: Maulud Nabi	Mar 22 : Ugadhi	Mid exams	
July 10: Bakrid	Oct 24 : Diwali	Mar 30: Srirama navami	End Examinations	
Aug 9:Moharum	Dec 25 :Christmas	Apr 5: Babu Jagjivan Ram Jayanti	Commencement of Class work	
Aug 15:Independence day	Jan 14-16: sankranti	Apr 7: Good friday	Workshops	
Aug 31:Ganesh Chaturdi	Jan 26:Republic Day	Apr 14:Ambetkar Jayanthi	Department fest/Elite	
Oct 2: Gandhi jayanthi	Feb 18 :Sivaratri	Jun 29: Bakrid		HoD
Oct 5: Vijayadasami	Mar 8 : holi			Department of IT

Course Description

The aim of this course is to introduce the student to the areas of cryptography and cryptanalysis. This course develops a basic understanding of the algorithms used to protect users online and to understand some of the design choices behind these algorithms. A wide variety of basic cryptographic primitives with recent developments in some advanced topics like identity-based encryption. The cryptanalysis part will help us understanding challenges for cyber security that includes network security, data security, mobile security, cloud security and endpoint security.

Course Objectives

This course aims at training students to master the:

- The concepts of classical encryption techniques and concepts of finite fields and number theory.
- Working principles and utilities of various cryptographic algorithms including secret key cryptography, hashes and message digests, and public key algorithms.
- Design issues and working principles of various authentication protocols, PKI standards.
- Various secure communication standards including Kerberos, IPsec, and SSL/TLS and email.
- Concepts of cryptographic utilities and authentication mechanisms to design secure applications

Course Outcomes

Students are able to

CO No's	Cos	Level
CO1	Understand various cryptographic techniques and network security algorithms.	L2
CO2	Apply various cryptographic techniques and network security algorithms for given scenario.	L3
CO3	Analyze various cryptographic techniques and network security algorithms for a given network applications.	L4
CO4	Evaluate various cryptographic techniques and network security algorithms for a given network applications.	L5

Lesson Plan

S. No	Unit	Topic	Teaching Aids	CO
1	I	Classical Encryption Technique	BB	CO1
2		Security Attacks	BB	CO1
3		Services & Mechanisms	BB	CO1
4		Symmetric Cipher Model	BB	CO1
5		Cyber Threats & Phishing Attack	BB	CO1
6		Web Based Attacks & SQL Injection Attacks	PPT	CO2
7		Buffer Overflow& Format String Vulnerabilities	PPT	CO2
8		TCP session hijacking, UDP Session Hijacking	PPT	CO3
9		Block Ciphers: Traditional Block Cipher Structure	BB/PPT	CO2
10		Block Cipher Design Principles	BB	CO2
11	II	Symmetric Key Cryptography	BB	CO1
12		Data Encryption Standard (DES)	BB/PPT	CO1
13		Advanced Encryption Standard (AES)	BB/PPT	CO1
14		Blowfish, IDEA	BB/PPT	CO1

15		Block Cipher Modes of Operations	BB	CO1
16		Number Theory: Prime and Relatively Prime Numbers	BB	CO1
17		Modular Arithmetic	BB	CO1
18		Fermat's and Euler's Theorems	BB	CO1
19		The Chinese Remainder Theorem	BB	CO1
20		Discrete Logarithms	BB	CO2
21	III	Public Key Cryptography	BB	CO2
22		Principles, Public Key Cryptography Algorithms, RSA Algorithm	BB	CO4
23		Diffie Hellman Key Exchange	BB/PPT	CO4
24		Elliptic Curve Cryptography	BB	CO3
25		Cryptographic Hash Functions	BB/PPT	CO4
26		Application of Cryptographic Hash Functions	BB/PPT	CO3
27		Requirements & Security	BB	CO2
28		Secure Hash Algorithm, Message Authentication Functions	BB	CO3
29		Requirements & Security, HMAC & CMAC	BB	CO4
30		Digital Signatures: NIST Digital Signature Algorithm	BB/PPT	CO3
31		Key Management and Distribution	BB	CO4
32	IV	User Authentication: Remote User Authentication Principles	BB	CO2
33		Kerberos. Electronic Mail Security: Pretty Good Privacy (PGP) And S/MIME	BB	CO4
34		Kerberos. Electronic Mail Security: Pretty Good Privacy (PGP) And S/MIME	BB/PPT	CO4
35		IP Security: IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload	BB	CO2

36		IP Security: IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload	BB/PPT	CO2
37		Combining Security Associations and Key Management	BB	CO3
38	V	Transport Level Security: Web Security Requirements	BB	CO3
39		Secure Socket Layer (SSL) and Transport Layer Security(TLS)	BB	CO2
40		Secure Shell(SSH)	BB/PPT	CO1
41		Firewalls: Characteristics, Types of Firewalls, Placement of Firewalls, Firewall Configuration, Trusted Systems.	BB	CO2
42		Firewalls: Characteristics, Types of Firewalls, Placement of Firewalls, Firewall Configuration, Trusted Systems.	BB/PPT	CO2

Evaluation Pattern

S. No	Components	Internal	External	Total
1	Theory	25	75	100
2	Engineering Graphics/Design/Drawing	25	75	100
3	Practical	20	30	50
4	Mini Project/Internship/Industrial Training/ Skill Development programmes/Research Project	-	50	50
5	Project Work – Part I	20	30	50
5	Project Work – Part II	60	90	150

Marks Range Theory (Max – 100)	Marks Range Lab (Max – 75)	Letter Grade	Level	Grade Point
≥ 90	≥ 67	O	Outstanding	10
≥80 to <90	≥60 to <67	S	Excellent	9
≥70 to <80	≥52 to <60	A	Very Good	8
≥60 to <70	≥45 to <52	B	Good	7
≥50 to <60	≥37 to <45	C	Fair	6
≥40 to <50	≥30 to <37	D	Satisfactory	5

<40	<30	F	Fail	0
			Absent	0

Timetable

Day/Time	09.00-09.50	09.50-10.40	11.00-11.50	11.50-12.40	01.40-02.30	02.30-03.20	03.20-04.10	04.10-05.00
Mon		CNS-A		CNS-B				
Tue	CNS-B					CNS-A		
Wed		CNS-B		CNS-A				
Thu	CNS-A				CNS-B			
Fri					CNS-A			
Sat			CNS-B		**********			

Unit wise Questions

Unit I

1. Discuss the principles of security.
2. Explain the various types' attacks in details.
3. Illustrate the encryption and decryption.
4. Explain the following substitution techniques:
    a. Caesar cipher
    b. Modified Caesar cipher
    c. Mono – alphabetic cipher
    d. Homophonic substitution cipher
    e. Polygram cipher
    f. Polyalphabetic cipher
5. Explain Playfair cipher for the keyword "PLAYFAIR EXAMPLE" plain text is "MY NAME IS ATUL".
6. Discuss hill cipher with an example.
7. Explain the following transposition technique:
    a. Rail – Fence Technique
    b. Simple columnar transposition technique

c. Vernam cipher

8. Explain symmetric and asymmetric key exchange cryptography.
9. Illustrate the Diffie – Hellman algorithm and perform the encryption and decryption with prime numbers 11 and 7.
10. Explain the key ranges and key sizes in cryptography.

Unit II

1. Explain in details algorithm types and modes with an example.
2. Discuss an overview of symmetric key cryptography.
3. Explain in details about DES.
4. Summarize the double and triple DES standards.
5. Explain the IDEA with working flow.
6. Explain the working flow and encryption for RC5.
7. Explain the encryption and decryption for BLOWFISH.
8. Summarize the AES with their operations.
9. Discuss how the symmetric key is used in various algorithms such as DES, IDEA, RC5, BLOWFLISH and AES.

Unit III

1. Explain the overview of an asymmetric key cryptography with matrix of public and private key.
2. Explain the RSA algorithm with an example.
3. Explain the comparison between asymmetric and symmetric key cryptography.
4. Explain the digital signature with message digest algorithm.
5. Summarize the MD5 with working procedure.
6. Explain the secure Hash algorithm.
7. Explain the following:
   a. MAC b. HMAC
8. Discuss the Knapsack algorithm with an example.

Unit IV

1. Explain the digital certificates and creation of digital certificate.
2. Explain how a digital certificate van be verified.
3. Discuss the certificate hierarchies and self signed digital certificate.
4. Discuss the certification revocation with offline and online revocation techniques.
5. Explain the private key management.
6. Discuss the PKIX model services and architectural model.
7. Explain the public key cryptography standard 5 (PKCS#5).
8. Explain the XML key management specification.