SIR C.R.REDDY COLLEGE OF ENGINEERING, ELURU

DEPARTMENT OF INFORMATION TECHNOLOGY

COURSE HANDOUT

SUBJECT: CRYPTOGRAPHY AND NETWORK SECURITY

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

INSTRUCTOR: Smt.G.KRISHNAVENI

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: 0884-2340991

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/III Year /B. Tech/B. Pharmacy/2022 *Date 14.09.2022*

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 III Year - B. Tech/B. Pharmacy for the AY 2022-23
(2020-21 Admitted Batch)

I SEMESTER			
Description	**From**	**To**	**Weeks**
Community Service Project	**15.07.2022**	30.07.2022	2W
I Unit of Instruction	01.08.2022	24.09.2022	8W
I Mid Examinations	26.09.2022	01.10.2022	1W
II Unit of Instructions	03.10.2022	26.11.2022	8W
II Mid Examinations	28.11.2022	03.12.2022	1W
Preparation & Practicals	05.12.2022	10.12.2022	1W
End Examinations	12.12.2022	25.12.2022	2W
Commencement of II Semester Class Work	**02.01.2023**		
II SEMESTER			
I Unit of Instructions	**02.01.2023**	25.02.2023	8W
I Mid Examinations	27.02.2023	04.03.2023	1W
II Unit of Instructions	06.03.2023	29.04.2023	8W
II Mid Examinations	01.05.2023	06.05.2023	1W
Preparation & Practicals	08.05.2023	13.05.2023	1W
End Examinations	15.05.2023	27.05.2023	2W

*** As per the APSCHE Guidelines Out of the Total 180 hours of Community Service Project leading to 4 Credits, two weeks will be offline and remaining project work can be done during the III-I semester weekends and holidays. The summer internship can be done in online cum offline during III-I and III-II semesters.**

14/9/22

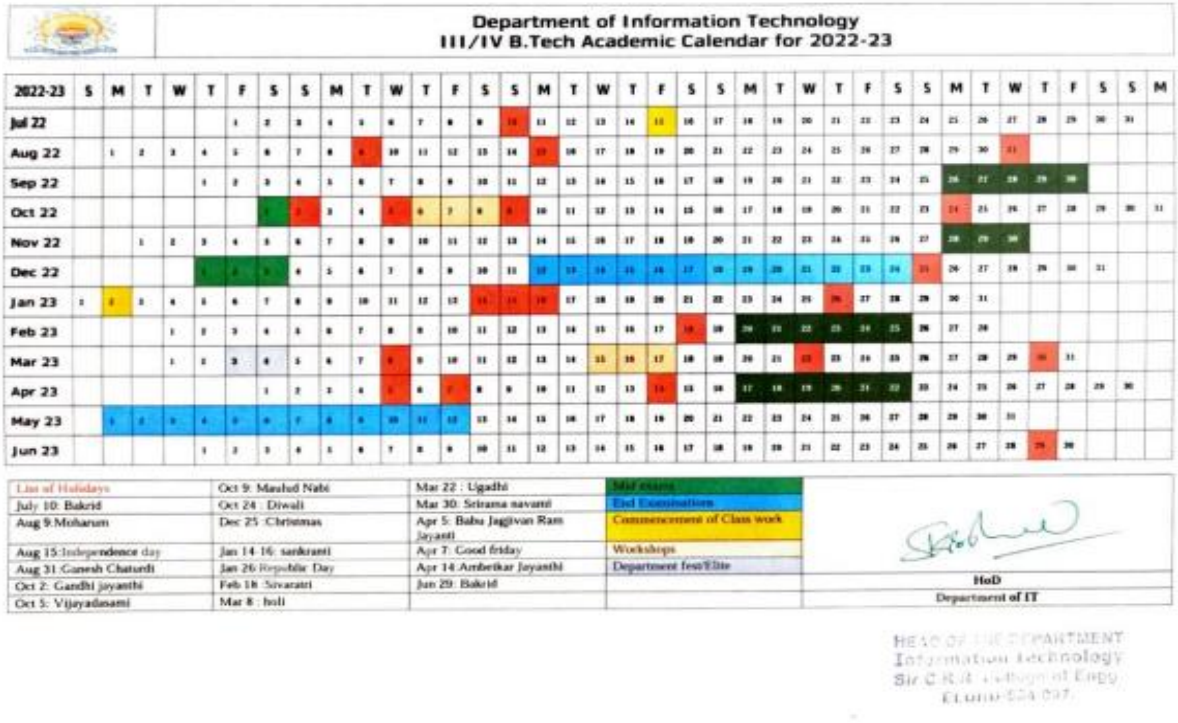
Director,
Academics & Planning, JNTUK

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

Department Academic Calendar

Department Academic Calendar



Department of Information Technology
III/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
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																																					
Jan 23																																					
Feb 23																																					
Mar 23																																					
Apr 23																																					
May 23																																					
Jun 23																																					

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

HoD
Department of IT

HEAD OF THE DEPARTMENT
Information Technology
Sir C.R.R. College of Engg
ELURU-534 007.

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. This course also gives the knowledge of Application layer, transport layer and network layer security protocols such as PGP,S/MIME,SSL, TSL etc.

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.

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	Introduction to cryptography	BB	CO1
2		Security goals	BB	CO1
3		Introduction to cryptographic attacks	BB	CO1
4		Non-cryptanalytic attacks	BB	CO1
5		Passive versus Active attacks	BB	CO1
6		Security services	PPT	CO1
7		Security mechanisms	PPT	CO1
8		Mathematics of cryptography	PPT	CO2
9		GCD, Extended Euclidean algorithm	BB/PPT	CO2
10		Matrices and linear congruence examples	BB	CO2
11	II	Mathematics of Symmetric Key Cryptography-groups	BB	CO2

12		Properties And rings	BB/PPT	CO1
13		Fields and properties	BB/PPT	CO1
14		Introduction to modern block ciphers	BB/PPT	CO1
15		Full size key substitution block ciphers	BB	CO1
16		Partial size key ciphers	BB	CO1
17		D boxes, compression D boxes	BB	CO1
18		Expansion D boxes	BB	CO1
19		S boxes procedure	BB	CO1
20		Linear Cryptanalysis	BB	CO2
21		Synchronous stream ciphers	BB	CO2
22		DES	BB	CO1
23		DES function	BB/PPT	CO2
24		Key generation	BB	CO2
25		DES analysis	BB/PPT	CO3
26	III	Advanced encryption standard	BB/PPT	CO3
27		Working of AES	BB	CO2
28		AES key expansion	BB	CO2
29		Introduction to Asymmetric Encryption and principles	BB	CO1
30		Mathematics of Asymmetric key	BB/PPT	CO2
31		Cardinality of primes	BB	CO2
32		Euler's theorem	BB	CO2
33		Factorization methods	BB	CO2
34		Public key cryptography	BB/PPT	CO2
35		RSA algorithm	BB	CO2
36		RSA algorithm analysis	BB/PPT	CO3
37		Diffie hellmen key Exchange algorithm	BB	CO3
38		Elgamal cryptosystem	BB	CO3
39		Key Encryption	BB	CO2
40		ECC encryption	BB/PPT	CO2

41		Hash function	BB	CO2
42		Applications of cryptographic functions	BB/PPT	CO2
43	IV	Digital signatures	BB	CO3
44		Requirements& security for a hash function	BB/PPT	CO1
45		SHA algorithm	BB	CO2
46		Message authentication functions	BB	CO3
47		HMAC algorithm	BB	CO2
48		Cipher based message authentication code	BB/PPT	CO2
49		Digital signatures	BB	CO2
50		Key management and distribution	BB/PPT	CO2
51	V	Introduction to network security	BB	CO2
52		Email security	BB	CO2
53		Pretty good privacy	BB	CO2
54		PGP algorithm	BB/PPT	CO2
55		Hash algorithm	BB	CO2
56		PGP certificates	BB/PPT	CO2
57		Public key ring model	BB	CO2
58		PGP packets	BB	CO1
59		PGP messages	BB	CO1
60		S/MIME	BB/PPT	CO3
61		Enveloped data content type	BB	CO3
62		SSL(Secure socket layer)	BB/PPT	CO3
63		Handshake protocol	BB	CO3
64		Security at network layer	BB	CO3
65		Two security protocols	BB	CO3
66		Encapsulating Security Payload(ESP**)**	BB/PPT	CO3
67		IPsec	BB	CO3
68		System security	BB	CO1

Evaluation Pattern

S. No	Components	Internal	External	Total
1	Theory	30	70	100
2	Engineering Graphics/Design/Drawing	30	70	100
3	Practical	15	35	50
4	Mini Project/Internship/Industrial Training/ Skill Development programmes/Research Project	-	50	50
5	Project Work	60	140	200

Marks Range Theory (Max – 100)	Marks Range Lab (Max – 50)	Level	Letter Grade	Grade Point
≥ 90	≥ 45	Outstanding	A+	10
≥80 to <89	≥40 to <44	Excellent	A	9
≥70 to <79	≥35 to <39	Very Good	B	8
≥60 to <69	≥30 to <34	Good	C	7
≥50 to <59	≥25 to <29	Fair	D	6
≥40 to <49	≥20 to <24	Satisfactory	E	5
<40	<20	Fail	F	0
-		Absent	AB	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)				CNS(A)	
Wed		CNS(B)			CNS(A)			
Thu								
Fri	CNS(A)		CNS(B)					
Sat			CNS(B)					

Unit wise Questions

Unit I

1. Tabulate the substitution Techniques in detail ?
2. Describe the Transposition Techniques in detail?
3. Explain the factorization?
4. List the different types of attacks and explain in detail.
5. Describe Chinese remainder theorem with example.
6. Evalute321 mod 11 using Fermat's theorem.
7. Summarize the following in detail (i) Modular Exponentiation (8) (ii) Finite fields
8. Apply Caesar cipher and k=5 decrypt the given Cipher text "YMJTYMJWXNIJTKXNQJSHJ".
9. Apply Vigenerecipher, encrypt the word "explanation" using the key "leg".
10. Discuss briefly the Discrete Algorithms.
11. Differentiate between transposition cipher and substitution cipher. Apply two stage transpositions Cipher on the "treat diagrams as single units" using the keyword "sequence".
12. Discuss about the Groups, Rings and Field

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 cardinality of primes?
2. Explain Euler's and Fermat's theorem?
3. Explain the overview of an asymmetric key cryptography with matrix of public and private key.
4. Explain the RSA algorithm with an example.

5. Explain the comparison between asymmetric and symmetric key cryptography.
6. Explain the digital signature with message digest algorithm.
7. Summarize the MD5 with working procedure.
8. Explain the secure Hash algorithm.
9. Explain the following:
   a. MAC b. HMAC
10. Discuss the Knapsack algorithm with an example.

Unit IV

1) Explain different schemes of iterated Hash functions.

2) Discuss about digital signature.

3) Define the Chinese remainder theorem and its applications.

4) Find the value of x for the following sets of congruence using Chinese remainder theorem $x \equiv 2 \mod 7$ and $x \equiv 3 \mod 9$. (c) Explain the Elliptic Curve Cryptosystem in detail.

5) What is digital signature? Explain Elliptic Curve Digital Signature Scheme. ?

6) Explain various public-key distribution methods.

Unit V

1. How does PGP provide authentication and confidentiality for email services and for file transfer applications? Draw the block diagram and explain the components.
2. (ii) Explain the general format of PGP message.
3. Summarize the Operations of PGP? Brief the various services provided by PGP. (ii) Discuss the threats faced by an e-mail and explain its security requirements to provide a secure e-mail service.
4. List the different protocols of SSL. Explain in detail Handshake protocol. (ii) Tell how does the server get authenticated to client in SSL?
5. Sketch and analyze the IPSec Document Overview diagram. Draw and explain PGP Cryptographic function for Authentication.
6. Differentiate between transport modes vs. tunnel mode encryption in IPsec.(8) (ii) With a neat diagram, Describe handshake protocol in SSL.
7. Analyze the Cryptographic algorithms used in S/MIME. (ii) Explain S/MIME certification processing