SCHEME OF COURSE WORK

Course Details:

Course Title	**: Network Security and Cryptography**		
Course Code	**: 13IT2111**	**L T P C**	**: 4 1 0 3**
Program:	**: M.Tech.**		
Specialization:	**: Software Engineering**		
Semester	**: II**		
Prerequisites	**: Computer Networks**		
Courses to which it is a prerequisite	**: Cyber Security**		

Course Outcomes (COs):

1	Understand various attacks, services, mechanisms and various conventional and modern encryption techniques.
2	Analyze conventional encryption system and various algorithms in it.
3	Understand number theory and various algorithms and theorems involved in it.
4	Understand Hash and Mac algorithms and authentication applications.
5	Analyze IP Security Overview and Intruders, Viruses and Worms.

Program Outcomes (POs):

A graduate of Information Technology will be able to

1	Ability to demonstrate in-depth knowledge of Software Engineering with analytical and synthesizing skills.
2	Ability to analyze complex problems critically and provide viable solutions.
3	Ability to evaluate potential solutions to a problem and arrive at optimal solutions.
4	Ability to apply research methodologies to develop innovative techniques for solving complex Information Technology related problems.
5	Ability to apply techniques and tools to solve complex problems.
6	Ability to work as an effective team member in a collaborative and multidisciplinary project to achieve common goals.
7	Ability to manage a software team and to maintain financial records as per standards.
8	Ability to effectively communicate with clients, peers and society at large.
9	Ability to take up lifelong learning to be in tune with the fast-changing software related technologies.
10	Ability to follow ethical practices in the software industry and accept social responsibility.
11	Ability to learn independently from mistakes and surge forward with positive attitude and enthusiasm.

Course Outcome Versus **Program Outcomes:**

COs	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**
CO-1		S	M	S	M				M		
CO-2		S		S	S					M	
CO-3		M	S	S	S						
CO-4		M	S		M					S	
CO-5		S	S	S						S	

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

Assessment Methods:	Assignment / Mid-Test / End Exam

Teaching-Learning and Evaluation

Week	TOPIC / CONTENTS	Course Outcomes	Sample questions	TEACHING-LEARNING STRATEGY	Assessment Method & Schedule
1	Attacks, Services and Mechanisms, Security attacks, Security services, A Model for Internetwork security Conventional Encryption model	CO-1	1. What are active and passive attacks?	▫ Lecture ▫ PPT	Assignment (Week 4 - 6) Mid-Test 1 (Week 9)
2	Classical Encryption Techniques Modern Techniques:Simplified DES, Block Cipher Principles	CO-2	1. Explain Polyalphabetic cipher and Monoalphabetic cipher 2. What is the difference between block cipher and stream cipher	▫ Lecture ▫ PPT	
3	Data Encryption standard, Strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles	CO-2	1. Explain DES algorithm	▫ Lecture ▫ Discussion	
4	Modes of operations, Algorithms: Triple DES, International Data Encryption algorithm	CO-2		▫ Lecture ▫ Discussion	
5	Blowfish, RC5, CAST-128, RC2, Characteristics of Advanced Symmetric block ciphers, Conventional Encryption: Placement of Encryption function	CO-2		▫ Lecture ▫ PPT	Mid-Test 1 (Week 9)
6	Traffic confidentiality, Key distribution, Random Number Generation, Public Key Cryptography: Principles	CO-2	1. Explain RSA algorithm 2. Explain Diffie-Hellman key exchange algorithm	▫ Lecture ▫ PPT ▫ Discussion	
7	RSA Algorithm, Key Management, Diffie - Hellman Key exchange, Elliptic Curve Cryptograpy	CO-2		▫ Lecture ▫ PPT ▫ Discussion	
8	Number theory: Prime and Relatively prime numbers, Modular arithmetic, Fermat's and Euler's theorems, Testing for primality, Euclid's Algorithm, The Chinese remainder theorem, Discrete logarithms	CO-3	1. State Fermat's theorem. Using it compute 3**96 mod 7 2. Discuss Primality testing algorithm	▫ Lecture ▫ PPT	

9	**Mid-Test 1**				
10	Message authentication and Hash functions: Authentication requirements and functions, Message Authentication, Hash functions, Security of Hash function and MACs	CO-3	1. Difference between Message Digest and Message Authentication Code 2. Explain SHA-1 algorithm	▫ Lecture ▫ PPT	Assignment (Week 14 - 16) Mid-Test 2 (Week 18)
11	Hash and Mac Algorithms: MD File, Message digest Algorithm, Secure Hash Algorithm, RIPEMD-160, HMAC	CO-4		▫ Lecture ▫ PPT	
12	Digital signatures and Authentication protocols, Digital signature standards, Authentication Applications: Kerberos	CO-4		▫ Lecture ▫ PPT	
13	X.509 directory Authentication service, Electronic Mail Security: Pretty Good Privacy, S/MIME.	CO-4	1. Explain PGP email security 2. What are the services provided by IPSEC 3. Explain SSL protocol for providing web security	▫ Lecture ▫ PPT	
14	IP Security: Overview, Architecture, Authentication, Encapsulating Security Payload, Combining security Associations	CO-5		▫ Lecture ▫ PPT	
15	Key Management. Web Security: Web Security requirements, Secure sockets layer and Transport layer security, Secure Electronic Transaction	CO-5		▫ Lecture ▫ PPT	Mid-Test 2 (Week 18)
16	Intruders, Viruses and Worms: Intruders, Viruses and Related threats.	CO-5	1.Explain various types of firewalls. 2. What are the three classes of intruders? 3. What are the different types of viruses? Discuss the Antivirus approaches	▫ Lecture ▫ Discussion	
17	Fire Walls: Fire wall Design Principles, Trusted systems	CO-5		▫ Lecture ▫ Discussion	
18	**Mid-Test 2**				
19/20	**END EXAM**				