SCHEME OF COURSE WORK

Course Details:

Course Title	**: NETWORK SECURITY AND CRYPTOGRAPHY**		
Course Code	**:** 13IT2111	**L T P C**	**:4 0 0 3**
Programme:	**: M.Tech.**		
Specialization:	**: Cyber Security**		
Semester	**:Ist Semester**		
Prerequisites	**: Discrete Mathematical Structures**		
Courses to which it is a prerequisite	**: Computer Networks.**		

Course Outcomes (COs):

1	Discuss various attacks, services, mechanisms and various conventional and modern encryption techniques.
2	Describe conventional encryption system and various algorithms in it.
3	Practice number theory and apply its concepts on various algorithms and theorems involved in it.
4	Explain Hash and Mac algorithms and authentication applications.
5	Analyze IP Security Overview and discuss on Intruders, Viruses and Worms.

Program Outcomes (POs):

A graduate of M.Tech Cyber Security Specialization will be able to

1	Apply the knowledge of mathematics, science and engineering to solve problems related to cyber security in general to solve problem related to cyber security in various areas like Network Security, Cryptography, Digital Forensics, Biometric Security, and Intrusion Deletion Systems and so on.
2	Analyze complex security issues, make creative judgment and draw smart conclusions from Forensic evidences, identify security threats and vulnerabilities.
3	Formulate the problems that arise because of the application of cyber laws to various cyberspace scenarios and in Intrusion detection systems and computer network, evaluate alternate solutions and determine optimal solutions that are amicable to health, safety, cultural, and environmental requirements of public.
4	Extract appropriate information from Forensic Investigations, apply research methods and tools to extract information pertaining to Computer Networks Intrusion Detection Systems, Biometric Systems and Wireless Networks and analyze and interpret the data.
5	Use tools and software's such as shell and Perl script to crack security protocols Santoku OS, Helix3pro test vulnerabilities using security scanner and test and show functionalities of security databases through support packages.
6	Participate in collaborative and multidisciplinary endeavors, recognize opportunities and challenges such as one typical of Forensic investigations and contribute positively and be a team player.

7	Acquire project management and finance control abilities in timely manner based on the projects Worked out at the end of their graduation.
8	Gain the skills to communicate effectively with the social and technical organizations based on the subject matters and desertions.
9	Engage themselves in lifelong learning in the context of rapid technological Changes in cyber Security Specialization.
10	Will appreciate ethical and social responsibilities in Professional and Societal context. And the Students will gain basic knowledge to provide services to the society and organizations.
11	Will gain the ability in carrying out tasks independently by reflective learning. And they gain Capability of knowing things by self mistakes and from others mistakes.

Course Outcome versus **Program Outcomes:**

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	S	S										
CO2	S	M										
CO3	S			M								
CO4	M	M										
CO5	S		M	M								

S - Strongly correlated, *M* - *Moderately* correlated, *Blank - No correlation*

Assessment Methods:	Assignment / Quiz / Seminar / Case Study / Mid-Test / End Exam

Teaching-Learning and Evaluation

Week	TOPIC / CONTENTS	Course Outcomes	Sample questions	TEACHING-LEARNING STRATEGY	Assessment Method & Schedule
1	**Introduction:** Attacks, Services and Mechanisms, Security attacks, Security services, A Model for Internetwork security.	CO-1	1).What are the different types of attacks and mechanisms in network security?	▫ Lecture ▫ Discussion	Quiz(Week 6) Mid-Test 1
2	**Classical Techniques:** Conventional Encryption model, Steganography, Classical Encryption Techniques.	CO-1 ,CO-2	1).Explain play fair cipher in detail.	▫ Lecture ▫ Discussion/ ▫ Solving exercise problems	Quiz(Week 6) Mid-Test 1
3	**Modern Techniques:** Simplified DES, Block Cipher Principles, Data Encryption standard, Strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles and Modes of operations.	CO-1,CO-2	1).Differentiate between block cipher and stream cipher. 2).Explain block cipher design principles and modes of operation.	▫ Lecture ▫ Discussion/ ▫ Seminar	Quiz(Week 6) Mid-Test 1
4	**Algorithms:** Triple DES, IDEA algorithm, Blowfish, RC5, CAST-128, RC2, Characteristics of Advanced Symmetric block ciphers.	CO-1,CO-2	1).With a diagram explain the complete encryption technique of cast-128. 2).Briefly explain the operation of AES algorithm.	▫ Lecture ▫ Discussion/ ▫ Seminar	Assignment (Week 8) Mid-Test 1

5	**Conventional Encryption:** Placement of Encryption function, Traffic confidentiality, Key distribution, Random Number Generation.	CO-2	1).Explain Blum Blum shub generator in detail.	▫ Lecture ▫ Discussion/ ▫ Seminar	Quiz(Week 6) Mid-Test 1
6	**Public Key Cryptography:** Principles, RSA Algorithm, Key Management, Diffie-Hellman Key exchange, Elliptic Curve Cryptography.	CO-2, CO3	1).consider a Diffe hellman scheme with a common prime q=13 and a primitive route a=7. a)If Alice has a public key Y_A=5,what is Alice private key X_A ? b)If Bob has a public key Y_B=12,what is the secret key K shared with Alice?	▫ Lecture ▫ Discussion/ ▫ Solving exercise problems	Quiz(Week 6) Mid-Test 1
7	**Number theory:** Prime and Relatively prime numbers, Modular arithmetic, Fermat's and Euler's theorems.	CO-3	1.Explain Fermat's and Euler's theorems.	▫ Lecture ▫ Discussion/ ▫ Solving exercise problems	Assignment (Week 8) Mid-Test 1
8	Testing for primality, Euclid's Algorithm, the Chinese remainder theorem, Discrete logarithms.	CO-3	1).Explain Euclid's theorem. 2).Find all the primitive routes of 19.	▫ Lecture ▫ Discussion/ ▫ Solving exercise problems	Assignment (Week 8) Mid-Test 1
9	**Mid-Test 1**	CO-1,CO-2, CO-3			
10	**Message authentication and Hash functions:** Authentication requirements and functions, Message Authentication, Hash functions, Security of Hash function and MACs.	CO-4	1).Analize the basic uses of message authentication code (MAC).	▫ Lecture ▫ Discussion/ ▫ Seminar	Assignment (Week 15) Mid-Test 2
11	**Hash and Mac Algorithms:** MD File, Message digest Algorithm, Secure Hash Algorithm, RIPEMD-160, HMAC.	CO-4	1).what is SHA? Explain briefly with a diagram.	▫ Lecture ▫ Discussion/ ▫ Seminar	Assignment (Week 15) Mid-Test 2
12	**Digital signatures and Authentication protocols:** Digital signatures, Authentication Protocols, Digital signature standards.	CO-4	1).What is digital signature? Briefly explain about digital signature standards.	▫ Lecture ▫ Discussion/ ▫ Seminar	Assignment (Week 15) Quiz(Week 16) Mid-Test 2
13	**Authentication Applications:** Kerberos, X.509 directory Authentication service**.** Electronic Mail Security: Pretty Good Privacy, S/MIME**.**	CO-4	1).Explain about KerberosV4 2).Explain S/MIME.	▫ Lecture ▫ Discussion/ ▫ Seminar	Assignment (Week 15) Quiz(Week 16) Mid-Test 2
14	**IP Security:** Overview, Architecture, Authentication, Encapsulating Security Payload Combining security Associations, Key Management.	CO-5	1).Discuss the scope of ESP encryption and authentication in both transport mode and tunnel mode.	▫ Lecture ▫ Discussion/ ▫ Seminar	Assignment (Week 15) Quiz(Week 16) Mid-Test 2
15	**Web Security:** Web Security requirements, Secure sockets layer and Transport layer security, Secure Electronic Transaction.	CO-5	1.a)Explain the concept of dual signature. b)Explain about SSL.	▫ Lecture ▫ Discussion/ ▫ Seminar	Assignment (Week 15) Quiz(Week 16) Mid-Test 2
16	**Intruders, Viruses and Worms:** Intruders, Viruses and Related threats. Fire Walls: Fire wall Design Principles, Trusted systems.	CO-5	1).List and explain about different types of firewalls.	▫ Lecture ▫ Discussion/ ▫ Demonstration	Quiz(Week 16) Mid-Test 2
17	**Mid-Test 2**	CO-4, CO-5			
18/19	**END EXAM**				

Faculty Member