EASWARI ENGINEERING COLLEGE, CHENNAI-600 089
DEPARTMENT OF INFORMATION TECHNOLOGY
LESSON PLAN

SUBJECT CODE	: IT2352
SUBJECT TITLE	: CRYPTOGRAPHY AND NETWORK SECURITY
HOURS DISTRIBUTION	**:**(L T P C 3 0 0 3)
COURSE/ BRANCH	: B.Tech Information Technology
SEMESTER	: VI
ACADEMIC YEAR	: 2014 - 2015
FACULTY NAME	: Ms.R.S.Lysa Packiam

OBJECTIVE OF COURSE

- To acquire fundamental knowledge on the concepts of Number theory, Encryption, Decryption and understand various public and symmetric key crypto systems.
- To learn about the intruders, viruses , firewalls and its needs

OUTCOME OF COURSE

Upon understanding this course the students will be able to

1. Compare various Cryptographic Techniques
2. Design Secure applications
3. Inject secure coding in the developed applications

PREREQUISTE

Basic Knowledge Of Discrete Mathematics (Algebra), Information Theory And Communication Systems.

UNITS	TOPIC NO	TOPIC	PERIOD	BOOKS REFERRED
1	**UNIT – I(9)**			
	OBJECTIVE To understand the basics of information security and learn the concepts of Number theory necessary of cryptology.			
	1	Security trends	1	T1
	2	Attacks and services	1	T2
	3	Classical cryptosystems	1	T1
	4	Different types of ciphers	1	T1
	5	LFSR sequences	1	T1
	6	Basic Number theory	1	T1
	7	Congruences – Chinese Remainder theorem	1	T1
	8	Modular exponentiation – Fermat and Euler's theorem	1	T1
	9	Jacobi symbols – Finite fields – continued fractions	1	T1
2	**UNIT – II(9)**			
	OBJECTIVE Discuss the fundamental ideas of public-key cryptography and to understand various encryption and decryption techniques for secure data transmission			
	10	Simple DES	1	T1
	11	Differential cryptoanalysis	1	T1
	12	DES – Modes of operation	1	T1
	13	Triple DES	1	T1
	14	AES	1	T1
	15	RC4	1	Hand Outs
	16	RSA	1	T1
	17	Attacks	1	T1
	18	Primality test – factoring	1	T1

3	**UNIT – III(9)**			
	OBJECTIVE To learn various digital signature schemes, their services and to understand the criteria for cryptographic hash functions.			
	19	Discrete Logarithms	1	T1
	20	Computing discrete logs	1	T1
	21	Diffie-Hellman key exchange –ElGamal Public key cryptosystems	1	T1
	22	Hash functions	1	T1
	23	Secure Hash – Birthday attacks	1	T1
	24	MD5	1	Hand Outs
	25	Digital signature	1	T1
	26	RSA – ElGamal	1	T1
	27	DSA	1	T1

4	**UNIT – IV(9)**			
	OBJECTIVE To understand the security services provided for e-mail and learn the authentication protocol			
	28	Authentication applications	1	T1
	29	Kerberos	1	T1
	30	X.509	1	T1
	31	PKI – Electronic Mail security	1	Hand Outs
	32	PGP	1	T1
	33	S/MIME	1	T2
	34	IP security	1	T2
	35	Web Security	1	T2
	36	SSL,TLS, SET	1	T2

5	**UNIT – V(9)**			
	OBJECTIVE To learn about the Intrusion, Viruses , firewalls and its configurations.			
	37	Intruders, Intrusion Techniques	1	T2
	38	Intrusion Detection	1	T2
	39	Viruses and related threats-Malicious Programs	1	T2
	40	Nature of Viruses, Type of Viruses	1	T2
	41	Virus counter measures	1	T2
	42	Firewalls design Principles, firewall characteristics	1	T2
	43	Types of firewalls	1	T2
	44	Firewall configuration	1	T2
	45	Security Standards	1	T2

ASSIGNMENT

SL.NO	TOPICS	SUBMISSION DUE
1	Assignment Problem Sheet I	Feb 12 2015
2	Assignment Problem Sheet Ii	March 11 2015

CONTENT BEYOND SYLLABUS

SL.NO	TOPICS
1	Modern Techniques Of Cryptography

TEXT BOOKS

1. Wade Trappe, Lawrence C Washington, “ Introduction to Cryptography with coding theory”, 2nd ed, Pearson, 2007.

2. William Stallings, “Crpyptography and Network security Principles and Practices”, Pearson/PHI, 4th ed, 2006.

REFERENCES

1. W. Mao, “Modern Cryptography – Theory and Practice”, Pearson Education, Second Edition, 2007.

2.Charles P. Pfleeger, Shari Lawrence Pfleeger – Security in computing Third Edition – Prentice Hall of India, 2006

HOD **FACULTY**

PROGRAMME EDUCATIONAL OBJECTIVES

1. Apply their knowledge of Information Technology and skills for the overall benefit of a diverse society.
2. Use the theory, techniques, and methodologies acquired to create high-quality computing systems that function effectively and reliably in the emerging and futuristic Information Technology Applications and infrastructure.
3. Apply the principles of computer science, mathematics, and scientific investigation to solve real world problems appropriate to the discipline.
4. Will function effectively as individuals and team members in the workplace, growing into technical or project management leadership roles.
5. Deal appropriately with the ethical situations encountered in the workplace.
6. Pursue life-long learning and obtain the tools to successfully identify and adapt to ever changing technologies.
7. Adapt and learn in response to advances in information technology.

PROGRAMME OUTCOMES(a-k)

a) Engineering Knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

b) Problem Analysis: Identify, formulate, research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

c) 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.

d) Investigation of Complex Problem: 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.

e) Modern Tools 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.

f) 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.

g) Environment & Sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

h) Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

i) Individual & Team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

j) 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.

k) Project management & 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.

l) 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.

UNITS	Course outcome	OB1	OB2	OCa	OCb	OCc	OCd	OCe	OCf	OCg	OCh	OCi	OCj	OCk
UNIT 1	Compare various Cryptographic Techniques	S		S										
	Design Secure applications	M	M	S	S	S		S	S	S	S			M
	Inject security in the developed applications	M		S	S	S	M	S		M	S			M
UNIT 2	Compare various Cryptographic Techniques	S		S										
	Design Secure applications	S	M	S	S	S		S	W	S	S			M
	Inject security in the developed applications	S		S	S	S	M	S	W	M	S			M
UNIT 3	Compare various Cryptographic Techniques	S		S										
	Design Secure applications	S	M	S	S	S		S	W	S	S			M
	Inject security in the developed applications	S		S	S	S	M	S	W	M	S			M
UNIT 4	Compare various Cryptographic Techniques	S	M	M			M	S						
UNIT 5	Compare various Cryptographic Techniques	W	S	S			M	S			S		M	

STRONG	S
MEDIUM	M
WEAK	W

MAPPING OF COURSE OUTCOMES WITH PEO & THE PROGRAMME OUTCOME- CRYPTOGRAPHY AND NETWORK SECURITY-IT2352