Accredited by NAAC

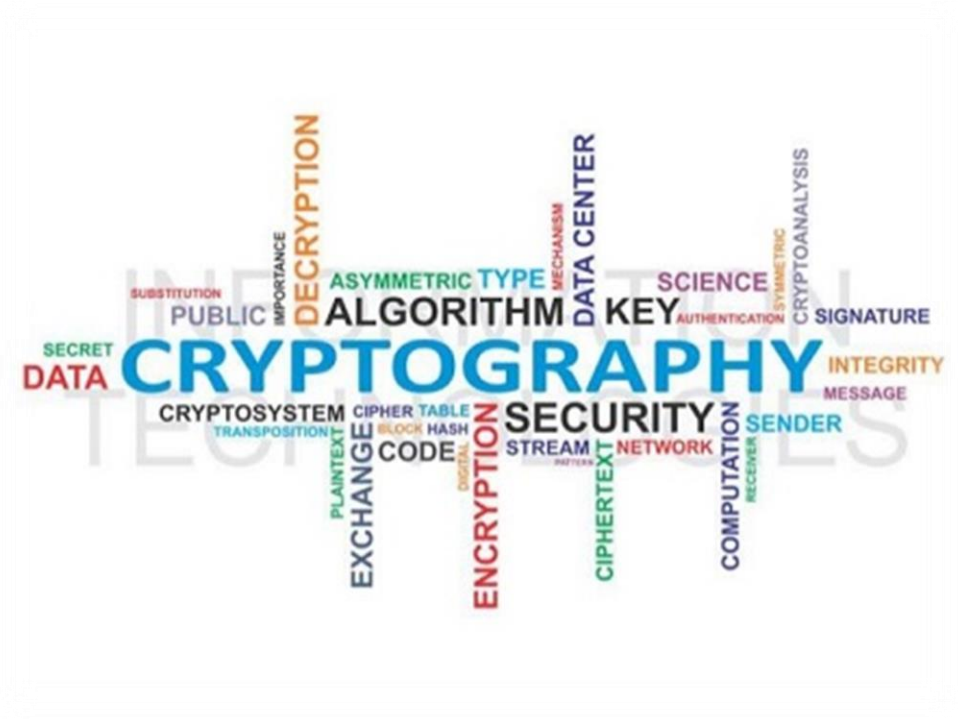
Accredited by NBA (CSE, ECE)

KOMMURI PRATAP REDDY INSTITUTE OF TECHNOLOGY

R18 JNTUH CSE IV-I SEMESTER

CS701PC: CRYPTOGRAPHY AND NETWORK SECURITY

ACADEMIC YEAR 2021-22 COURSE FILE



Prepared by

E.SAMATHA SREE CHATURVEDI

B.Tech, MBA (HR), M.Tech (CSE), (PhD-ML)

Assistant Professor

Department of CSE

Vision of the Institute

To emerge as a premier institute for high quality professional graduates who can contribute to economic and social developments of the Nation.

Mission of the Institute

Mission	Statement
IM_1	To have holistic approach in curriculum and pedagogy through industry interface to meet the needs of Global Competency.
IM_2	To develop students with knowledge, attitude, employability skills, entrepreneurship, research potential and professionally ethical citizens.
IM_3	To contribute to advancement of Engineering & Technology that would help to satisfy the societal needs.
IM_4	To preserve, promote cultural heritage, humanistic values and spiritual values thus helping in peace and harmony in the society.

Vision of the Department

To Provide Quality Education in Computer Science for the innovative professionals to work for the development of the nation.

Mission of the Department

Mission	Statement
DM_1	Laying the path for rich skills in Computer Science through the basic knowledge of mathematics and fundamentals of engineering
DM_2	Provide latest tools and technology to the students as a part of learning infrastructure
DM_3	Training the students towards employability and entrepreneurship to meet the societal needs.
DM_4	Grooming the students with professional and social ethics.

Program Educational Objectives (PEOs)

PEO's	Statement
PEO1	The graduates of Computer Science and Engineering will have successful career in technology.
PEO2	The graduates of the program will have solid technical and professional foundation to continue higher studies.
PEO3	The graduate of the program will have skills to develop products, offer services and innovation.
PEO4	The graduates of the program will have fundamental awareness of industry process, tools and technologies.

Program Outcomes

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, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
PO3	**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.
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 modelling 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 societal and environmental context, 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 network:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
PO10	**Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, 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 multidisciplinary environments.
PO12	**Life-Long learning:** Recognize the need for, and have the preparation and able to engage in independent and life-long learning in the broadest context of technological change.

PROGRAM SPECIFIC OUTCOME'S:

PSO1	**Foundation of mathematical concepts**: To use mathematical methodologies to crack problem using suitable mathematical analysis, data structure and suitable algorithm.
PSO2	**Foundation of Computer Science:** The ability to interpret the fundamental concepts and methodology of computer systems. Students can understand the functionality of hardware and software aspects of computer systems.
PSO3	**Foundation of Software development:** The ability to grasp the software development lifecycle and methodologies of software systems. Possess competent skills and knowledge of software design process.

SYLLABUS

UNIT - I

Security Concepts: Introduction, The need for security, Security approaches, Principles of security, Types of Security attacks, Security services, Security Mechanisms, A model for Network Security
Cryptography Concepts and Techniques: Introduction, plain text and cipher text, substitution techniques, transposition techniques, encryption and decryption, symmetric and asymmetric key cryptography, steganography, key range and key size, possible types of attacks.

UNIT - II

Symmetric key Ciphers: Block Cipher principles, DES, AES, Blowfish, RC5, IDEA, Block cipher operation, Stream ciphers, RC4.

Asymmetric key Ciphers: Principles of public key cryptosystems, RSA algorithm, Elgamal Cryptography, Diffie-Hellman Key Exchange, Knapsack Algorithm.

UNIT - III

Cryptographic Hash Functions: Message Authentication, Secure Hash Algorithm (SHA-512), Message authentication codes: Authentication requirements, HMAC, CMAC, Digital signatures, Elgamal Digital Signature Scheme.

Key Management and Distribution: Symmetric Key Distribution Using Symmetric & Asymmetric Encryption, Distribution of Public Keys, Kerberos, X.509 Authentication Service, Public – Key Infrastructure

UNIT - IV

Transport-level Security: Web security considerations, Secure Socket Layer and Transport Layer Security, HTTPS, Secure Shell (SSH)

Wireless Network Security: Wireless Security, Mobile Device Security, IEEE 802.11 Wireless LAN, IEEE 802.11i Wireless LAN Security

UNIT - V

E-Mail Security: Pretty Good Privacy, S/MIME IP Security: IP Security overview, IP Security architecture, Authentication Header, Encapsulating security payload, Combining security associations, Internet Key Exchange

Case Studies on Cryptography and security: Secure Multiparty Calculation, Virtual Elections, Single sign On, Secure Inter-branch Payment Transactions, Cross site Scripting Vulnerability.

TEXT BOOK

1. Cryptography and Network Security - Principles and Practice: William Stallings, Pearson Education, 6th Edition

2. Cryptography and Network Security: Atul Kahate, Mc Graw Hill, 3rd Edition

REFERENCES

1. Cryptography and Network Security: C K Shyamala, N Harini, Dr T R Padmanabhan, Wiley India, 1st Edition.

2. Cryptography and Network Security: Forouzan Mukhopadhyay, Mc Graw Hill, 3rd Edition

3. Information Security, Principles, and Practice: Mark Stamp, Wiley India.

4. Principles of Computer Security: WM. Arthur Conklin, Greg White, TMH

5. Introduction to Network Security: Neal Krawetz, CENGAGE Learning

6. Network Security and Cryptography: Bernard Menezes, CENGAGE Learning

COURSE OBJECTIVES

- Explain the objectives of information security
- Explain the importance and application of each of confidentiality, integrity, authentication and availability
- Understand various cryptographic algorithms.
- Understand the basic categories of threats to computers and networks
- Describe public-key cryptosystem.
- Describe the enhancements made to IPv4 by IPSec
- Understand Intrusions and intrusion detection
- Discuss the fundamental ideas of public-key cryptography.
- Generate and distribute a PGP key pair and use the PGP package to send an encrypted email message.
- Discuss Web security and Firewalls

COURSE OUTCOMES

Students will be able to:

C411.1:Classifythe various classical encryption techniques. [Understand]

C411.2:Comparevarious Public key cryptographic techniques. [Analyze]

C411.3:Evaluateauthentication and hash algorithms. [Apply]

C411.4: Choose the intrusion detection and its solutions to overcome the attacks. [Evaluate]

C411.5: Develop strong password methods. [Create]

Mapping of Course Outcomes with PO's and PSO's:

High -3 Medium -2 Low-1

Course Outcomes	Program Outcomes												Program Specific Outcomes		
CO/PO	**PO 1**	**PO 2**	**PO 3**	**PO 4**	**PO 5**	**PO 6**	**PO 7**	**PO 8**	**PO 9**	**PO 10**	**PO 11**	**PO 12**	**PSO1**	**PSO2**	**PSO3**
C411.1	3	3	-	-	-	-	-	-	-	2	-	3	3	3	2
C411.2	3	2	-	-	-	-	-	-	-	2	2	-	2	-	-
C411.3	3	2	-	-	-	2	-	-	-	-	-	-	-	-	-
C411.4	3	3	3	3	2	-	-	-	3	3	3	-	3	3	3
C411.5	3	2	3	3	3	-	-	-	3	3	3	3	3	3	3
C411	3	2.4	1.5	1.5	1	0.4	-	-	1.5	2	1.6	1.5	2.2	1.8	1.6

CO-PO Mapping Justification

C411.1:Classifythe various classical encryption techniques. [Understand]

	Justification
PO1	Students will be able to know the concept of Mathematics.
PO2	Students will be able to solve complex problems and interpret the data.
PO10	Students will be able to communicate with the people effectively.
PO12	Students will be able to know how to learn about the evolving technologies.

C411.2:Comparevarious Public key cryptographic techniques.[Analyze]

	Justification
PO1	Students will able to identify different problems and they can analyze.
PO2	Students will able to analyze the complexity of the problems.
PO10	Students will be able to explain the encryption and decryption techniques easily.

PO11	Students will be able to learn the principles of cryptographic techniques.

C411.3:Evaluateauthentication and hash algorithms.[Apply]

	Justification
PO1	Students will be able to apply the knowledge of basic mathematics while using algorithms.
PO2	Students will be able to design the solutions for different authentication mechanisms.
PO6	Students will be able to evaluate the algorithms based on the contextual knowledge.

C411.4: Choose the intrusion detection and its solutions to overcome the attacks.[Evaluate]

	Justification
PO1	Students will be able to apply the mathematical knowledge on the different attacks.
PO2	Students will be able to develop the solutions for different types of attacks the system will undergo.
PO3	Students will be able to design the solutions to overcome the attacks.
PO4	Students will be able to conduct interpretation of data and provide proper conclusions.
PO5	Students will be able to learn the modern tools which are used to overcome the attacks.
PO9	Students will be able to communicate as an individual if any attack occurs.
PO10	Students will be able to make effective presentations on the recent attack.
PO11	Students will be able to apply all these mechanisms in different environments.

C411.5: Developstrong password methods.[Create]

	Justification
PO1	Students will be able to generate passwords by applying the knowledge of mathematics.
PO2	Students will be able to design and develop the strong passwords to overcome the attacks.
PO3	Students will be able design solutions for complex problems.
PO4	Students will be able to analyze and interpret the data based on the problem.
PO5	Students will be able to learn the new tools which are used for developing passwords.
PO9	Students will be able to do any work effectively in any environment.
PO10	Students will be able to write effective reports and make effective presentations.
PO11	Students will be able to demonstrate their work in any environment.
PO12	Students will be able to recognize the need for developing the methods to create passwords.

Lesson Plan – (CS701PC) CRYPTOGRAPHY AND NETWORK SECURITY

Faculty Name: E.Samatha Sree	**Year/Sem:** IV/I	**Academic Year:** 2021-2022

w.e.f: 06-09-2021

L. No	Name of the Topic	Plan Date	Actual Date	Teaching Method
1	**UNIT – 1** Introduction	**06-09-2021**	06-09-2021	Chalk & Talk
2	The Need for Security	**08-09-2021**	08-09-2021	Chalk & Talk
3	Security Approaches ,Principles Of Security	**09-09-2021**	09-09-2021	Chalk & Talk
4	Types Of Security Attacks	**10-09-2021**	10-09-2021	Chalk & Talk
5	Security Services ,Security Mechanisms	**15-09-2021**	16-09-2021	Chalk & Talk
6	A Model for Network Security.	**16-09-2021**	16-09-2021	Chalk & Talk
7	Introduction, Plain text and Cipher Text, Substitution Techniques,	**17-09-2021**	17-09-2021	Chalk & Talk
8	Transposition Techniques	**18-09-2021** **22-09-2021**	18-09-2021 22-09-2021	Chalk & Talk
10	Encryption & Decryption	**23-09-2021**	23-09-2021	Chalk & Talk
11	Symmetric and Assymetric Cryptography	**24-09-2021** **25-09-2021**	25-09-2021	Chalk & Talk
13	Steganography, Key range and Key Size	**29-09-2021**	30-09-2021	Chalk & Talk
14	Possible Types Of Attacks.	**30-09-2021**	30-09-2021	Chalk & Talk
15	Review	**30-09-2021**	01-10-2021	Chalk & Talk
15	**UNIT – 2** Block Cipher Principles	**01-10-2021**	01-10-2021	Chalk & Talk

16	DES,AES	**07-10-2021**	07-10-2021	Chalk & Talk
17	Blowfish ,RC5	**08-10-2021**	18-10-2021	Chalk & Talk
18	IDEA	**20-10-2021**	19-10-2021	Chalk & Talk
19	Block Cipher Operation	**21-10-2021**	21-10-2021	Chalk & Talk
20	Stream Ciphers,RC4	**22-10-2021**	22-10-2021	Chalk & Talk
21	Principles of Public Key Crypto Systems	**23-10-2021**	23-10-2021	Chalk & Talk
22	RSA Algorithm, Elgamal Cryptography	**27-10-2021**	27-10-2021	Chalk & Talk
23	Diffie Hellman Key Exchnage, Knapsack Algorithm	**28-10-2021**	28-10-2021	Chalk & Talk
	Review	**29-10-2021**	29-10-2021	Chalk & Talk
24	**UNIT – 3** Message Authentication , Secure Hash Algorithm (SHA -512)	**29-10-2021**	29-10-2021	Chalk & Talk
25	Authentication Requirements, HMAC	**30-10-2021**	30-10-2021	Chalk & Talk
26	CMAC	**03-11-2021**	03-11-2021	Chalk & Talk
27	Digital Signatures	**04-11-2021**	04-11-2021	Chalk & Talk
28	Elgamal Digital Signature Scheme.	**05-11-2021**	05-11-2021	Chalk & Talk
29	Symmetric Key Distribution Using Symmetric and Asymmetric Encryption	**06-11-2021**	06-11-2021	Chalk & Talk
30	Symmetric Key Distribution Using Symmetric and Asymmetric Encryption	**17-11-2021**	17-11-2021	Chalk & Talk
31	Distribution of Public Key	**18-11-2021**	18-11-2021	Chalk & Talk
32	Kerberos	**19-11-2021**	19-11-2021	Chalk & Talk

33	X.509 Authentication Service	**20-11-2021**	20-11-2021	Chalk & Talk
34	Public Key Infrastructure	**24-11-2021** **25-11-2021**	25-11-2021	Chalk & Talk
35	Review	**25-11-2021**	26-11-2021	Chalk & Talk
36	**UNIT – 4** Web Security Considerations	**26-11-2021**	26-11-2021	Chalk & Talk
37	Secure Socket Layer and Transport Layer Security	**27-11-2021**	27-11-2021	Chalk & Talk
38	HTTPS , Secure Shell (SSH).	**01-12-2021**	01-12-2021	Chalk & Talk
39	Wireless Security , Mobile Device Security	**02-12-2021**	02-12-2021	Chalk & Talk
40	IEEE 802.11 Wireless LAN	**03-12-2021**	03-12-2021	Chalk & Talk
41	IEEE 802.11i Wireless LAN Security	**04-12-2021**	04-12-2021	Chalk & Talk
	Review	**04-12-2021**	04-12-2021	Chalk & Talk
	UNIT – 5			
42	Pretty Good Privacy	**08-12-2021**	08-12-2021	Chalk & Talk
43	S/MIME	**09-12-2021**	09-12-2021	Chalk & Talk
44	IP Security Overview	**10-12-2021**	10-12-2021	Chalk & Talk
45	IP Security Architecture	**15-12-2021**	15-12-2021	Chalk & Talk
46	Authentication Header	**16-12-2021**	16-12-2021	Chalk & Talk
47	Encapsulating Security Payload	**17-12-2021**	17-12-2021	Chalk & Talk
48	Combining Security Associations	**18-12-2021**	18-12-2021	Chalk & Talk

49	Internet Key Exchange	**22-12-2021**	22-12-2021	Chalk & Talk
50	Secure Multi Party Calculation	**23-12-2021**	23-12-2021	Chalk & Talk
51	Virtual Elections	**24-12-2021**	24-12-2021	Chalk & Talk
52	Single Sign on	**29-12-2021**	29-12-2021	Chalk & Talk
53	Secure Inter Branch Payment Transactions	**30-12-2021**	30-12-2021	Chalk & Talk
54	Secure Inter Branch Payment Transactions	**31-12-2021**	31-12-2021	Chalk & Talk
55	Cross site Scripting Vulnerability	**05-01-2022**	05-01-2022	Chalk & Talk
56	Review	**06-01-2022**	06-01-2022	Chalk & Talk

Web resources:

1. https://nptel.ac.in/courses/106/105/106105031/

2. https://en.wikipedia.org/wiki/Cryptography

TIME TABLE

Class: IV-B.Tech I Sem **A.Y: 2021-22** **W.E.F- 06-09-2021**
LH:- B-303

Period / Day	I 9:30-10:20	II 10:20 -11:10	11:10-11:20	III 11:20-12:10	IV 12:10-1:00	1:00-1:40	V 1:40-2:30	VI 2:30-3:20	VII 3:20-4:10
MON	Electronic Sensors		BREAK	CGNS LAB/IOMP		LUNCH	SEED CLASSES		
TUE	ASN			CGNS LAB/IOMP			SEED CLASSES		
WED	CGNS	SEED		SEED CLASSES			SPPM	ASN	DM
THU	ASN	DM		SPPM	LIB/INT		CGNS	Electronic Sensors	SPORTS
FRI	DM	SPPM		Electronic Sensors	CGNS		Project Stage-1		REM/COUNS
SAT	SPPM	CGNS		ASN	Electronic Sensors		DM	SEMINAR	

UNIVERSITY CALENDAR

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

Academic Calendar 2021-22

B. TECH./B.PHARM. III & IV YEARS I & II SEMESTERS

I SEM

S. No	Description	Duration	
		From	To
1	Commencement of I Semester classwork	**06.092021**	
2	1st Spell of Instructions (including Dussehra Recess)	06.09.2021	06.11.2021 (9 Weeks)
3	Dussehra Recess	11.10.2021	16.10.2021 (1 Week)
4	First Mid Term Examinations	08.11.2021	13.11.2021 (1 Week)
5	Submission of First Mid Term Exam Marks to the University on or before	20.11.2021	
6	2nd Spell of Instructions	15.11.2021	08.01.2022 (8 Weeks)
7	Second Mid Term Examinations	10.01.2022	18.01.2022 (1 Week)
8	Preparation Holidays and Practical Examinations	19.01.2022	25.01.2022 (1 Week)
9	Submission of Second Mid Term Exam Marks to the University on or before	25.01.2022	
10	End Semester Examinations	27.01.2022	09.02.2022

ASSIGNMENT-1

1. Explain model for Internetwork Security.
2. Discuss about the types of Security attacks in network security
3. Differentiate symmetric and asymmetric key cryptography?.
4. Use RSA algorithm, Perform encryption and decryption with p=3,q=11,e=7 and N=5.
5. Explain briefly about DES algorithm.
6. Explain the Cipher block modes of operation**.**
7. Draw a neat sketch to explain the concept of Secured Hash Algorithm (SHA)
8. Explain about the process of Diffie Hellman Key Exchange Algorithm.

ASSIGNMENT-2

1. Describe HMAC Algorithm.
2. Describe Signing and Verification in Digital Signature Algorithm.
3. Describe Signing and Verification in Digital Signature Algorithm.
4. What is meant by transport mode and tunnel mode? How is authentication header implemented in these two modes?
5. Explain IP security architecture and also explain basic combinations of security associations with neat diagram.
6. Discuss IEEE 802.11i Wireless LAN Security.
7. Give a brief note on virtual elections.
8. Explain the four protocols defined by secure socket layer.

The following Table Contains Digital Notes Links.

Name of the Content	**Resource URL**
Digital Notes Unit-I to Unit-V	**https://drive.google.com/file/d/1Ujh9frWCwV7SS9aOWhd0AxKAtWhe6Rrv/view?usp=sharing**