



INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

Dundigal, Hyderabad - 500 043

COMPUTER SCIENCE AND ENGINEERING

COURSE DESCRIPTION FORM

Course Title	INFORMATION SECURITY			
Course Code	A60522			
Regulation	R15 - JNTUH			
Course Structure	Lectures	Tutorials	Practicals	Credits
	4	-	-	4
Course Coordinator	Ms. Geetavani.B, Assistant Professor, CSE			
Team of Instructors	Dr. P L Srinivasa Murthy ,Professor ,CSE Mr. N Rajasekar, Assistant Professor, CSE Mr. P V Narsimha Rao, Assistant Professor, CSE			

I. COURSE OVERVIEW:

This course provides an introduction to the field of network security. Specific topics to be examined include threats and vulnerabilities to network architectures and protocols. The course is designed to provide fundamental skills needed to analyze the internal and external security threats against a network, and to develop security policies that will protect an organization's information. Students will learn how to evaluate network and Internet security issues and design.

II. PREREQUISITE(S):

Level	Credits	Periods/ Week	Prerequisites
UG	4	4	Computer Networks

III. MARKS DISTRIBUTION:

Sessional Marks	University End Exam marks	Total marks
Midterm Test There shall be two midterm examinations. Each midterm examination consists of essay paper, objective paper and assignment. The essay paper is for 10 marks of 60 minutes duration and shall contain 4 questions. The student has to answer 2 questions, each carrying 5 marks. The objective paper is for 10 marks of 20 minutes duration. It consists of 10 multiple choice and 10 fill-in-the blank questions, the student has to answer all the questions and each carries half mark. First midterm examination shall be conducted for the first two and half units of syllabus and second midterm examination shall be conducted for the remaining portion. Five marks are earmarked for assignments. There shall be two assignments in	75	100

Sessional Marks	University End Exam marks	Total marks
every theory course. Assignments are usually issued at the time of commencement of the semester. These are of problem solving in nature with critical thinking. Marks shall be awarded considering the average of two midterm tests in each course.		

IV. EVALUATION SCHEME:

S. No	Component	Duration	Marks
1.	I Mid Examination	80 minutes	20
2.	I Assignment	-	5
3.	II Mid Examination	80 minutes	20
4.	II Assignment	-	5
5.	External Examination	3 hours	75

V. COURSE OBJECTIVES:

At the end of the course, the students will be able to:

- I. Identify and classify computer and security threats and develop a security model to prevent, detect and recover from attack
- II. Understand various public-key cryptographic Algorithms.
- III. Study PGP key pair and use the PGP package to send an encrypted e-mail message.
- IV. Understand IP protocol security through IPSec.
- V. Analyze security of data in network through firewall.

VI. COURSE OUTCOMES:

After completing this course the student must demonstrate the knowledge and ability to:

1. Differentiate network security and computer security.
2. Understand various attacks on network.
3. Understand various conventional cryptography algorithms and asymmetric encryption algorithms.
4. Expertise in Message authentication, Hash function and Public key encryption.
5. Analyze how PGP and S/MIME is used to protect messages transmitted through e-mail
6. Remembering requirements for web security and implementing security through SSL/TLS.
7. Understand various intruders, firewall design principles.

VII. HOW PROGRAM OUTCOMES ARE ASSESSED:

Program Outcomes		Level	Proficiency assessed by
PO1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.	H	Assignments, Tutorials
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.	H	Assignments
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.	H	Mini Projects
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.	S	--
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.	S	Mini Projects
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.	N	--
PO7	Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	N	--
PO8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.	N	--
PO9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	N	--
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.	N	--
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.	N	--
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.	S	--

N – None

S – Supportive

H - Highly Related

VIII. HOW PROGRAM SPECIFIC OUTCOMES ARE ASSESSED:

Program Specific Outcomes		Level	Proficiency assessed by
PSO1	Professional Skills: The ability to research, understand and implement computer programs in the areas related to algorithms, system software, multimedia, web design, big data analytics, and networking for efficient analysis and design of computer-based systems of varying complexity.	H	Lectures, Assignments
PSO2	Problem-Solving Skills: The ability to apply standard practices and strategies in software project development using open-ended programming environments to deliver a quality product for business success.	H	Projects
PSO3	Successful Career and Entrepreneurship: The ability to employ modern computer languages, environments, and platforms in creating innovative career paths, to be an entrepreneur, and a zest for higher studies.	S	Guest Lectures

N - None

S - Supportive

H - Highly Related

IX. SYLLABUS:

UNIT – I

Attacks on Computers and Computer Security: Introduction, The need for security, Security approaches, Principles of security, Types of Security attacks, Security Services, Security Mechanism, 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 & Algorithms (DES, AES, Blowfish), Differential and Linear Cryptanalysis, Block cipher modes of operation, Stream ciphers, RC4 Location, and placement of encryption function, key distribution Asymmetric key Ciphers: Principles of public key cryptosystems, Algorithms (RSA Diffie-Helman, ECC) Key Distribution.

UNIT – III

Message Authentication Algorithm and Hash Functions: Authentication requirements, Functions, Message, authentication codes, Hash Functions, Secure hash algorithm, Whirlpool, HMAC, CMAC, Digital Signatures, knapsack algorithm

Authentication Application: Kerberos, X.509 Authentication Service, Public – Key Infrastructure, Biometric Authentication.

UNIT – IV

E-mail Security: Pretty Good Privacy, S/MIME IP Security: IP Security overview, IP Security architecture, Authentication Header, Encapsulating Security payload, Combining Security associations, key management.

UNIT – V

Web Security: Web security considerations, Secure Socket Layer and Transport Layer Security, Secure electronic transaction Intruders, Virus and Firewalls: Intruders, Intrusion detection password management, virus and related threats, Countermeasures, Firewall design principles, Types of firewalls.

Case Studies on Cryptography and Security: Secure Inter-branch Payment Transactions, Cross site Scripting Vulnerability, Virtual Electronics.

TEXT BOOKS:

1. Cryptography and Network Security: William Stallings, Pearson Education, 4th Edition.
2. Cryptography and Network Security: Atul Kahate, McGraw Hill, 2nd Edition.

REFERENCE BOOKS:

1. Cryptography and Network Security: C K Shymala, N harini, Dr. T R Padmanabhan, Wiley India, 1st Edition.
2. Cryptography and Network Security: Forouzan Mukhopadhyay, Mc Graw Hill 2nd Edition.
3. Information Security, Principles and Practice: Mark Stamp, WileyIndia.
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.

X. COURSE PLAN:

At the end of the course, the students are able to achieve the following course learning outcomes:

Lecture No.	Topics to be covered	Course Learning Outcomes	Reference
1 – 3	Introduction, The need for security, Security approaches, Principles of security Types of Security attacks, Security	Understand the importance of identifying threats to network	T1:1.3-1.7
4 – 6	Security Mechanism, A model for Network Security. Introduction, plain text and cipher text	Evaluate various types of attacks on the network.	R2, R3
7-12	transposition techniques encryption and decryption symmetric and asymmetric key cryptography, steganography	Understand how Unauthorized person acquires data in middle of transmission of data in network	T1:2.1-2.2,2.4
12-16	key range and key size Possible types of attacks. Symmetric key Ciphers Block Cipher principles	Analyze how security depends on location of encryption devices in network	T1:2.5-2.6,3.1
17-22	Algorithms (DES,AES, Blowfish) Block cipher modes of operation Stream ciphers	Understand various public key cryptography algorithms	T1:3.3-3.4
23-26	RC4 Location placement of encryption function	Illustrate how security provided through signature	T1:3.5,3.6,
27-33	key distribution Asymmetric key Ciphers Principles of public key cryptosystems	Compare various security aspects for entering into secure network	T1:4.1-4.2
34-37	Algorithms (RSA Diffie-Helman, ECC) Key Distribution Message Authentication Algorithm and HashFunctions: Authentication requirements	Understand various methods of message authentication algorithms	T1:5.1
38-40	Functions, Message authentication codes, Hash Functions Secure hash algorithm	Understand how authentication header provides authentication	T1:5.2
41-45	Whirlpool, HMAC, CMAC Digital Signatures, knapsack algorithm Authentication Application: Kerberos	Analyze the importance of secured architecture for internet protocol	T1:6.1-6.3
46-49	Public – Key Infrastructure, Biometric Authentication. Pretty Good Privacy S/MIME IP Security: IP Security overview	Understand PGP functionality	T1:7.1-7.2
50-54	IP Security architecture, Authentication Header Encapsulating Security payload, Combining Security associations, key Management.	Understand how devices are managed on IP network	T1:7.2-7.3
55-59	Web security considerations, Secure Socket Layer and Transport Layer Security	Analyze how SSL provides security in www	T1:8.1-8.3
60-63	Types of firewalls virus and related threats, Countermeasures, Firewall design principles.	Understand various types of firewalls and viruses.	T:11.1-11.2
64-65	Case Studies on Cryptography and Security: Secure Inter-branch Payment Transactions, Cross site Scripting Vulnerability, Virtual Electronics	Analyze different Inter branch payment transactions cross site Scripting.	T:11.2-11.6

XI. MAPPING COURSE OBJECTIVES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Objectives	Program Outcomes												Program Specific Outcomes		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
I	H	H										S	H	S	
II	S	H	H										H	S	
III			H	S									S	H	
IV	H	S											H	S	
V		H			S								H		S

S – Supportive

H - Highly Related

XII. MAPPING COURSE OUTCOMES LEADING TO THE ACHIEVEMENT OF PROGRAM OUTCOMES AND PROGRAM SPECIFIC OUTCOMES:

Course Outcomes	Program Outcomes												Program Specific Outcomes		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
1	H	S	S										H	S	
2	H			S						H			S	H	
3					S								H	S	
4	S	H						H		S			S		H
5	H	S				H							S	H	
6	H			S								S	H	S	
7	S			H						H			S	H	

S – Supportive

H - Highly Related

Prepared By,

Geetavani.B, Assistant Professor, CSE

Dr. P L Srinivasa Murthy, Professor, CSE

Mr. N.Rajasekar, Assistant Professor, CSE

Mr. P V Narasimha Rao , Assistant Professor, CSE

HOD, CSE