INSTITUTE OF AERONAUTICAL ENGINEERING
(Autonomous)
Dundigal, Hyderabad - 500 043

COURSE DESCRIPTION

Department	**INFORMATION TECHNOLOGY**				
Course Title	**INFORMATION SECURITY**				
Course Code	AITB22				
Program	B.Tech				
Semester	VI				
Course Type	Elective				
Regulation	R-18				
Course Structure	Theory			Practical	
	Lecture	Tutorials	Credits	Laboratory	Credits
	3	-	3	-	-
Course Coordinator	Dr P L Srinivasa murthy				

I COURSE PRE-REQUISITES:

Level	Course Code	Semester	Prerequisites
B.Tech	AITB10	V	Computer Networks

II COURSE OVERVIEW:

This course focuses on the fundamentals of security that are used in protecting both the information present in computer storage as well as information passing over any computer networks. It includes attacks, security mechanisms, and secret-key and public-key cryptography. The authentication protocols and key management techniques for providing security in Email, IP and web, Firewalls and virtual private networks are learned.

III MARKS DISTRIBUTION:

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

IV CONTENT DELIVERY / INSTRUCTIONAL METHODOLOGIES:

✓	Power Point Presentations	✓	Chalk & Talk	✓	Assignments	x	MOOC
x	Open Ended Experiments	x	Seminars	x	Mini Project	x	Videos
x	Others						

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 CIE 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 FIVE modules and each module 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 module. Each question carries 14 marks. There could be a maximum of two sub divisions in a question.
The expected percentage of cognitive level of the questions is broadly based on the criteria given in below Table.

Percentage of Cognitive Level	Blooms Taxonomy Level
10%	Remember
45%	Understand
18%	Apply
27%	Analyze

Continuous Internal Assessment (CIA):

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

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 8^{th} and 17^{th} 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 - Online Examination

Two Quiz exams shall be online examination consisting of 25 multiple choice questions and are to be answered by choosing the correct answer from a given set of choices (commonly four). Such a question paper shall be useful in testing of knowledge, skills, application, analysis, evaluation and understanding of the students. Marks shall be awarded considering the average of two quiz examinations for every course.

Alternative Assessment Tool (AAT)

This AAT enables faculty to design own assessment patterns during the CIA. The AAT converts the classroom into an effective learning center. The AAT may include tutorial hours/classes, seminars, assignments, term paper, open ended experiments, METE (Modeling and Experimental Tools in Engineering), five minutes video, MOOCs etc. The AAT chosen for this course is given in table

Concept Video	Tech-talk	Complex Problem Solving
40%	40%	20%

VI COURSE OBJECTIVES:

The students will try to learn:

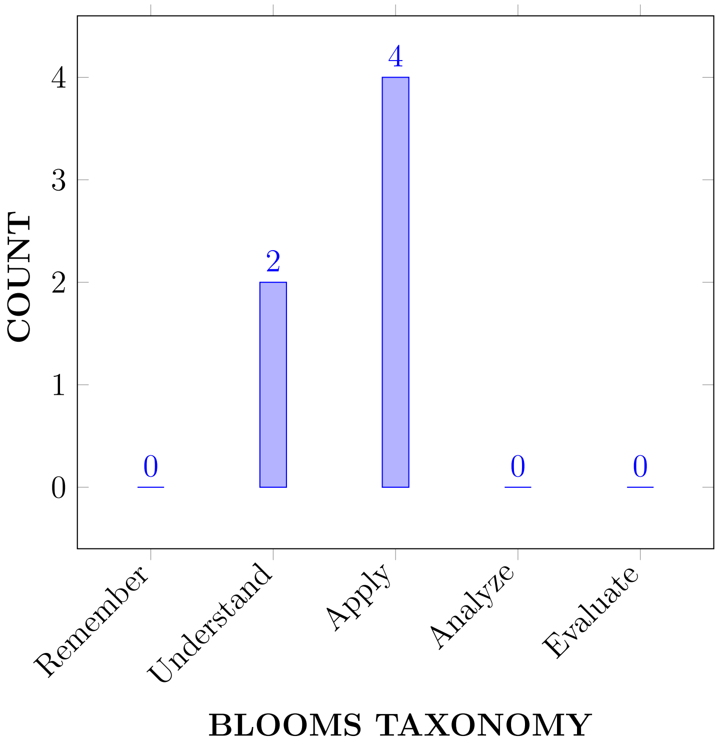
I	Understand security standards and practices. The scope and essentiality of threats, attacks to computers and networks associated to them
II	The symmetric and asymmetric key generation techniques used for providing message authentication, confidentiality and Integrity
III	The use cases on cryptography and security systems for server and client systems such as web, email and firewalls

VII COURSE OUTCOMES:

After successful completion of the course, students should be able to:

CO 1	**Outline** dmodel for network security and cryptographic algorithms to prevent attacks on computer and computer security.	Understand
CO 2	**Demonstrate** symmetric and asymmetric key ciphers for messaging end to end encryption used in different types of cryptographic algorithms	Understand
CO 3	**Make use of** tools and protocols used in message authentication and hashing functions for every day computing to remine secure	Apply
CO 4	**Choose** appropriate architecture and protocols used in email and IP security to protect against attackers and intruders	Apply
CO 5	**Select** firewalls to provide web security as case study in cryptography and network security	Apply
CO 6	**Utilize** cryptographic and security algorithms to enhance defence against cyber attacks and to improve organization working culture.	Apply

COURSE KNOWLEDGE COMPETENCY LEVEL



VIII PROGRAM OUTCOMES:

Program Outcomes	
PO 1	**Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
PO 2	**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.
PO 3	**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
PO 4	**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.
PO 5	**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
PO 6	**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.
PO 7	**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.
PO 8	**Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
PO 9	**Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
PO 10	**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.
PO 11	**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.
PO 12	**Life-Long Learning:** Recognize the need for and having the preparation and ability to engage in independent and life-long learning in the broadest context of technological change

IX HOW PROGRAM OUTCOMES ARE ASSESSED:

PROGRAM OUTCOMES		Strength	Proficiency Assessed by
PO 1	**Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.	2.3	SEE / CIE / AAT
PO 2	**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.	2.6	SEE / CIE / AAT
PO 3	**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	1.3	SEE / CIE / AAT
PO 4	**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.	1	SEE / CIE / AAT
PO 10	**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.	1	SEE / CIE / AAT
PO 12	**Life-Long Learning:** Recognize the need for and having the preparation and ability to engage in independent and life-long learning in the broadest context of technological change	1	SEE / CIE / AAT

3 = High; 2 = Medium; 1 = Low

X HOW PROGRAM SPECIFIC OUTCOMES ARE ASSESSED:

PROGRAM SPECIFIC OUTCOMES		Strength	Proficiency Assessed by
PSO 1	Understand, design and analyze computer programs in the areas related to Algorithms, System Software, Web design, Big data, Artificial Intelligence, Machine Learning and Networking.	3	SEE/CIE/AAT
PSO 2	Focus on improving software reliability, network security / information retrieval systems.	2	SEE/CIE/AAT
PSO 3	Make use of modern computer tools for creating innovative career paths, to be an entrepreneur and desire for higher studies.	2	SEE/CIE/AAT

3 = High; 2 = Medium; 1 = Low

XI MAPPING OF EACH CO WITH PO(s),PSO(s):

COURSE OUTCOMES	PROGRAM OUTCOMES												PSO'S		
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO 1	✓	✓	✓	✓	-	-	-	-	-	✓	-	✓	✓	✓	✓
CO 2	✓	✓	✓	-	-	-	-	-	-	✓	-	✓	✓	✓	✓
CO 3	✓	✓	✓	-	-	-	-	-	-	✓	-	✓	✓	✓	✓
CO 4	✓	✓	✓	-	-	-	-	-	-	✓	-	✓	✓	✓	✓
CO 5	✓	✓	✓	-	-	-	-	-	-	✓	-	✓	✓	✓	✓
CO 6	✓	✓	✓	✓	-	-	-	-	-	✓	-	✓	✓	✓	✓

XII JUSTIFICATIONS FOR CO – PO/ PSO MAPPING -DIRECT:

Course Outcomes	PO'S PSO'S	Justification for mapping (Students will be able to)	No. of Key competencies matched.
CO 1	PO 1	Summarize the knowledge of mathematics, Scientific and Engineering principals to prevent attacks on computer using network security and cryptographic algorithms	3
	PO 2	Classify different network security and cryptographic algorithms by problem identification, formulation, abstraction, data collection, design and provide solution to prevent attacks on computer	7
	PO 3	Outline the customer requirements, maintenance and engineering activities to prevent attacks on computer using network and cryptography algorithms.	3
	PO 4	Interpret the appropriate quantitative method, engineering principles and the ability to apply them to develop the cryptographic and network security algorithms to prevent attacks on computer.	4

Course Outcomes	PO'S PSO'S	Justification for mapping (Students will be able to)	No. of Key competencies matched.
	PO 10	Security problems on computers will be solved with clear applications of engineering network, security and cryptographic algorithms	2
	PO 12	Use appropriate techniques and algorithms in computer science related, industry oriented applications for preventing attacks on computers.	3
	PSO 1	Understand the problem specific constraints to prevent attacks on computers by applying appropriate network security and cryptographic algorithms.	4
	PSO 2	Focus on improving network security by selecting appropriate network security and cryptographic algorithms to prevent attacks on computer.	1
	PSO 3	Extend the use of modern computer tools for creating innovative career paths to prevent attacks on computer using network security and cryptographic algorithms.	1
CO 2	PO 1	Summarize the knowledge of mathematics, Scientific and Engineering principals to prevent attacks on computer using symmetric and asymmetric key ciphers for messaging end to end encryption.	3
	PO 2	Classify different network security and cryptographic algorithms by problem identification, formulation, abstraction, data collection, design and provide solution to prevent attacks on computer using symmetric and asymmetric key ciphers for messaging end to end encryption	6
	PO 3	Outline the customer requirements, maintenance and engineering activities to prevent attacks on computer using symmetric and asymmetric key ciphers for messaging end to end encryption.	3
	PO 10	Security problems on computers will be solved with clear applications of engineering network, security and cryptographic algorithms	2
	PO 12	BUse appropriate techniques and algorithms in computer science related, industry oriented applications for preventing attacks on computers.	3
	PSO 1	IUnderstand the problem specific constraints to provide end to end security by applying appropriate symmetric and asymmetric key ciphers for messaging end to end encryption used in different types of cryptographic algorithms.	4
	PSO 2	Focus on improving network security by selecting appropriate symmetric and asymmetric key ciphers to provide end to end security.	1
	PSO 3	BExtend the use of modern computer tools for creating innovative career paths to prevent attacks on computer using symmetric and asymmetric key ciphers for messaging end to end encryption used in different types of cryptographic algorithms.	1

Course Outcomes	**PO'S PSO'S**	**Justification for mapping (Students will be able to)**	**No. of Key competencies matched.**
CO 3	PO 1	Apply the knowledge of mathematics and Engineering principals to use the tools and protocols used in message authentication and hashing functions for every day computing to remain secure.	2
	PO 2	Classify different tools and protocols required for problem identification, formulation, abstraction, data collection, design and provide solution to prevent attacks on computer using MAC and Hash Function.	7
	PO 3	Outline the customer requirements, maintenance and engineering activities to remain secure in every day computing using MAC and Hash Functions.	3
	PO 10	Security problems on computers will be solved with clear applications of engineering network, security and cryptographic algorithms	2
	PO 12	Use appropriate techniques and algorithms in computer science related, industry oriented applications for preventing attacks on computers.	3
	PSO 1	Understand the problem specific constraints to prevent attacks on computers by applying appropriate network security and cryptographic algorithms.	4
	PSO 2	Focus on improving network security by selecting appropriate tools and protocols used in message authentication and hashing functions for every day computing to remain secure.	1
‘	PSO 3	Make use of modern computer tools for creating innovative career paths for every day computing to remain secure using MAC and Hash functions.	1
CO 4	PO 1	Apply the knowledge of mathematics and Engineering principals to Choose appropriate architecture and protocols to provide security to email against attackers and intruders.	2
	PO 2	Make use of appropriate architecture and protocols required for problem identification, formulation, abstraction, data collection, design and to provide security to E-mail and IP.	7
	PO 3	Outline the customer requirements, maintenance and engineering activities to provide security to email against attackers and intruders.	4
	PO 10	Security problems on computers will be solved with clear applications of engineering network, security and cryptographic algorithms	2
	PO 12	Use appropriate techniques and algorithms in computer science related, industry oriented applications for preventing attacks on computers.	3
	PSO 1	Understand the problem specific constraints to prevent attacks on E-mail and IP by choosing appropriate architecture and protocols.	4

Course Outcomes	PO'S PSO'S	Justification for mapping (Students will be able to)	No. of Key competencies matched.
	PSO 2	Focus on improving network security by selecting appropriate network security and cryptographic algorithms to prevent attacks on computer.	1
	PSO 3	Extend the use of modern computer tools for creating innovative career paths to prevent attacks on E-mail using appropriate algorithms.	1
CO 5	PO 1	Apply the knowledge of mathematics and Engineering principals to Select firewalls to provide web security as case study in cryptography and network security	2
	PO 2	Classify different firewalls required for problem identification, formulation, abstraction, data collection, design and to provide web security.	7
	PO 3	Outline the customer requirements, maintenance and engineering activities to provide web security using appropriate firewalls.	4
	PO 10	Security problems on computers will be solved with clear applications of engineering network, security and cryptographic algorithms .	2
	PO 12	Use appropriate techniques and algorithms in computer science related, industry oriented applications for preventing attacks on computers.	3
	PSO 1	Understand the problem specific constraints to provide web security by using appropriate firewall.	4
	PSO 2	Focus on improving network security by selecting appropriate firewalls and methods to provide web security.	1
	PSO 3	Extend the use of modern computer tools for creating innovative career paths to to provide web security by using appropriate firewall.	1
CO 6	PO 1	Apply the knowledge of mathematics and Engineering principals to to enhance defence against cyber-attacks and to improve organization working culture using cryptographic and security algorithms.	3
	PO 2	Classify different cryptographic and security algorithms required for problem identification, formulation, abstraction, data collection, design and provide solution to enhance defence against cyber-attacks and to improve organization working culture.	7
	PO 3	Outline the customer requirements, maintenance and engineering activities to enhance defence against cyber-attacks and to improve organization working culture using cryptographic and security algorithms	5
	PO 4	Interpret the appropriate quantitative method, engineering principles and the ability to enhance defence against cyber-attacks and to improve organization working culture	5
	PO 10	Security problems on computers will be solved with clear applications of engineering network, security and cryptographic algorithms	2

Course Outcomes	PO'S PSO'S	Justification for mapping (Students will be able to)	No. of Key competencies matched.
	PO 12	Use appropriate techniques and algorithms in computer science related, industry oriented applications for preventing attacks on computers.	3
	PSO 1	Understand the problem specific constraints to prevent attacks on computers by applying appropriate network security and cryptographic algorithms.	4
	PSO 2	Focus on improving network security by selecting appropriate network security and cryptographic algorithms to prevent attacks on computer.	1
	PSO 3	Extend the use of modern computer tools for creating innovative career paths to prevent attacks on computer using network security and cryptographic algorithms.	1

XIII TOTAL COUNT OF KEY COMPETENCIES FOR CO – PO/ PSO MAPPING:

COURSE OUTCOMES	PROGRAM OUTCOMES												PSO'S		
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO 1	3	7	3	4	-	-	-	-	-	2	-	1	4	1	1
CO 2	3	6	3	-	-	-	-	-	-	2	-	1	4	1	1
CO 3	2	7	3	-	-	-	-	-	-	2	-	1	4	1	1
CO 4	2	7	4	-	-	-	-	-	-	2	-	1	4	1	1
CO 5	2	7	4	-	-	-	-	-	-	2	-	1	4	1	1
CO 6	3	7	5	5	-	-	-	-	-	2	-	1	4	1	1

XIV PERCENTAGE OF KEY COMPETENCIES FOR CO – PO/ PSO

COURSE OUTCOMES	PROGRAM OUTCOMES												PSO'S		
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO 1	100	70	30	36.36	-	-	-	-	-	40	-	12.5	66.66	50	50
CO 2	100	60	30	-	-	-	-	-	-	40	-	12.5	66.66	50	50
CO 3	60	70	30	-	-	-	-	-	-	40	-	12.5	66.66	50	50
CO 4	60	70	40	-	-	-	-	-	-	40	-	12.5	66.66	50	50
CO 5	60	70	40	-	-	-	-	-	-	40	-	12.5	66.66	50	50
CO 6	60	60	40	45.45	-	-	-	-	-	40	-	12.5	66.66	50	50

XV COURSE ARTICULATION MATRIX (PO / PSO MAPPING):

CO'S and PO'S and CO'S and PSO'S on the scale of 0 to 3, 0 being no correlation, 1 being the low correlation, 2 being medium correlation and 3 being high correlation.

0 - $0 \leq C \leq 5\%$ – No correlation

1 - $5 < C \leq 40\%$ – Low/ Slight

2 - $40\ \% < C < 60\%$ –Moderate

3 - $60\% \leq C < 100\%$ – Substantial /High

COURSE OUTCOMES	PROGRAM OUTCOMES												PSO'S		
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO 1	3	3	1	1	-	-	-	-	-	1	-	1	3	2	2
CO 2	3	2	1		-	-	-	-	-	1	-	1	3	2	2
CO 3	2	3	1	-	-	-	-	-	-	1	-	1	3	2	2
CO 4	2	3	2	-	-	-	-	-	-	1	-	1	3	2	2
CO 5	2	3	2	-	-	-	-	-	-	1	-	1	3	2	2
CO 6	2	2	1	1	-	-	-	-	-	1	-	1	3	2	2
TOTAL	14	16	8	2	-	-	-	-	-	6	-	6	18	12	12
AVERAGE	2.3	2.6	1.3	1	-	-	-	-	-	1	-	1	3	2	2

XVI ASSESSMENT METHODOLOGY-DIRECT:

CIE Exams	✓	SEE Exams	✓	Seminars	✓
Laboratory Practices	-	Student Viva	-	Certification	-
Term Paper	-	5 Minutes Video	✓	Open Ended Experiments	-
Assignments	-	-	-	-	-

XVII ASSESSMENT METHODOLOGY INDIRECT:

✓	Early Semester Feedback	✓	End Semester OBE Feedback
X	Assessment of Mini Projects by Experts		

XVIII SYLLABUS:

MODULE I	ATTACKS ON COMPUTERS AND COMPUTER SECURITY
	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.
MODULE II	SYMMETRIC KEY CIPHERS
	Symmetric key ciphers:Block cipher principles andalgorithms (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.

MODULE III	**MESSAGE AUTHENTICATION ALGORITHM AND HASH FUNCTIONS**
	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.
MODULE IV	**E-MAIL SECURITY**
	E-mail Security: Pretty Good Privacy; S/MIMI IP Security: IP security overview, IP security architecture, authentication header, encapsulating security payload, combining security associations, key management.
MODULE V	**WEB SECURITY**
	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.

TEXTBOOKS

1. William Stallings, —Cryptography and Network Security‖, Pearson Education, 4th Edition, 2005.

2. Atul Kahate, —Cryptography and Network Security‖, McGraw-Hill, 2nd Edition, 2009.

REFERENCE BOOKS:

1. C K Shymala, N Harini, Dr. T R Padmanabhan, —Cryptography and Network Security‖, Wiley India, 1st Edition, 2016.

2. Behrouz A. Forouzan Debdeep Mukhopadhyay, —Cryptography and Network Security‖, McGraw- Hill, 2nd Edition, 2010.

WEB REFERENCES:

1. http://bookboon.com/en/search?q=INFORMATION+SECURITY

2. https://books.google.co.in/books/about/Cryptography_Network_Security_Sie_2E.html?id=Kokjwdf0
C

3. https://books.google.co.in/books/about/Information_Security.html?id=Bh45pU0_E_4C

4. www.technofest2u.blogspot.com

COURSE WEB PAGE:

https://lms.iare.ac.in/index ?route=course/details& course id=84

XIX COURSE PLAN:

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

S.No	Topics to be covered	CO's	Reference T1: 4.1
OBE DISCUSSION			
1	Course Description on Outcome Based Education (OBE): Course Objectives, Course Outcomes (CO), Program Outcomes (PO) and CO - PO Mapping	-	-
CONTENT DELIVERY (THEORY)			
2	Introduction, the need for security	CO 1	T1:1.1-1.4
3	security approaches, principles of security	CO 1	T1:1.5
4	types of security attacks, security services	CO 1	T2:2.2
5	security mechanism, a model for network security	CO 1	T2:2.2
6	Cryptography concepts and techniques: Introduction, plain text and cipher text,	CO 1	T2:2.1-2.2
7	substitution techniques	CO 1	T2:2.3-2.5
8	transposition techniques,	CO 1	T1:2.6
9	encryption and decryption	CO 1	T1:2.7-2.8
10	symmetric and asymmetric key cryptography,	CO 1	T1:3.1-3.2
11	steganography, key range and key size	CO 1	T1:3.2-3.4
12	possible types of attacks.	CO 1	T1:5.2
13	Symmetric key ciphers:Block cipher principles andalgorithms (DES,AES,Blowfish)	CO 2	T1:5.3
14	differential and linear cryptanalysis,	CO 2	T1:5.3
15	block cipher modes of operation,	CO 2	T1:5.3
17	stream ciphers,RC4 location, and placement of encryption function	CO 2	T1:5.4-5.5
18	key distribution; Asymmetric key ciphers: Principles of public key cryptosystems	CO 2	T1:5.6, 21.4
19	algorithms (RSA Diffie-Hellman, ECC) key distribution.	CO 2	T1:6.1
20	Message authentication algorithm and hash functions	CO 3	T1:6.2-6.3
21	Authentication requirements, functions, message	CO 3	T1:6.4
22	authentication codes, hash functions	CO 3	T1:6.5
23	secure hash algorithm	CO 3	T1:6.6-6.7
24	whirlpool, HMAC	CO 3	T1:8.1
26	CMAC	CO 3	T1:8.2
27	digital signatures,	CO 3	T1:8.3

29	knapsack algorithm	CO 3	T1:8.4-8.5
30	Authentication application: Kerberos	CO 3	T1:8.6
31	X.509 authentication service,	CO 3	T1:8.6
33	public – key infrastructure, biometric authentication.	CO 3	T1:9.5
34	E-mail Security: Pretty Good Privacy;	CO 4	T1:9.6
35	S/MIMI IP Security	CO 4	T1:10.1-10.2
36	IP security overview	CO 4	T1:10.3
37	IP security architecture	CO 4	T1:10.5
38	authentication header	CO 4	T1:10.6
39	encapsulating security payload	CO 4	T1:10.6
40	combining security associations	CO 4	T1:11.3
41	key management.	CO 4	T1:11.4
43	Web security: Web security considerations,	CO 5	T1:11.5
44	secure socket layer and transport layer security,	CO 5	T1:11.6
45	secure electronic transaction intruders	CO 5	T1:12.1-12.3
46	Virus and firewallst	CO 5	T1:12.4-12.6
48	Intruders, intrusion detection password management	CO 5	T1:12.7-12.8
49	virus and related threats, countermeasures	CO 6	T1:7.1-7.2
50	firewall design principles;	CO5	T1:8.1
51	Types of firewalls Case Studies on Cryptography and security	CO 5	T1:8.2
52	Secure inter-branch payment transactions	CO 6	T1:8.3
55	cross site scripting vulnerability	CO 6	T2:27.8
56	Secure inter-branch payment transactions	CO 6	T2:27.9
57	virtual electronics.	CO 6	T1:8.2-8.3
PROBLEM SOLVING/ CASE STUDIES			
16	Problems on Substitution techniques	CO 1	T1:5.3-5.3
25	Problems on transposition techniques	CO 1	T1:8.1-8.3
28	Problems on RSA algorithm	CO 2	T1:8.4-8.6 T1:9.1-9.2
32	Problems on encryption and decryption methods	CO 3	T1:9.4-9.6
42	Problems on ceaser cipher method	CO 1	T1:11.3-11.6

47	Problems on Hill Ciphermethod	CO 2	T1:12.1-12.6
53	Problems on performance issues	CO 2	T1:8.1-8.3
54	Problems on DES Algorithm	CO 2	T1:8.1-8.3
DISCUSSION OF DEFINITION AND TERMINOLOGY			
58	Definitions on information security terminologies	CO 1	T1:1.2
59	Definitions on symmetric and asymmetric cipher	CO 2	T1:1.5
60	Definitions on MAC and Hash functions	CO 3	T1:8,9
61	Definitions on E-mil and PGP	CO 4	T1:10,11
62	Definitions on Intruders, Firewalls	CO 5, CO 6	T1:9.1
DISCUSSION OF QUESTION BANK			
1	Tyoes of security attacks	CO 1	T1:1.2
2	Symmetric and asymmetric algrorthims	CO 2	T1:1.5
3	Authentication and hashing algorithms	CO 3	T1:8,9
4	Email security algorithms	CO 4	T1:10,11
5	Intrusion Detection system and firewalls	CO 5,6	T1: 9.1

Signature of Course Coordinator **HOD, CSE**