INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)
Dundigal, Hyderabad -500 043

COMPUTER SCIENCE AND ENGINEERING

COURSE DESCRIPTOR

Course Title	**INFORMATION SECURITY**				
Course Code	**ACS013**				
Programme	B.Tech				
Semester	VIII	CSE | IT			
Course Type	Core				
Regulation	IARE - R16				
Course Structure	**Theory**			**Practical**	
	Lectures	**Tutorials**	**Credits**	**Laboratory**	**Credits**
	3	-	3	-	-
Chief Coordinator	Ms. B Geetavani, Assistant Professor				
Course Faculty	Ms. P Navya, Assistant Professor Ms B Anupama, Assistant Professor Ms B Swathi, Assistant Professor				

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. COURSE PRE-REQUISITES:

Level	Course Code	Semester	Prerequisites	Credits
UG	ACS013	IV	Computer Networks	3

III. MARKSDISTRIBUTION:

Subject	SEE Examination	CIA Examination Examination	Total Marks
Information Security	70 Marks	30 Marks	100

IV. DELIVERY / INSTRUCTIONAL METHODOLOGIES:

✔	Chalk & Talk	✔	Quiz	✔	Assignments	✔	MOOCs
✔	LCD / PPT	✔	Seminars	✘	Mini Project	✔	Videos
✘	Open Ended Experiments						

V. EVALUATION METHODOLOGY:

The course will be evaluated for a total of 100 marks, with 30 marks for Continuous Internal Assessment (CIA) and 70 marks for Semester End Examination (SEE). Out of 30 marks allotted for CIA during the semester, marks are awarded by taking average of two CIA examinations or the marks scored in the make-up examination.

Semester End Examination (SEE): The SEE is conducted for 70 marks of 3 hours duration. The syllabus for the theory courses is divided into fiveunits and each unit carries equal weightage in terms of marks distribution. The question paper pattern is as follows. Two full questions with "either‟ or ‟choice" will be drawn from each unit. Each question carries 14 marks. There could be a maximum of two sub divisions in a question.

The emphasis on the questions is broadly based on the following criteria:

50 %	To test the objectiveness of the concept.
50 %	To test the analytical skill of the concept OR to test the application skill of the concept.

Continuous Internal Assessment (CIA):
CIA is conducted for a total of 30 marks (Table 1), with 25 marks for Continuous Internal Examination (CIE), 05 marks for Quiz/ Alternative Assessment Tool (AAT).

Table 1: Assessment pattern for CIA

Component	**Theory**		**Total Marks**
Type of Assessment	CIE Exam	Quiz / AAT	
CIA Marks	25	05	30

Continuous Internal Examination (CIE):
Two CIE exams shall be conducted at the end of the 8th and 16th week of the semester respectively. The CIE exam is conducted for 25 marks of 2 hours duration consisting of two parts. Part–A shall have five compulsory questions of one mark each. In part–B, four out of five questions have to be answered where, each question carries 5 marks. Marks are awarded by taking average of marks scored in two CIE exams.

Quiz / Alternative Assessment Tool (AAT):
Two Quiz exams shall be online examination consisting of 25 multiple choice questions and are be answered by choosing the correct answer from a given set of choices (commonly four). Marks shall be awarded considering the average of two quizzes for every course. The AAT may include seminars, assignments, term paper, open ended experiments, five minutes video and MOOCs.

VI. HOW PROGRAM OUTCOMES ARE ASSESSED:

Program Outcomes (POs)		**Strength**	**Proficiency assessed by**
PO1	**Engineering knowledge**: Apply the knowledge of mathematics, science, engineeringfundamentals, and an engineering specialization to the solution of complex engineering problems.	3	Assignments
PO2	**Problem analysis**: Identify, formulate, review research literature, and analyze complexengineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	2	Assignments
PO3	**Design/development of solutions**: Design solutions for complex engineering problems anddesign 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.	3	Guest Lectures

Program Outcomes (POs)		Strength	Proficiency assessed by
PO4	**Conduct investigations of complex problems**: Use research-based knowledge and researchmethods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	2	5 minutes Video/ Seminars
PO5	**Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modernengineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.	3	Seminars / Term Paper/ 5 minutes video

3 = High; 2 = Medium; 1 = Low

VII. HOW PROGRAM SPECIFIC OUTCOMES ARE ASSESSED:

Program Specific Outcomes (PSOs)		Strength	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.	2	Lectures, Assignments
PSO2	**Software Engineering Practices:** The ability to apply standard practices and strategies in software service management using open-ended programming environments with agility to deliver a quality service for business success	2	Seminars
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.	2	Guest Lectures

3 = High; 2 = Medium; 1 = Low

VIII. COURSE OBJECTIVES (COs):

The course should enable the students to:	
I	Learn the basic categories of threats to computers and networks
II	Understand various cryptographic algorithms and be familiar with public-key cryptography.
III	Apply authentication functions for providing effective security.
IV	Analyze the application protocols to provide web security.
V	Discuss the place of ethics in the information security area.

IX. COURSE OUTCOMES (COs):

CO'S	COURSE OUTCOMES	CLO'S	COURSE LEARNING OUTCOMES
CO 1	Understand the basic Concepts of attacks on computer,computer security.	CLO 1	Understand the different types of attacks, security mechanisms, security services.
		CLO 2	Explainvarious substitution techniques such as play-fair cipher, mono-alphabetic cipher and hill cipher.
		CLO 3	Understand various Transposition techniques such as row transposition and rail-fence.
		CLO 4	Describe the role of private and public key in encryption and decryption and key size.
		CLO 5	Apply the symmetric algorithm for message transmission and analyze the security level of it.
		CLO 6	Understand various asymmetric key encryption algorithms for message encryption and decryption.

CO’S	COURSE OUTCOMES	CLO’S	COURSE LEARNING OUTCOMES
CO 2	Understand the concepts of symmetric key ciphers.	CLO 7	Understand the block cipher modes of operation for encryption and decryption.
		CLO 8	Describe the need of stream ciphers in message encryption.
		CLO 9	Understand the role of elliptic curve cryptography in security.
		CLO 10	Analyze the drawbacks of RSA and able to design a security algorithm which overcomes that drawbacks.
CO 3	Describe the message authentication algorithm and hash functions.	CLO 11	Explain the role of the message authentication in message transmission.
		CLO 12	Explain the need of digital signature in message transmission.
		CLO 13	Explain and demonstrate the role of different types of hash functions for providing security.
		CLO 14	Understand the differences between the symmetric and symmetric cryptography algorithms for providing security.
CO 4	Understand the concepts of e-mail security.	CLO 15	Explain S/MIME and PGP for transmitting mail from sender to receiver.
		CLO 16	Explain IP security for internet protocol and analyze how it provides security.
CO 5	Understand the concepts of web security.	CLO 17	Describe the security socket layer and transport layer security for web security.
		CLO 18	Demonstrate various types of intrusion detection techniques.
		CLO 19	Understand various types of viruses and its vulnerabilities.
		CLO 20	Describe various types of firewalls and analyze the security levels of these.

X. COURSE LEARNING OUTCOMES (CLOs):

CLO Code	CLO’s	At the end of the course, the student will have the ability to:	PO’s Mapped	Strength of Mapping
ACS013.01	CLO 1	Understand the different types of attacks, security mechanisms, security services.	PO1, PO2	2
ACS013.02	CLO 2	Explainvarious substitution techniques such as play-fair cipher, mono-alphabetic cipher and hill cipher.	PO1, PO2	2
ACS013.03	CLO 3	Understand various Transposition techniques such as row transposition and rail-fence.	PO2, PO5	3
ACS013.04	CLO 4	Describe the role of private and public key in encryption and decryption and key size.	PO3	3
ACS013.05	CLO 5	Apply the symmetric algorithm for message transmission and analyze the security level of it.	PO2, PO3	3
ACS013.06	CLO 6	Understand various asymmetric key encryption algorithms for message encryption and decryption.	PO2, PO5	3
ACS013.07	CLO 7	Understand the block cipher modes of operation for encryption and decryption.	PO3, PO4	2
ACS013.08	CLO 8	Describe the need of stream ciphers in message encryption.	PO2, PO4	1
ACS013.09	CLO 9	Understand the role of elliptic curve cryptography in security.	PO2	3

CLO Code	CLO's	At the end of the course, the student will have the ability to:	PO's Mapped	Strength of Mapping
ACS013.10	CLO 10	Analyze the drawbacks of RSA and able to design a security algorithm which overcomes that drawbacks.	PO2, PO3	2
ACS013.11	CLO 11	Explain the role of the message authentication in message transmission.	PO1, PO2	2
ACS013.12	CLO 12	Explain the need of digital signature in message transmission.	PO2, PO5	2
ACS013.13	CLO 13	Explain and demonstrate the role of different types of hash functions for providing security.	PO1, PO2	3
ACS013.14	CLO 14	Understand the differences between the symmetric and symmetric cryptography algorithms for providing security.	PO1, PO2	3
ACS013.15	CLO 15	Explain S/MIME and PGP for transmitting mail from sender to receiver.	PO2, PO3	2
ACS013.16	CLO 16	Explain IP security for internet protocol and analyze how it provides security.	PO2	3
ACS013.17	CLO 17	Describe the security socket layer and transport layer security for web security.	PO2	2
ACS013.18	CLO 18	Demonstrate various types of intrusion detection techniques.	PO1, PO2	3
ACS013.19	CLO 19	Understand various types of viruses and its vulnerabilities.	PO2, PO3	2
ACS013.20	CLO 20	Describe various types of firewalls and analyze the security levels of these.	PO4	2

3 = High; 2 = Medium; 1 = Low

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

Course Outcomes	Program Outcomes (POs)					Program Specific Outcomes (PSOs)		
	PO1	PO2	PO3	PO4	PO5	PSO1	PSO2	PSO3
CO 1	3	3	3		3	2		
CO 2		2		2		2	2	
CO 3	3	2			3	2	2	
CO 4		2	3			2	2	
CO 5	3	2	3	3		2	2	2

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

CLOs	Program Outcomes (POs)												Program Specific Outcomes (PSOs)		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CLO 1	3	2											2		
CLO 2	3	2											3		
CLO 3		3			3								2		

CLOs	Program Outcomes (POs)												Program Specific Outcomes (PSOs)		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CLO 4			3										3		
CLO 5		3	3										2		
CLO 6		3			3								2		
CLO 7			3	2										2	
CLO 8		1		2									2		
CLO 9		3													
CLO 10		2		2										3	
CLO 11	3	2												2	
CLO 12		1			3								2		
CLO 13	3	2												2	
CLO 14	3	2												2	
CLO 15		2	3										2	3	
CLO 16		2												2	
CLO 17		2													2
CLO 18	3	3												2	
CLO 19		2	3										2		
CLO 20				3										2	

3 = High; 2 = Medium; 1 = Low

XIII. ASSESSMENT METHODOLOGIES–DIRECT

CIE Exams	PO1, PO2, PO3, PO4, PO5,PSO1, PSO2,PSO3	SEE Exams	PO1, PO2, PO3, PO4, PO5, PSO1,PSO2 ,PSO3	Assignments	PO1	Seminars	PO2
Laboratory Practices	-	Student Viva	-	Mini Project	-	Certification	-
Term Paper	-						

XIV. ASSESSMENT METHODOLOGIES-INDIRECT

✔	Early Semester Feedback	✔	End Semester OBE Feedback
✘	Assessment of Mini Projects by Experts		

XV. SYLLABUS

UNIT-I	ATTACKS ON COMPUTERS AND COMPUTER SECURITY	Classes: 08
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.		

<table>
<tr><td><b>UNIT -II</b></td><td><b>SYMMETRIC KEY CIPHERS</b></td><td><b>Classes: 10</b></td></tr>
<tr><td colspan="3">Symmetric key ciphers: Block cipher principles and 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 - Hellman, ECC) key distribution.</td></tr>
<tr><td><b>UNIT -III</b></td><td><b>MESSAGE AUTHENTICATION ALGORITHM AND HASH FUNCTIONS</b></td><td><b>Classes: 08</b></td></tr>
<tr><td colspan="3">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.</td></tr>
<tr><td><b>UNIT -IV</b></td><td><b>E-MAIL SECURITY</b></td><td><b>Classes: 10</b></td></tr>
<tr><td colspan="3">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.</td></tr>
<tr><td><b>UNIT -V</b></td><td><b>WEB SECURITY</b></td><td><b>Classes: 09</b></td></tr>
<tr><td colspan="3">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.</td></tr>
<tr><td colspan="3"><b>Text Books:</b></td></tr>
<tr><td colspan="3">1. William Stallings, “Cryptography and Network Security”, Pearson Education, 4th Edition, 2005.
2. AtulKahate, “Cryptography and Network Security”, McGraw-Hill, 2nd Edition, 2009.</td></tr>
<tr><td colspan="3"><b>Reference Books:</b></td></tr>
<tr><td colspan="3">. 1. C K Shymala, N Harini, Dr. T R Padmanabhan, “Cryptography and Network Security”, Wiley India, 1st Edition, 2016.
2. Behrouz A. ForouzanDebdeepMukhopadhyay, “Cryptography and Network Security”, McGrawHill, 2nd Edition, 2010.</td></tr>
<tr><td colspan="3"><b>Web References:</b></td></tr>
<tr><td colspan="3">1. http://bookboon.com/en/search?q=INFORMATION+SECURITY 2.
2. https://books.google.co.in/books/about/Cryptography_Network_Security_Sie_2E.html?id=Kokjwdf0E7QC
3. https://books.google.co.in/books/about/Information_Security.html?id=Bh45pU0_E_4C</td></tr>
<tr><td colspan="3"><b>E-Text Books:</b></td></tr>
<tr><td colspan="3">1. https://books.google.co.in/books/about/Information_Security.html 2
2. http://www.amazon.in/Cryptography-Network-Security-BehrouzForouzan/dp/007070208X</td></tr>
</table>

XVI. COURSE PLAN:

The course plan is meant as a guideline. Probably there may be changes.

Lecture No	Topics to be covered	Course Learning Outcomes (CLOs)	Reference
1	Understand and explore the basics of security and the need for security.	CLO 1	T1:1.1,1.2
2-4	Understand security approaches, principles of security, types of security attacks, security services and security mechanisms.	CLO 1	T1:1.3,1.4, 1.5,1.6
5-6	Discuss substitution and transposition techniques.	CLO2	T1:2.2,2.3
7	Understands the security depends on location of encryption devices in network	CLO3	T1:2.5
8	Discuss various public and private cryptography encryption and decryption, key size.	CLO 4	T1: 3.1
9-11	Discuss various symmetric cryptography encryption and decryption algorithms	CLO5	T1: 3.2-3.5, 5.1,5.2, 6.1.
12-14	Demonstrate the various asymmetric cryptography encryption and decryption algorithms	CLO6	T1:9.1,9.2, 10.1, 10.4
15	Demonstrate various security aspects of block ciphers for entering into secure network	CLO7	T1:6.2
16	Discuss various security aspects of stream ciphers for entering into secure network	CLO8	T1:6.3
17	Understand RSA algorithm encryption and decryption with examples.	CLO10	T1: 9.1,9.2
18	Illustrate elliptic curve cryptography with examples.	CLO9	T1: 10.2,10.3
19-21	Understand various methods of message authentication algorithms	CLO 11	T1:11.1-11.3
22	Discuss the importance of digital signature for data transmission.	CLO12	T1:13.1-13.3
23-24	Demonstrate various techniques of hash function with examples.	CLO 13	T1:11.4,11.5
25-26	Discuss the importance of different hash algorithms	CLO 14	T1:12.1-12.4
27-30	Understand PGP functionality and its importance.	CLO 15	T1:15.1
31-33	Understand S/MIME functionality and its importance.	CLO 15	T1:15.2
34-36	Discuss how devices are managed on IP network.	CLO 16	T1:16.1-16.5
37-39	Demonstrate how SSL and TLS provides security in World Wide Web	CLO 17	T1:17.1-17.3
40-41	Understand various types of firewalls and its importance.	CLO 20	T1:20.1-20.2
42-43	Understand various types of viruses and its vulnerabilities.	CLO19	T1:19.1-19.4
44-45	Discuss different Inter branch payment transactions cross site scripting.	CLO 18	T1:18.1-18.3

XVII. GAPS IN THE SYLLABUS - TO MEET INDUSTRY / PROFESSION REQUIREMENTS:

S No	Description	Proposed actions	Relevance with POs	Relevance with PSOs
1	Security mechanisms implementationon real world problems	Work Shops/ Guest Lectures / NPTEL/ Laboratory Practices	PO2, PO3	PSO1, PSO2
2	Working Process of intrusion detection and avoidance	Work Shops/ Laboratory Practices	PO1, PO3, PO5	PSO2, PSO2
3	Laboratory practice on IP security for providing security to IP network.	Work Shops/ Laboratory Practices/ Guest Lectures	PO1, PO2, PO3, PO4	PSO1, PSO2

Prepared by:

Ms. B Geetavani, Assistant Professor

HOD, CSE