Year: B. Tech III (Semester V)

Subject Name: Information and Network Security **Subject Code:** BTCO13501
Type of course: Professional Core Course
Prerequisite (if any): Mathematical Preliminaries

List of Courses where this course will be prerequisite: --

Rationale: The subject covers various important topics concerning information security like symmetric and asymmetric cryptography, key distribution, message authentication, hashing and digital signatures, Email security, firewalls and the utility of the subject in various real life applications.

Teaching and Examination Scheme:

TEACHING SCHEME				Theory Marks			Practical Marks		Total
L	T	P	C	TEE	CA1	CA2	TEP	CA3	
3	0	2	4	60	25	15	30	20	150

CA1: Continuous Assessment (assignments/projects/open book tests/closed book tests CA2: Sincerity in attending classes/class tests/ timely submissions of assignments/self-learning attitude/solving advanced problems TEE: Term End Examination TEP: Term End Practical Exam (Performance and viva on practical skills learned in course) CA3: Regular submission of Lab work/Quality of work submitted/Active participation in lab sessions/viva on practical skills learned in course

Content:

Sr. No.	Content	Total Hrs
1	Introduction : Information Security - Objectives, CIAAN (Confidentiality, Integrity, Availability, Authentication, Non-Repudiation), Mechanisms, Attacks, Symmetric Cipher Model, Cryptography and Cryptanalysis, Classical encryption techniques	4
2	Symmetric ciphers : Stream ciphers and block ciphers, Block Cipher structure, Data Encryption Standard (DES), Modes of Operations, Multiple DES, Advanced Encryption Standard (AES)	9
3	Asymmetric ciphers and its security aspects : Public key characteristics, PKC applications, PKC requirements, Principles of Public-Key Cryptosystems, RSA algorithm, Diffie-Hellman Key Exchange algorithm	8
4	Message Authentication and Hash Functions : authentication requirements and authentication functions, MAC - Message Authentication Codes, SHA, MD5	5
5	Digital signature and authentication: protocols, properties and requirements of digital signature, Elgamal and Schnorr - digital signature schemes, DSS	4

6	Key Management and Distribution : need for key distribution, symmetric key distribution using symmetric and asymmetric encryptions, public keys distribution techniques, A Simple Protocol using KDC	4
7	Network Security : Spoofing, Keyloggers and Spyware, DOS and DDOS attack, SQL injection, Buffer Overflow, Attack on wireless Networks.	4
8	Network Defense tools: Network Defense tools Firewalls and Packet Filters: Firewall Basics, Packet Filter Vs Firewall, Packet Characteristic to Filter, Stateless Vs Stateful Firewalls, Network Address Translation (NAT) and Port Forwarding, Snort: Intrusion Detection System	5
9	Advanced Topics	2

Suggested Specification table with Marks (Theory): (For B.Tech only)

Distribution of Theory Marks					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
15	20	15	5	5	0

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create and above Levels (Revised Bloom's Taxonomy)

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Reference Books:

Sr. No	Title of book /article	Author(s)	Publisher and details like ISBN	Year of publication / Publication Edition
1	Cryptography And Network Security, Principles And Practice	William Stallings	Pearson	Latest Edition
2	Cryptography & Network Security	Forouzan, Mukhopadhyay	McGrawHill	
3	Cryptography and Network Security	Atul Kahate	TMH	
4	Information Security Fundamentals	Peltier, Thomas R	CRC Press. Boca Raton, FL: Auerbach Publications	

			ISBN No.: 978-1-4398-1063-7	
5	Build Your Own Security Lab : A Field Guide for network testing	Michael Gregg	Wiley India	

Course Outcomes:

Sr. No.	CO statement	Marks % weightage
CO-1	Compare and contrast the principles of symmetric and asymmetric cryptography.	20%
CO-2	Select and compile various symmetric key and asymmetric key algorithms.	20%
CO-3	Detect authenticity of messages using message authentication mechanisms.	20%
CO-4	Verify the sender and receiver of the message using digital signature..	10%
CO-5	Select various key management and distribution mechanisms.	10%
CO-6	Evaluate and assess the computer and network systems for associated risks.	20%

List of Open learning website:

- http://www.cryptix.org/
- http://www.cryptocd.org/
- http://www.cryptopp.com/

List of Open Source Software:

- Software : cryptool (www.cryptool.org)

FOR LAB SESSIONS:

List of Experiments:

Sr. No	Practical
1.	Write a program to implement caesar and monoalphabetic cipher.
2.	Write a program to implement the Playfair cipher.
3.	Write a program to implement Hill Cipher.
4.	Write a program to implement the columnar transposition cipher.

5.	Write a program to implement a rail fence transposition cipher.
6.	Write a program to implement the Vigenere Cipher.
7.	Write a program to implement S-DES Cipher.
8.	Write a program to implement the RSA Cryptosystem.
9.	Write a program to implement a Diffie-hellman key exchange algorithm.
10.	Evaluate network defense tools for following (i) IP spoofing (ii) DOS attack
11.	Study the features of firewalls in providing network security and set Firewall Security.
12.	Steps to ensure Security of any one web browser (Mozilla Firefox/Google Chrome)